

# 渠道合作伙伴

## 用户指南

### 产品文档



腾讯云

---

**【版权声明】**

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

## 文档目录

### 用户指南

#### 一级经销商

##### 成为一级经销商

##### 注册成为一级经销商

##### 企业注册文件示例

##### 银行证明示例

##### 合同签署

##### 登录伙伴中心

##### 员工管理

##### 客户业务

##### 经销业务

##### 管理经销商

##### 邀请和审核经销商

##### 查询经销商

##### 分配信用额度

##### 分配代金券额度

##### 经销商账单管理

##### 财务管理

##### 返佣管理

##### 协议管理

##### Tencent Cloud International Data Processing Agreement (with Distributors)

### 二级经销商

#### 受邀注册为二级经销商

##### 登录伙伴中心

##### 员工管理

##### 客户业务

##### 管理客户关系

##### 查询客户

##### 子客账户冻结

##### 为客户分配信用

##### 为客户分配代金券

##### 客户账单管理

##### 协议管理

##### 业务相关

##### Tencent Cloud Second-Level Reseller Terms and Conditions

## Tencent Cloud International Data Processing Agreement (with Second-Level Resellers)

## 经销商

## 成为经销商

[注册成为经销商](#)[企业注册文件示例](#)[银行证明示例](#)[线上合同签署](#)

## 登录伙伴中心

## 账户管理

[查询合作伙伴基础信息](#)

## 员工管理

[基本概念](#)[子账号登录经销商平台](#)[预设角色](#)[新增角色](#)[新增员工](#)[其他权限](#)

## 子客业务

## 子客管理

[查询子客](#)[子客账户冻结和恢复](#)[为子客分配信用](#)[代金券申请操作指引](#)[为客户分配代金券](#)[申请厂商代金券](#)[管理子客关联关系](#)[子客账单管理](#)[子客账单字段说明](#)

## 财务管理

[折扣管理](#)[账户信息](#)[订单管理](#)[账单管理](#)[经销商账单](#)[账单字段说明](#)[账单存至COS存储桶](#)[COS存储桶API获取账单](#)[结算管理](#)



发票管理

返佣管理

对账单管理

返佣明细

协议管理

业务相关

腾讯云国际合作伙伴条款

腾讯云代金券条款

Tencent Cloud International Data Processing Agreement (with Resellers)

子客

受邀绑定成为子客

购买产品

账户管理

代金券

信用额度

账户冻结

账户资产变化的影响

对新购的影响

对停服和恢复的影响

账单管理

子客账单

账单详情

下载账单

续费管理

协议管理

业务相关

TENCENT CLOUD RESELLER CUSTOMER TERMS OF SERVICE

合作伙伴学堂

合作伙伴学院权限申请

登录合作伙伴学院

协议管理

腾讯云国际合作伙伴学堂隐私声明

腾讯云国际合作伙伴学堂服务条款

腾讯云国际合作伙伴学堂申请表范例

访问管理

访问管理概述

预设策略

支持访问管理的 API 接口

# 用户指南

## 一级经销商

### 成为一级经销商

### 注册成为一级经销商

最近更新时间：2023-07-17 10:08:40

注册成为一级经销商，可参考[注册成为经销商](#)。

说明：

- 1、因不同国家地区管理不同，如需您提供更多资质证明，腾讯侧员工会联系您线下补充材料，作为入驻审核使用。

# 企业注册文件示例

最近更新时间：2022-11-16 16:37:45

企业注册文件示例可参考 [企业注册文件示例](#)。

# 银行证明示例

最近更新时间：2022-11-16 16:37:45

银行证明示例可参考 [银行证明示例](#)。

# 合同签署

最近更新时间：2023-07-17 09:41:21

一级经销商暂不提供线上合同签署功能，合同详情请联系您的商务获取。

# 登录伙伴中心

最近更新时间：2022-11-16 16:37:45

登录伙伴中心，可参考 [登录伙伴中心](#)。

# 员工管理

最近更新时间：2023-03-09 11:34:02

员工管理可参考文档[员工管理](#)。

# 客户业务

最近更新时间：2023-07-17 09:41:55

一级经销商，可同时开展一级转售、二级转售业务：

- 1、客户业务（一级转售）：一级经销商直接与客户开展业务，一级经销商——客户，可参考[子客业务](#)。
- 2、二级经销业务（二级转售）：一级经销商，与其转售商开展业务，一级经销商——转售商——客户。



# 经销业务

## 管理经销商

### 邀请和审核经销商

最近更新时间：2023-07-17 09:43:02

说明：

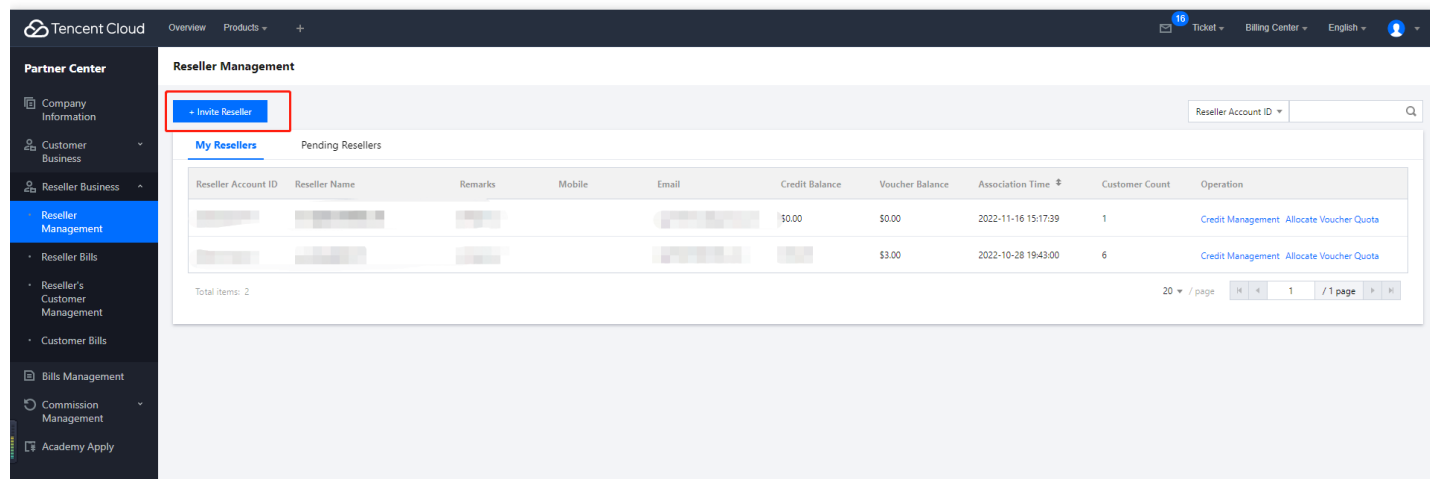
1、经销商解绑：暂不支持线上解绑，如您的经销商有解绑需求，请联系腾讯销售进行线下解绑处理。

#### 1、邀请经销商

可发送邀请链接给经销商，成为一级经销商的经销商。

说明：

仅支持经销商注册新腾讯云账号，申请绑定成一级经销商的经销商，经销商已有的腾讯云账号不可开展转售业务。



The screenshot displays the Tencent Cloud Partner Center interface, specifically the 'Reseller Management' section. The sidebar on the left contains navigation links for 'Partner Center', 'Company Information', 'Customer Business', 'Reseller Business', 'Reseller Management', 'Reseller Bills', 'Reseller's Customer Management', 'Customer Bills', 'Bills Management', 'Commission Management', and 'Academy Apply'. The main content area is titled 'Reseller Management' and features a red box highlighting the 'Invite Reseller' button. Below this, there are two tabs: 'My Resellers' and 'Pending Resellers'. The 'My Resellers' tab is active, showing a table with the following columns: Reseller Account ID, Reseller Name, Remarks, Mobile, Email, Credit Balance, Voucher Balance, Association Time, Customer Count, and Operation. The table contains two rows of data. The first row shows a reseller with a credit balance of \$0.00 and a customer count of 1. The second row shows a reseller with a credit balance of \$3.00 and a customer count of 6. The bottom of the table indicates 'Total Items: 2' and '20 / page'.

Reseller Account ID	Reseller Name	Remarks	Mobile	Email	Credit Balance	Voucher Balance	Association Time	Customer Count	Operation
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	\$0.00	\$0.00	2022-11-16 15:17:39	1	<a href="#">Credit Management</a> <a href="#">Allocate Voucher Quota</a>
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	\$3.00	\$3.00	2022-10-28 19:43:00	6	<a href="#">Credit Management</a> <a href="#">Allocate Voucher Quota</a>

## Invite Reseller



You can send the invitation link to your resellers. After they complete the registration and submit the application materials, you can review their applications on this page.

You can upload an attachment about the application materials requirements and descriptions here for your reseller's reference. You can also modify the [template](#) we offer as needed before uploading it.

[Select File](#)

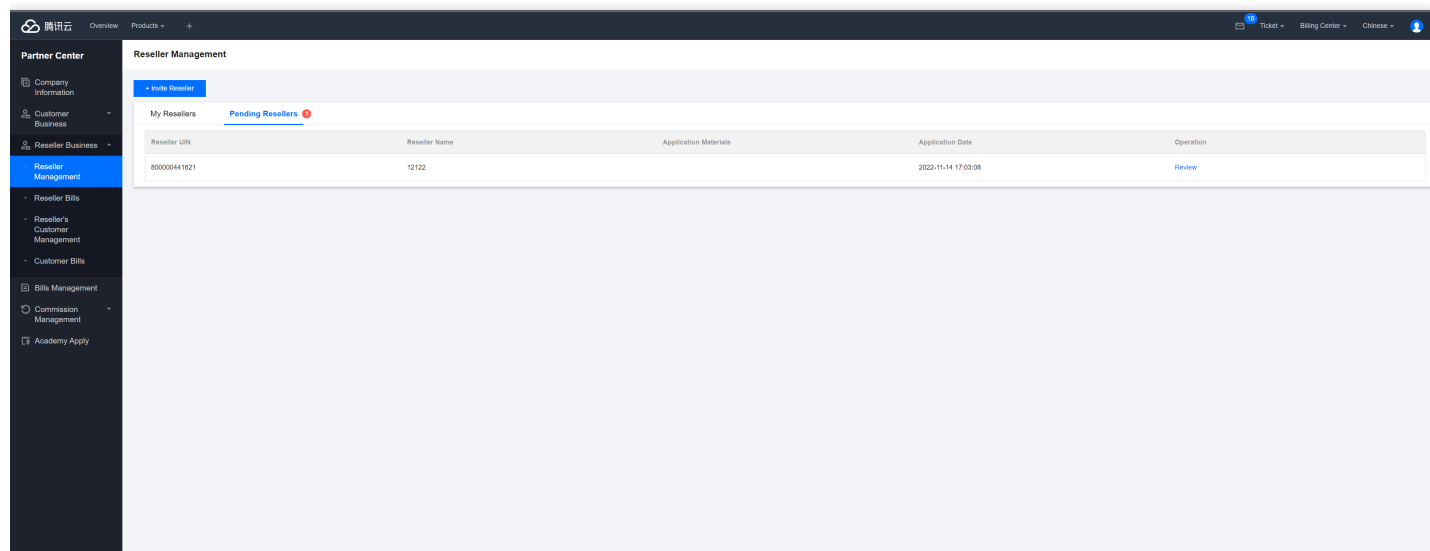
Supported formats: DOCX, PDF.

[Copy URL](#)

[Send Email](#)

## 2、审核经销商

经销商提交绑定申请后，需一级经销商经销审核，确认是否可绑定。



Reseller ID	Reseller Name	Application Materials	Application Date	Operation
800000441621	12122		2020-11-14 17:03:05	<a href="#">Review</a>

**Review Reseller**

Please review whether the account "800000441621" (username: 12122) can become your reseller.

If you approve this application, the binding will take effect immediately. Please comply with Tencent Cloud Partner Program Terms and Conditions.

☐ I have confirmed and agree to the above information

**Approve****Reject****Review Reseller**

Please enter the reason for rejection

0 / 100

**Reject****Cancel**

# 查询经销商

最近更新时间：2023-07-17 09:42:29

一级经销商可以查询其名下所有的经销商，以及查看经销商的基本信息、可用信用额度等。

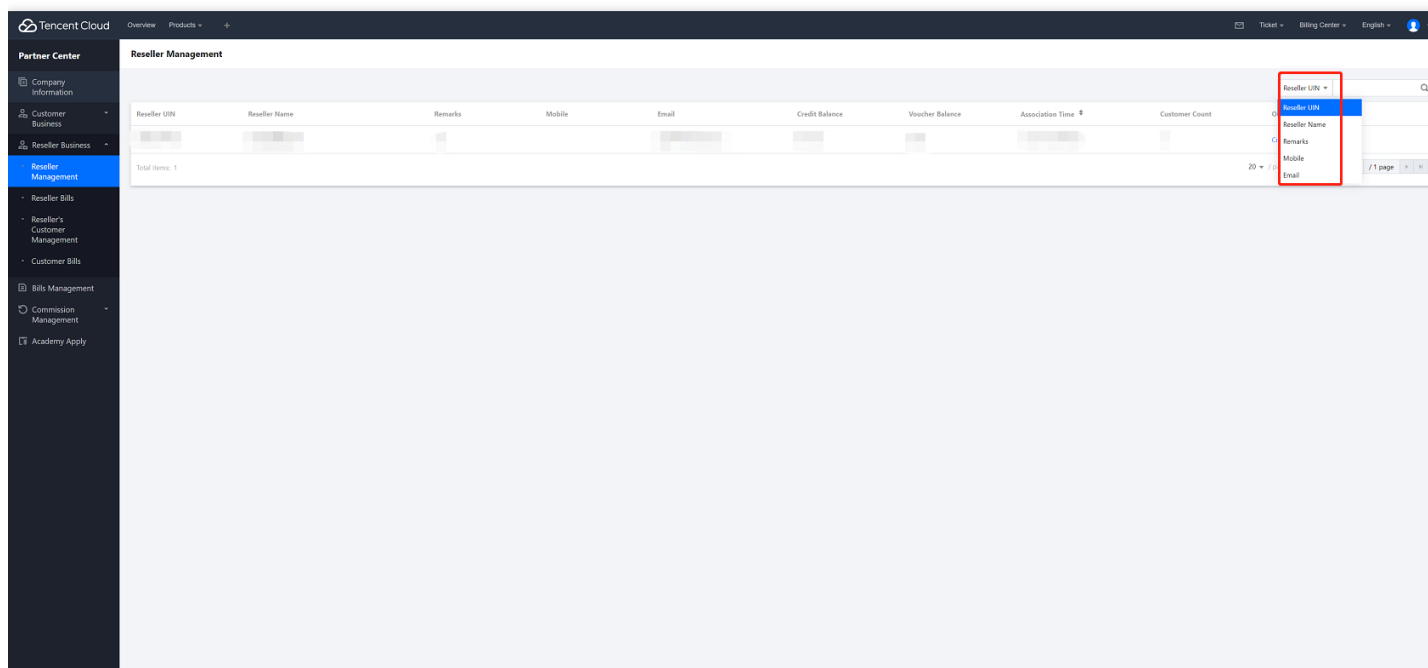
第一步：使用一级经销商账号登录[腾讯云](#)，进入[伙伴中心](#)。

第二步：左侧导航栏中选择【经销商业务】。

第三步：管理经销商。

## 1、查询经销商

一级经销商可根据账号ID、名称等查询经销商。



# 分配信用额度

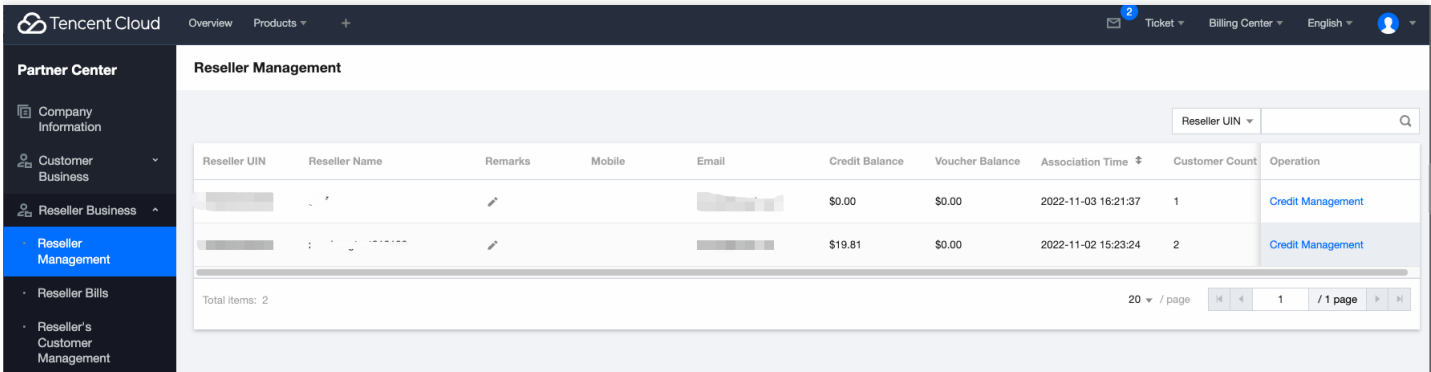
最近更新时间：2023-07-17 09:43:40

一级经销商可以查询其名下所有的经销商，以及查看经销商的基本信息、可用信用额度等。

第一步：线下联系您的销售经理，申请给经销商分配的信用额度。（注：该信用额度区别于一级经销商的自用额度，请联系销售经理申请时说明申请信用额度为经销商信用额度分配使用）。

第二步：使用一级经销商账号登录[腾讯云](#)，进入[伙伴中心](#)。

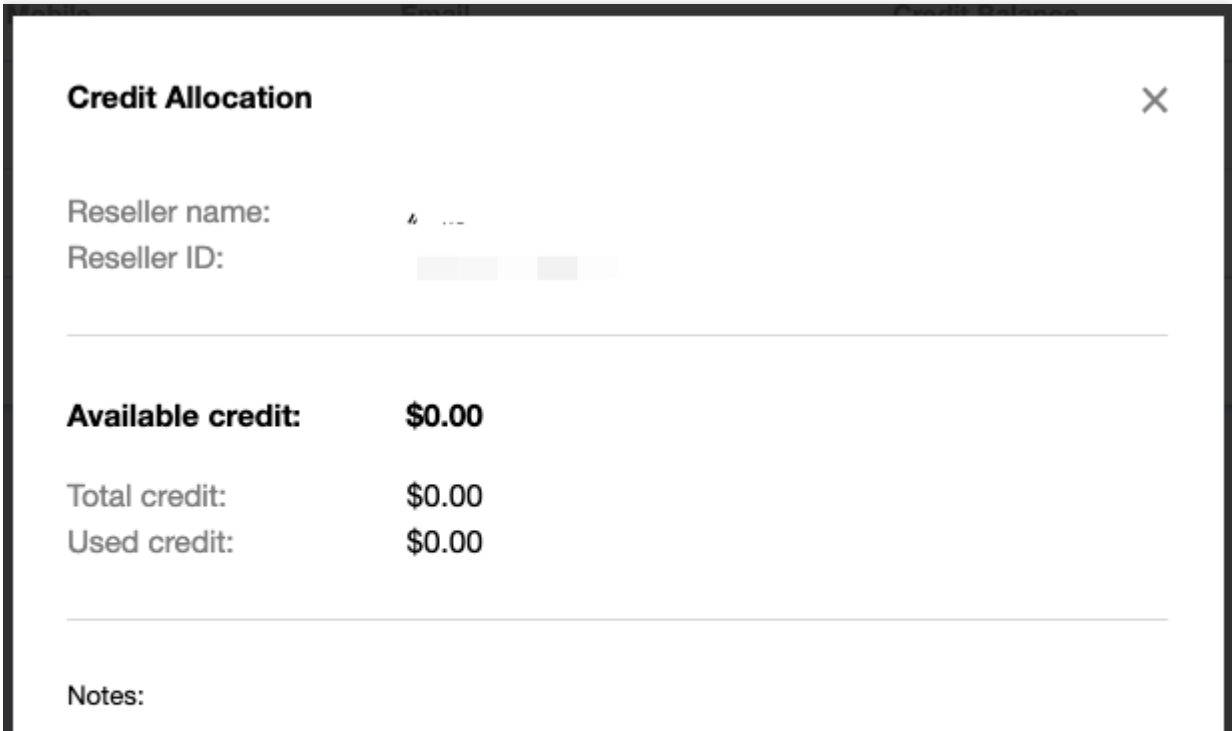
第三步：左侧导航栏中选择【经销商业务】，选择【经销商管理】页签，在列表为经销商分配信用。



第四步：为经销商调整信用。

## 1、分配信用

- 在经销商列表中，选中一条经销商记录，单击操作列的【信用管理】，进入分配信用页面。
- 设置【信用额度】，点击【确认】，系统提示分配成功信息。



1. The credit is granted by you to your resellers only for the purpose of allocating credit among customers.
2. Credit control is only a tool provided by Tencent Cloud for partners to control the approximate amount of credit available to customers. Due to the different billing modes and settlement cycles of Tencent Cloud services, there may be delays and differences in the monitoring of the fees incurred by customers.
3. Your resellers will contact you to adjust the credit offline if their credit balance is insufficient.
4. In the reseller mode, all fees incurred by customers are paid by the partner, so caution should be exercised.
5. A credit will immediately take effect once set.

---

**Allocable credit: \$980.00**

\* Allocated amount: (USD)

Available credit: \$0.00

---

Confirm

Close

[Allocation Record](#)

说明：

1. 信用是合作伙伴授予其经销商的信用额度，仅可供经销商用于分配子客信用使用。
2. 信用控制只是腾讯云为合作伙伴提供的一种工具，用于控制客户的大概信用额度。由于腾讯云服务的计费模式和结算周期不同，对客户产生的费用的监控可能存在延迟和差异。
3. 当经销商信用额度不足时，经销商线下联系您进行额度调整。
4. 在经销模式下，经销商下的子客，产生的所有费用都由合作伙伴支付，因此应谨慎行事。
5. 信用额度一旦设定，将立即生效。

## 2、回收信用

如果分配经销商的信用额度较高，您可输入负值，回收经销商可用信用额度。最高【可回收经销商信用额度】≤【经销商可用信用额度】。

Credit Allocation

×

Reseller name:

Reseller ID:

290020220020

Available credit:

\$19.81

Total credit:

\$20.00

Used credit:

\$0.19

Notes:

1. The credit is granted by you to your resellers only for the purpose of allocating credit among customers.

2. Credit control is only a tool provided by Tencent Cloud for partners to control the approximate amount of credit available to customers. Due to the different billing modes and settlement cycles of Tencent Cloud services, there may be delays and differences in the monitoring of the fees incurred by customers.

3. Your resellers will contact you to adjust the credit offline if their credit balance is insufficient.

4. In the reseller mode, all fees incurred by customers are paid by the partner, so caution should be exercised.

5. A credit will immediately take effect once set.

Allocable credit: \$983.00

\* Allocated amount: (USD)

-3

✓

Available credit: \$16.81

版权所有：腾讯云计算（北京）有限责任公司

第19 共442页

Confirm

Close

Allocation Record

说明：

1、当经销商可用信用额度为0或者负值时，不会触发子客停服、影响子客新购产品。

### 3、分配记录

点击【信用分配页面-分配记录】，可查询一级经销商对经销商的信用分配记录。

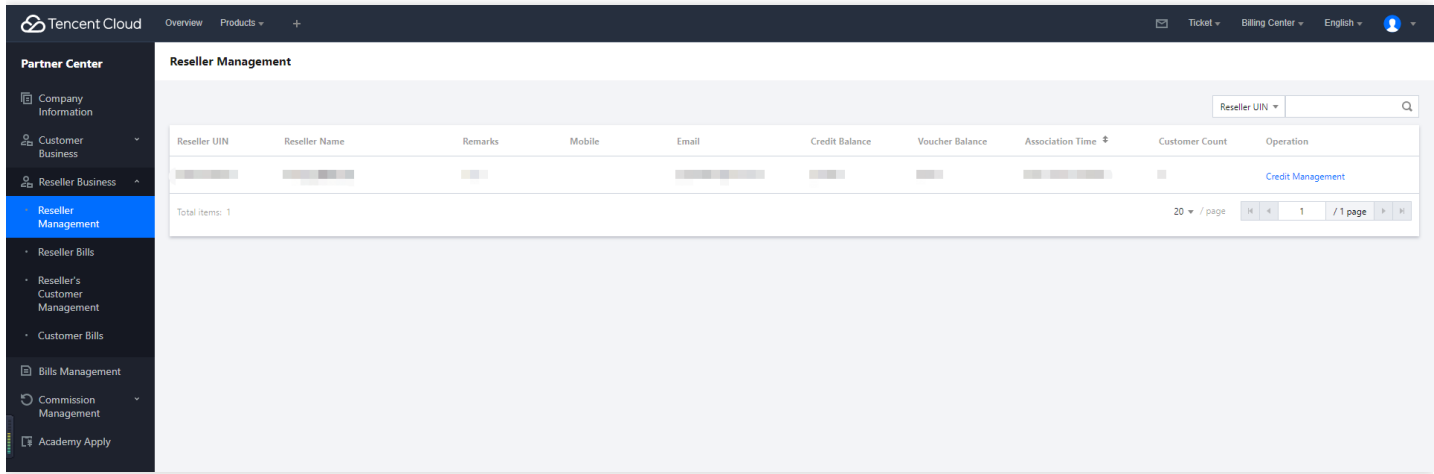
<div> <div>Tencent Cloud</div> <div>OverviewProducts+</div> <div> <div>2</div> <div>Ticket</div> <div>Billing Center</div> <div>English</div> <div></div> </div> </div>			
<div> <div>Partner Center</div> <div> <div>Company Information</div> <div>Customer Business</div> <div>Reseller Business</div> <div>Reseller Management</div> <div>Reseller Bills</div> <div>Reseller's Customer Management</div> </div> </div>			
<div> <div>Allocation Record</div> <div>(200028228023)</div> </div>			
Allocation Time	Current Allocated Credit	Total Allocated Credit	Operator
2022-11-02 15:30:50	\$20.00	\$20.00	
2022-11-02 15:30:42	\$-20.00	\$0.00	
2022-11-02 15:30:32	\$20.00	\$20.00	
<div> <div>Total items: 3</div> <div> <div>1</div> <div>/ 1 page</div> </div> </div>			



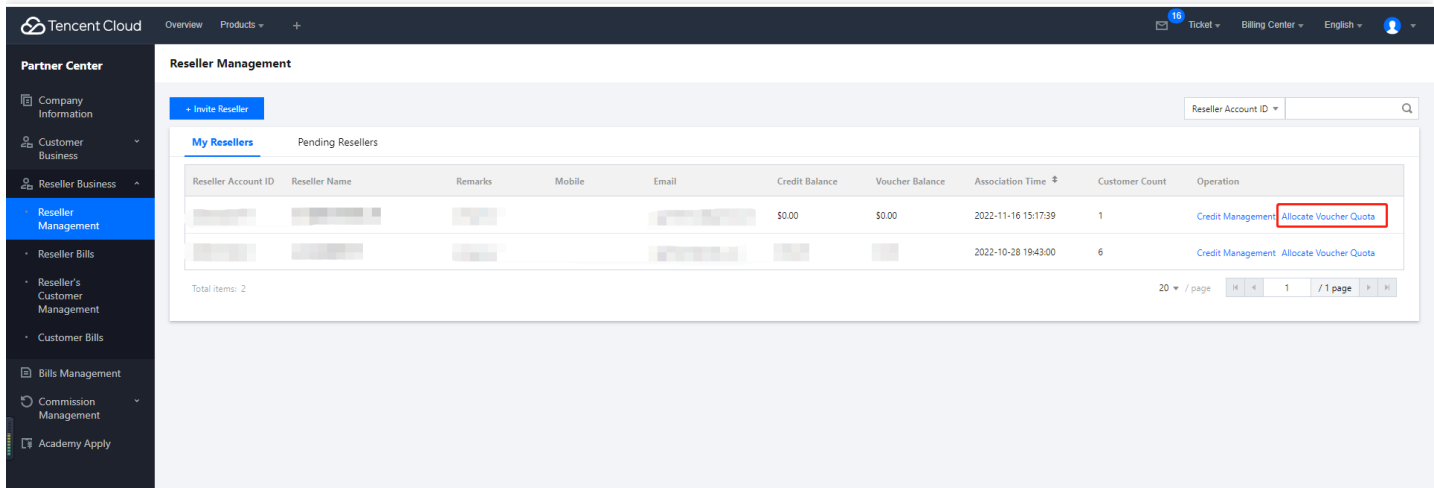
# 分配代金券额度

最近更新时间：2023-10-31 10:27:22

- 第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。
- 第二步：选择 [经销商业务](#)>[经销商管理](#) 菜单进入经销商管理页面。



第三步：点击【分配代金券额度】，填写赋予二级经销商可用的代金券额度，填写正数从一级经销商代金券额度池划拨给二级经销商，填写负数表示从二级经销商额度池回收额度。



Allocate Voucher Quota

×

Reseller Name

Reseller's Existing Quota

\$3.00

Reseller's Available Quota

\$4.00

Current Allocable Balance

Allocated Amount \*

-1

✓

Remaining Allocable Balance

Remarks

0 / 1000

Confirm

Close

第四步：填写代金券额度后，点击【提交】。

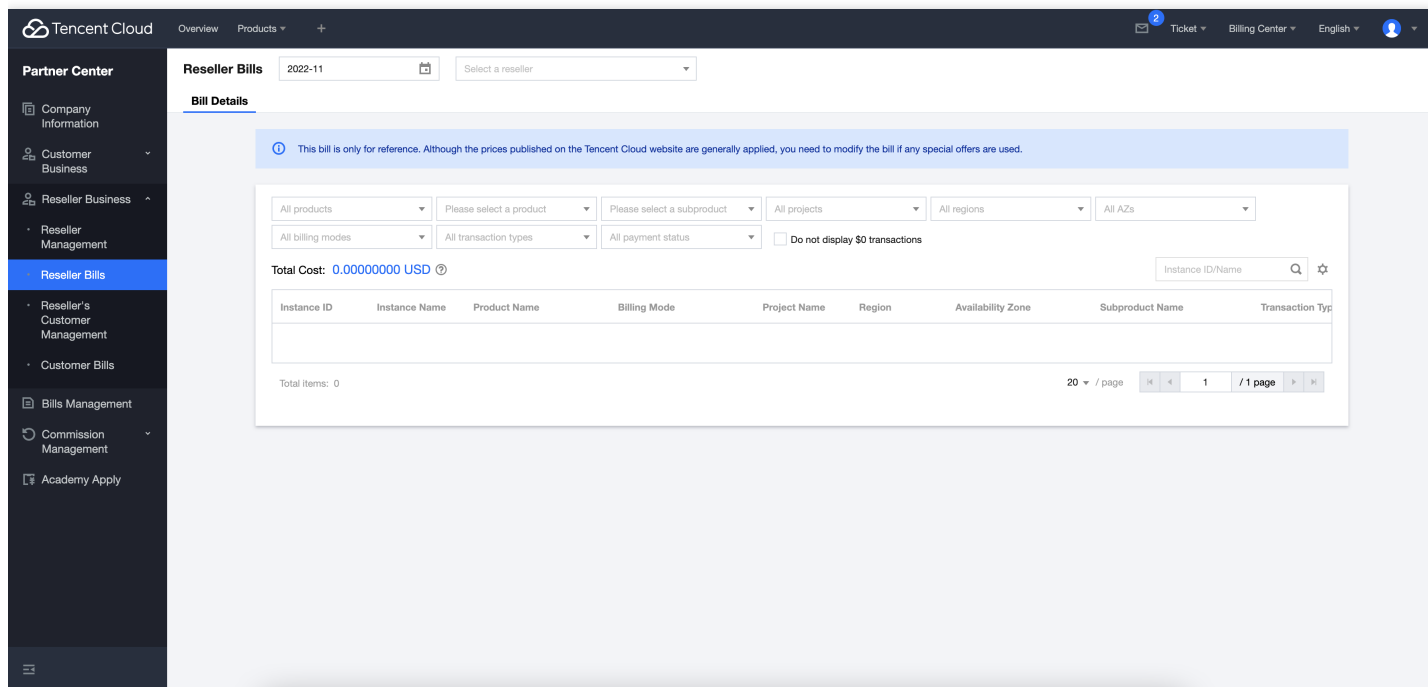
# 经销商账单管理

最近更新时间：2022-11-16 16:37:45

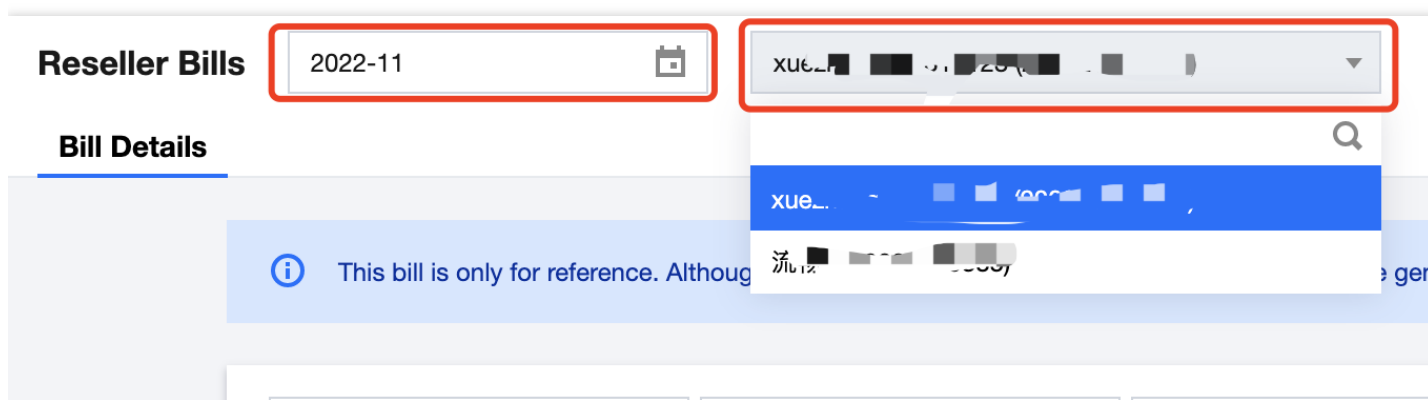
## 经销商账单查询

第一步：使用伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。

第二步：点击左侧菜单【经销商业务>经销商账单】进入经销商账单页面。



第三步：选择账单月份及您的经销商UIN/名称展示该月份指定经销商的账单。



# 财务管理

最近更新时间：2022-11-16 16:37:45

总经销财务管理，可参考 [财务管理](#)。

# 返佣管理

最近更新时间：2022-11-16 16:37:45

返佣管理可参考文档 [返佣管理](#)。

## 协议管理

# Tencent Cloud International Data Processing Agreement (with Distributors)

最近更新时间：2024-06-26 17:44:47

If you have (a) registered as a Partner under the Tencent Cloud Distributor Agreement and (b) entered into a distributor arrangement (whether or not involving integration services) with us under a Distributor Agreement, this Data Processing Agreement (“**DPA**”) applies to any processing of Personal Data in connection with such Distributor Agreement. In the event of any conflict between this DPA, the Distributor Agreement, Console Documentation and Purchase Order, this DPA shall prevail to the extent of the inconsistency. References to “Partner” and “Tencent” in this DPA have the same meaning as set out in the Distributor Agreement.

**Now it is hereby agreed** as follows:

### 1. Definitions

**1.1** Capitalised terms shall have the meaning given to them in the Distributor Agreement, unless otherwise defined below:

“**Personal Data**”, “**Special Categories of Data/Sensitive Data**”, “**Process/Processing**”, “**Controller**”, “**Processor**”, and “**Data Subject**” shall have the same meaning as in the relevant Applicable Data Protection Laws. “**Applicable Data Protection Law**” shall mean:

- a. the General Data Protection Regulation 2016/679 (the “**GDPR**”);
- b. the Privacy and Electronic Communications Directive 2002/58/EC;
- c. the UK Data Protection Act 2018 (“**DPA**”), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (“**UK GDPR**”), and the Privacy and Electronic Communications Regulations 2003;
- d. the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq. as amended by the California Privacy Rights Act of 2020, Cal. Civil Code § 1798.100 et seq. (collectively, “**CCPA**”), the Virginia Consumer Data Protection Act (“**VCDPA**”), the Colorado Privacy Act (“**CPA**”), Connecticut Data Privacy Act (“**CDPA**”), Utah Consumer Privacy Act (“**UCPA**”), Iowa Consumer Data Protection Act (“**ICDPA**”), Indiana Consumer Data Protection Act (“**INCDPA**”), Montana Consumer Data Privacy Act (“**MCDPA**”), Tennessee Information Protection Act (“**TIPA**”), Texas Data Privacy and Security Act (“**TDPSA**”), Oregon Consumer Privacy Act (“**OCPA**”), Florida Digital Bill of Rights (“**FDBR**”) (collectively, “**Applicable US Data Protection Law**”); and
- e. any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or

the use of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

“**Data Discloser**” means the Party who transfers Personal Data to the other Party.

“**Data Receiver**” means the Party who receives Personal Data from the Data Discloser for Processing in accordance with the terms of this Agreement.

“**Distributor Agreement**” means the Tencent Cloud Distributor Agreement in place between Tencent and the Partner.

“**Lawful Export Measure**” means a method allowing for the lawful transfer of Personal Data from a data exporter to a data importer, as may be stipulated by Applicable Data Protection Law or a Regulator from time to time, which may include (depending upon the Applicable Data Protection Laws) model transfer terms prescribed by Applicable Data Protection Laws; or prior registration, licensing or permission from a Regulator.

“**Party**” means a party to this DPA.

“**Partner Console**” means the area designated as console in the Tencent Cloud portal at <http://www.tencentcloud.com>.

“**Personal Data Breach**” means any improper, unauthorised or unlawful access to, use of, or disclosure of, or any other compromise which affects the availability, integrity or confidentiality of Personal Data.

“**Member State**” means the member states of the European Union from time to time.

“**Regulator**” means the data protection supervisory authority which has jurisdiction over a Party’s Processing of Personal Data.

“**Relevant Data Export**” means:

- a. a transfer of Personal Data:
  - i. from a Party which is subject to Applicable Data Protection Law in respect of that Personal Data;
  - ii. to another Party that is in a Third Country or a territory which otherwise (but for the operation of this DPA) does not offer an adequate level of protection as required by Applicable Data Protection Law; and
  - iii. which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law; and
- b. the onward transfer of Personal Data pursuant to (a) to a Third Country or a territory which otherwise (but for the operation of this DPA) does not offer an adequate level of protection as required by Applicable Data Protection Law and which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law.

“**Security Standards**” shall mean the technical and organisational security measures set out in Schedule C.

“**Standard Contractual Clauses**” means:

- a. in the case of transfers of Personal Data relating to Data Subjects in the European Economic Area (“**EEA**”), the standard contractual clauses for the transfer of Personal Data to data processors established in third countries set out in the Commission Decision of 4 June 2021 (C(2021) 3972), as amended and restated from time to time;
- b. in relation to transfers of Personal Data from the UK, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner,

and in each case as amended, updated or replaced from time to time, as attached to and incorporated into this DPA to cover Personal Data transfers to Controllers or Processors as applicable established in Third Countries which do not ensure an adequate level of data protection; and

c. in each case, as amended, updated or replaced from time to time, as attached to and incorporated into this DPA to cover Personal Data transfers to Controllers or Processors, as applicable, established in Third Countries which do not ensure an adequate level of data protection.

**“Third Country”** means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time; and (iii) in relation to Personal Data transfers from any other jurisdiction, any country other than those approved as providing adequate protection for Personal Data by the relevant competent authority of such country from time to time.

**1.2** References to a statutory provision include any subordinate legislation made from time to time under that provision.

**1.3** References to this DPA include the Schedules.

**1.4** Headings shall be ignored in construing this DPA.

**1.5** If a word or phrase is defined, its other grammatical forms have a corresponding meaning.

**1.6** The words “include”, “includes” and “including”, and any succeeding words shall be construed without limitation to the generality of any preceding words or concepts.

**1.7** If there is any inconsistency between the Clauses and Schedules to this DPA the Clauses shall take precedence.

## SCOPE OF THIS AGREEMENT

### 2. General

**2.1** This DPA governs the transfer of Personal Data between Tencent and Partner. This DPA is divided into the following sections:

a. Module A (Transfers between Controllers) sets forth the terms governing any transfer (including a Relevant Data Export) between the Parties, each acting as an independent Data Controller;

b. Module B (Transfers from a Data Controller to a Data Processor) sets forth the terms governing any transfer (including a Relevant Data Export) from Partner (acting as a Data Controller) to Tencent (acting as a Data Processor); and

c. Module C (Transfers from a Data Processor to a Data Controller) sets forth the terms governing any transfer (including a Relevant Data Export) from Partner (acting as a Data Processor) to Tencent (acting as a Data Controller).



# MODULE A – TRANSFERS BETWEEN DATA CONTROLLERS

## 3. APPLICATION OF THIS MODULE A

**3.1** The Parties agree that this Module A applies in each case and only where Personal Data is transferred from Data Discloser to Data Receiver, in circumstances where each Party is acting as an independent Data Controller.

**3.2** The details of the transfers covered by this Module A are specified in Schedule B which forms an integral part of this Module A.

**3.3** In the case of a Relevant Data Export to a Third Country, clause 7 shall govern the terms of the transfer and clauses 4, 5 and 6 shall not apply.

## 4. OBLIGATIONS OF BOTH PARTIES

**4.1** Each Party shall:

- a. Process Personal Data fairly and lawfully;
- b. ensure that Personal Data is accurate and up to date, and inform the other without undue delay if it becomes aware that any of the Personal Data is inaccurate or out of date;
- c. provide reasonable assistance as necessary to the other to enable them to comply with subject access requests and to respond to any other queries or complaints from Data Subjects;
- d. carry out any reasonable request from the other to amend, transfer or delete any Personal Data (to the extent applicable); and
- e. notify the other promptly about any enquiries from a Regulator in relation to Personal Data and cooperate promptly and thoroughly with such Regulator, to the extent required under Applicable Data Protection Law.

## 5. OBLIGATIONS OF DATA DISCLOSER

**5.1** The Data Discloser warrants and undertakes that:

- a. Personal Data have been collected, Processed, and transferred in accordance with Applicable Data Protection Laws, as applicable to the Data Discloser;
- b. it has obtained all consents, authorizations, approvals and rights and provided all notices necessary, including as required by Applicable Data Protection Law, to provide the Personal Data to the Data Receiver and permit the Data Receiver to use the Personal Data in accordance with this DPA;

- c. it has used reasonable efforts to determine that the Data Receiver is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Module A;
- d. it has taken all steps required by Applicable Data Protection Law to avoid “selling” Personal Data to Data Receiver under this Module A (as defined in such laws), including transferring Personal Data at the direction of the relevant individual, or otherwise taken all steps required to comply with obligations relating to “selling” under such Applicable Data Protection Law; and
- e. the Data Discloser shall provide a copy of this Module A and associated Schedules to the Regulator where required.

## 6. OBLIGATIONS OF DATA RECEIVER

### 6.1 Data Receiver warrants and undertakes that:

- a. it will comply with all relevant obligations of Applicable Data Protection Law, including by providing the same level of privacy protections required of controllers and businesses by Applicable Data Protection Law;
- b. it will have in place appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the data to be protected including those in the Security Standards, and shall ensure that those measures continue to provide an appropriate level of security;
- c. in the event of a Personal Data Breach, it shall take appropriate measures to address the Personal Data Breach, and shall (if the breach is likely to result in a risk to individuals) notify the Data Discloser and cooperate with the Data Discloser in relation to any required notifications to the Regulator and/ or to relevant Data Subjects.
- d. it will have in place procedures so that any third party it authorises to have access to Personal Data, including Data Processors, will respect and maintain the confidentiality and security of Personal Data. Any person acting under the authority of the Data Receiver, including a Data Processor, shall be obligated to Process Personal Data only on instructions from the Data Receiver. This provision does not apply to persons authorised or required by law or regulation to have access to Personal Data;
- e. it shall notify the Data Receiver promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The Data Receiver shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. The Data Receiver will provide relevant information about disclosure requests to the Data Discloser, including in relation to its legality review and any challenges to the request;
- f. it will inform the Data Discloser if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Module A;
- g. it will Process Personal Data for purposes described in Schedule B (*Description of Transfer*), and has the legal authority to give the warranties and fulfil the undertakings set out in this Module A;

- h. it shall put in place appropriate technical or organisational measures in order to retain Personal Data for no longer than necessary for the purposes for which it is processed; and
- i. it will keep appropriate documentation of the Processing it carries out under this Module A, and shall make such documentation available to the relevant Regulator(s).

## 7. EXPORT OF PERSONAL DATA

**7.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 1: Controller to Controller, set out in Schedule D-1, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser, who shall comply with the data exporter’s obligations set out in Schedule D-1, and the applicable Data Receiver, who shall comply with the data importer’s obligations set out in Schedule D-1, for that particular transfer of Personal Data for that particular transfer of Personal Data. In relation to any onward transfer of such Personal Data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 1: Controller to Controller set out in Schedule D-1; or (ii) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E, in respect of that Personal Data.

**7.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser. In relation to any onward transfer of such Personal Data by the Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the obligations set out in the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses set out in Schedule D-2, in respect of that Personal Data.

**7.3** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure,. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply mutatis mutandis for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another data importer, the receiving data importer shall comply with the same data importer obligations.

# MODULE B – TRANSFERS FROM DATA CONTROLLER TO DATA PROCESSOR

## 8. APPLICATION OF THIS MODULE B

**8.1** The Parties agree that this Module B applies in each case and only where Personal Data is transferred from Partner (acting as a Data Controller) to Tencent (acting as a Data Processor).

**8.2** The details of the transfers (as well as the Personal Data) covered by this Module B are specified in Schedule B which form an integral part of this Module B.

**8.3** In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, as relevant, clause 12 shall govern the terms of the transfer and clauses 9, 10 and 11 shall not apply.

**8.4** Nothing in this DPA shall relieve Partner or Tencent of liabilities imposed by virtue of their roles in the Processing relationship.

## 9. OBLIGATIONS OF DISTRIBUTOR

**9.1** Partner agrees and warrants that:

- a. it has used reasonable efforts to determine that Tencent is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Module B;
- b. it has obtained all consents, authorizations, approvals and rights and provided all notices necessary, including as required by Applicable US Data Protection Law, to provide the Personal Data to Tencent and permit Tencent to use the Personal Data in accordance with this DPA;
- c. it has disclosed the Personal Data to Tencent for the limited purposes set forth in Schedule B; and
- d. the Processing, including the transfer itself, of Personal Data has been and will continue to be carried out in accordance with the relevant provisions of Applicable Data Protection Law (and, where applicable, has been notified to the relevant authorities of the country in which Partner is established).

**9.2** Partner warrants that it has no reason to believe that any applicable local laws, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent Tencent from fulfilling its obligations under this Module B.

## 10. OBLIGATIONS OF TENCENT

**10.1** Tencent agrees and warrants that it will:

- a. Process Personal Data only on documented instructions of Partner and this DPA for the limited purposes set forth in Schedule B and in compliance with Applicable US Data Protection Law;
- b. not retain, use or disclose Personal Data (i) outside of the direct business relationship between Partner and Tencent or as otherwise permitted by Applicable Data Protection Law, or (ii) for any purpose other than for the limited purposes set forth in Schedule B;
- c. not combine Personal Data received from or on behalf of Partner with any Personal Data that may be collected from Tencent's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Applicable Data Protection Law;
- d. ensure that persons authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- e. take all technical and organisational security measures required by Applicable Data Protection Law relating to data security, and shall ensure that those measures continue to provide an appropriate level of security;
- f. taking into account the nature of the Processing, assist Partner by implementing appropriate technical and organisational measures, insofar as this is practicable, for the fulfilment of Partner's obligation to respond to requests for exercising the Data Subject's rights laid down in Applicable Data Protection Law;
- g. notify (as applicable) and assist Partner in ensuring compliance with data security, Personal Data Breach, data protection impact assessments, and engaging in other consultations, pursuant to Applicable Data Protection Law, taking into account the nature of Processing and the information available to Tencent;
- h. inform Partner if it becomes aware that any of Personal Data is inaccurate or out of date, and cooperate with Partner to erase or rectify the relevant Personal Data;
- i. notify Partner promptly if Tencent makes a determination that it can no longer meet its obligations under Applicable US Data Protection Law;
- j. permit Partner to take reasonable and appropriate steps to help ensure that Tencent uses Personal Data in a manner consistent with Partner's obligations under Applicable US Data Protection Law and to stop and remediate any unauthorized use of Personal Data;
- k. notify Partner promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. Tencent shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. Tencent will provide relevant information about disclosure requests to Partner, including in relation to its legality review and any challenges to the request;
- l. inform Partner if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Module B; and
- m. keep appropriate documentation of the Processing it carries out under this Module B, and make available to Partner (and any relevant Regulator) information sufficient to demonstrate compliance with Applicable Data Protection Law and allow for and contribute to audits, including inspections, conducted by Partner.

## 11. SUB-CONTRACTING

**11.1** Tencent may authorize any sub-processor to Process the Personal Data on its behalf provided that, where (and to the extent) required by Applicable Data Protection Laws, Tencent enters into a written agreement with the sub-processor containing terms which are substantially the same as those contained in this DPA. Partner hereby grants Tencent general written authorisation to engage sub-processors listed at

<https://www.tencentcloud.com/services/thirdParties>. Tencent shall, to the extent required by Applicable Data Protection Laws, inform Partner of any intended changes concerning the addition or replacement of the sub-processors. In such a case, Partner will have fourteen (14) days from the date of receipt of the notice to approve or reject the change. In the event of no response from Partner, the sub-processor will be deemed accepted. If Partner rejects the replacement sub-processor, Tencent may terminate the DPA with immediate effect on written notice to Partner. Tencent shall remain fully responsible to Partner for the performance of any sub-processor's obligations under its contract with the Partner.

## 12. EXPORT OF PERSONAL DATA

**12.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**12.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**12.3** In relation to any onward transfer of the Personal Data by Tencent to another party, Tencent shall comply with the relevant obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E; or (ii) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2.

**12.4** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the

Personal Data by that data importer to another person, the other person shall comply with the same importer obligations.

## MODULE C – TRANSFERS FROM A DATA PROCESSOR TO A DATA CONTROLLER

### 13. APPLICATION OF THIS MODULE C

**13.1** The Parties agree that this Module C applies in each case and only where Personal Data is transferred from Partner (acting as a Data Processor) to Tencent (acting as a Data Controller).

**13.2** The details of the transfers (as well as Personal Data) covered by this Module C are specified in Schedule B which form an integral part of this Module C.

**13.3** In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, clause 15 shall govern the terms of the transfer and clause 14 shall not apply.

### 14. OBLIGATIONS OF PARTNER

**14.1** Partner shall comply with the terms of clause 10 of Module B, and references to “Tencent” shall be read as a reference to “Partner”, and references to “Partner” shall be read as references to “Tencent”, for such purposes, in relation to any such Processing.

**14.2** Before Processing Personal Data, Partner shall implement, and ensure that its authorised personnel comply with, appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as well as ensuring that those measures continue to provide an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing as set out in Schedule C, or otherwise agreed and documented between Tencent and Partner from time to time, and shall continue to comply with them during the term of this DPA. Such measures shall include, as appropriate to the risk:

- a. the pseudonymisation and encryption of Personal Data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.



**14.3** In the event that Partner directly receives a request from a Data Subject regarding Data Subject's Personal Data, or for the rectification or erasure of such Personal Data, or any other request or query from a Data Subject relating to its own Personal Data (including Data Subjects' exercising rights under Applicable Data Protection Laws, such as rights of objection, restriction of processing, data portability or the right not to be subject to automated decision making) (a "**Data Subject Request**"), Partner will:

- a. notify Tencent immediately of the Data Subject Request (without responding to that Data Subject Request, unless it has been otherwise authorised by Tencent to do so);
- b. provide details of the Data Subject Request (and any other relevant information Tencent may reasonably request) to Tencent within 3 business days of receipt of the Data Subject Request; and
- c. provide such assistance to Tencent as Tencent may require for the purposes of responding to the Data Subject Request and to enable Tencent to comply with all obligations which arise as a result thereof.

**14.4** In the event there is, or Partner reasonably believes that there is, any Personal Data Breach in respect of Personal Data which is Processed by Partner under or in connection with this DPA, then upon becoming aware of such Personal Data Breach, Partner shall:

- a. immediately notify Tencent in writing of all known details of the Personal Data Breach relating to the Personal Data, including:
  - i. a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects and records concerned;
  - ii. the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - iii. a description of the likely consequences of the Personal Data Breach; and
  - iv. a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;
- b. provide Tencent with regular status updates on any Personal Data Breach (including actions taken to resolve the incident) and share additional information related to the breach as soon as more details become available;
- c. mitigate any harmful effect that is known to Partner of a use or disclosure of the Personal Data in violation of this DPA or in connection with a Personal Data Breach;
- d. assist Tencent in remediating or mitigating any potential damage from a Personal Data Breach.
- e. within 4 weeks of closure of the incident, provide Tencent a written report describing the Personal Data Breach, the root cause analysis, actions taken by Partner during its response and Partner's plans for future actions to prevent a similar Personal Data Breach from occurring;
- f. not disclose to third parties (including Regulators) any information about a Personal Data Breach involving the Personal Data without prior written and express permission from Tencent for such disclosure; and
- g. assist Tencent with notifying the Personal Data Breach to any Regulator or the Data Subject in accordance with, and in the timeframe required by, the Applicable Data Protection Laws.

**14.5** Partner shall not subcontract to any third party any of its obligations to Process Personal Data under this Module C unless all of the following provisions of this clause have first been complied with:



- a. Partner has supplied to Tencent such information as Tencent may require to ascertain that such subcontractor has the ability to comply with Partner's obligations set out in this DPA and with Tencent's instructions;
- b. Partner has obtained the prior written consent of Tencent; and
- c. the proposed subcontractor has entered into a contract with Partner which requires the subcontractor to take adequate technical and organisational measures to safeguard the security and integrity of the relevant Personal Data and only Process data in accordance with the documented instructions of Tencent (including as set out in such contract with the proposed subcontractor), and which contains obligations on the relevant subcontractor which are no less onerous than the obligations on the Partner in, and which is no less protective of the Personal Data than, the terms of this DPA. The Partner shall provide, at Tencent's request, a copy of such subcontractor contract, and subsequent amendments, to Tencent.

**14.6** In the event that Tencent consents to subcontracting the Processing of Personal Data, Partner remains liable for the Processing under the terms of this DPA. The Partner shall notify Tencent of any failure by a subcontractor to fulfil its obligations under the relevant subcontractor contract.

**14.7** Partner will not, without the consent of Tencent, either:

- a. Process Personal Data in any Third Country; or
- b. permit any third party including its subcontractors to Process Personal Data in any Third Country.

**14.8** Partner shall permit Tencent at any time upon seven (7) days' notice, to be given in writing, to have access to the appropriate part of Partner's premises, systems, equipment, and other materials and data Processing facilities to enable Tencent (or its designated representative) to inspect or audit the same for the purposes of monitoring compliance with Partner's obligations under this DPA. Such inspection shall:

- a. be carried out by Tencent or an inspection body composed of independent members and in possession of the required professional qualifications and bound by a duty of confidentiality, selected by Tencent, where applicable, in agreement with the Regulator; and
- b. not relieve Partner of any of its obligations under this DPA.

## 15. EXPORT OF PERSONAL DATA

**15.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 4 : Processor to Controller set out in Schedule F, which incorporate the provisions of Schedule B, and which together will form contractual terms between Tencent and Partner for that particular transfer of Personal Data.

**15.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**15.3** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure. To the

extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations.

## MISCELLANEOUS (APPLICABLE TO ALL MODULES)

### 16. COOPERATION WITH REGULATORS

**16.1** The Parties agree that they shall and, where applicable, shall procure that their representatives shall cooperate, on request, with any relevant Regulator in the performance of its tasks pursuant to Applicable Data Protection Law.

### 17. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR A REGULATOR

In respect of any action or omission under this DPA:

- a. in the event of a dispute or claim brought by a Data Subject or a Regulator concerning the Processing of Personal Data against Tencent, Partner will inform Tencent about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion;
- b. Partner agrees to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by a Regulator. If they do participate in the proceedings, Partner may elect to do so remotely (such as by telephone or other electronic means); and
- c. each Party shall abide by a decision, as applicable, of a competent court of Tencent's country of establishment; of a competent court of the relevant Data Subject's country of habitual residence; or of the Regulator which is final and against which no further appeal is possible.

## 18. LIABILITY

**18.1** Without prejudice to any other rights or remedies that Tencent may have, Partner hereby acknowledges and agrees that a person with rights under this DPA may be irreparably harmed by any breach of its terms and that damages alone may not be an adequate remedy. Accordingly, a person bringing a claim under this DPA shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this DPA.

**18.2** Partner agrees that it will (in addition to, and without affecting, any other rights or remedies that Tencent may have whether under statute, common law or otherwise) indemnify, defend and hold harmless Tencent, its affiliates, and their respective employees, officers and directors (the “Tencent Parties”), on demand from and against all claims, liabilities, costs, expenses, loss or damage incurred by a Tencent Party (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) arising directly or indirectly from a breach of Applicable Data Protection Law or this DPA by Partner or enforcement of any rights under it.

## 19. TERMINATION

**19.1** Termination of this DPA shall be governed by the applicable provisions in the relevant provisions in the Distributor Agreement.

**19.2** Upon termination of this DPA:

- a. each Party shall, except to the extent it acts as a Data Controller of such Personal Data, at the other Party's option, either forthwith:
  - i. return all of the Personal Data and any copies thereof which it is Processing or has Processed upon behalf of that Party. The return of the Personal Data shall result in the full deletion of the Personal Data existent in the IT equipment and systems used by the Party; or
  - ii. destroy all of the Personal Data and any copies thereof which it has Processed on behalf of that Party promptly and in any case within 14 days of being requested to do so by that Party. The Party shall certify the deletion of such data in writing to the other Party; and
  - iii. cease Processing Personal Data on behalf of the other Party under this DPA.

## 20. MISCELLANEOUS

Applicable clauses in relation to Assignment, Variation, Further Assurance, Invalidity, Waiver and Notices of the applicable Distributor Agreement shall apply *mutatis mutandis* to this DPA.

## 21. ENTIRE AGREEMENT

These terms are the final and complete expression of all agreements between Partner and Tencent regarding Processing of Personal Data and supersede all prior oral and written agreements regarding these matter. In the event of any conflict between this DPA or the Distributor Agreement, this DPA shall prevail to the extent of the inconsistency solely to the extent such inconsistency relates to the Processing of Personal Data or any Applicable Data Protection Law.

## 22. COUNTERPARTS

This DPA may be entered into in any number of counterparts, all of which taken together shall constitute one and the same instrument.

## 23. GOVERNING LAW

**23.1** Subject to clause 24.2, this DPA shall be governed by Singapore law.

**23.2** The law governing Module A (Transfers between Data Controllers), 2 (Transfers from a Data Controller to a Data Processor), in respect of each transfer, be the law of the country in which the Data Discloser is established. The law governing Section 3 (Transfers from a Processor to a Controller) of this DPA shall, in respect of each transfer, be the law of the country in which the Data Receiver is established.

**23.3** Any dispute shall be referred to, and finally resolved by, arbitration administered by the Singapore International Arbitration Centre in accordance with the Arbitration Rules of the Singapore International Arbitration Centre for the time being in force when the notice of arbitration is submitted. The tribunal shall consist of one arbitrator. The seat of arbitration shall be Singapore and the language to be used in the arbitral proceedings shall be English.

## SCHEDULE A: LIST OF PARTIES

### Module A (Transfers between Controllers)

**Data Exporter and Importer(s) - Tencent:**

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Contact: cloudlegalnotices@tencent.com

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor):  
Controller

**Data Exporter and Importer(s) – Partner:**

Name: The relevant entity that entered into the Distributor Agreement with Tencent.

Address: The address provided to Tencent when signing up to act as a distributor of Tencent cloud services. Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Distributor of Tencent Role (controller/processor):  
Controller

## **Module B (Transfers from a Data Controller (Partner) to a Data Processor (Tencent))**

**Data exporter(s) –Partner:**

Name: The relevant Party that entered into the Distributor Agreement with Tencent.

Address: The address provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Partner of Tencent  
Role (controller/processor): Controller

**Data importer(s) –Tencent:**

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Contact: cloudlegalnotices@tencent.com

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor):  
Processor

## **Module C (Transfers from a Data Processor (Partner) to a Data Controller (Tencent))**

**Data exporter(s) –Partner:**

Name: The relevant Party that entered into the Distributor Agreement with Tencent.

Address: The address provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Partner of Tencent Role (controller/processor):  
Processor

**Data importer(s) –Tencent:**

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor):  
Controller

## SCHEDULE B: DESCRIPTION OF TRANSFERS

*Categories of data subjects whose personal data is transferred*

Individuals employed by or representing the Partner

End Users(s), End Customers

Individuals employed by or representing the Second-Level Reseller

Categories of personal data transferred

**Individuals employed by or representing the Partner:** name, job title, mobile phone, email address

**End User(s), End Customer(s):** Name, Email address, address, business registration number (and photo), job title, mobile number, payment details (bank name, account name, bank account, swift code), invoice information (Payer Account ID, Owner Account ID, Operator Account ID), and any other personal data made available by or on behalf of Partner/Partner's End User(s), or otherwise accessible directly or indirectly via the Partner Console.

**Individuals employed by or representing the Second-Level Reseller:** [name, job title, mobile phone, email address]

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

*No sensitive personal data transferred*

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

For the duration of the DPA

*Nature of the processing*

Partner will act as a distributor of Tencent cloud services for certain End Users and to Second-Level Resellers who Resell Tencent cloud services to End Users. Partner shall administer and manage Resell activities relating to its End Users and Second-Level Resellers through the functions and tools provided through Partner Console or via other processes authorized or designated by Tencent and this will involve processing personal data.

*Purpose(s) of the data transfer and further processing*

To facilitate the Reselling of Tencent Services by the Partner, including (without limitation and in each case to the extent the relevant services, features, support or functions are provided):

making available or accessible, directly or indirectly, Personal Data via the Partner Console

provision of integrated / value-added services by the Partner to its customers (if applicable)

customer account creation via email invite sent by Partner on the Tencent Cloud console

placement of orders / Purchase Orders for Tencent Services

fulfilment of orders / Purchase Orders (i.e. performance of Tencent Services)

billing (for Tencent to issue invoices to Partner)

payment by Partner to Tencent

for Tencent to respond to requests for and to provide after-sales customer support

access to online training materials and support from Tencent

access to dedicated online documents and support from Tencent

provision of certification training by Tencent

provision of certification vouchers by Tencent

assigning dedicated solution architect(s) for support

usage of Tencent's Partner Badge by Partner

Partner company listing in Tencent's Partner Directory

Usage of logo featured on Tencent's Partner Portal

participation in Tencent's marketing activities (details subject to Tencent's approval)

joint case study opportunities (details subject to Tencent's agreement)

joint press release development (details subject to Tencent's agreement)

opportunities for co-branding and co-marketing activities

marketing development fund (details subject to Tencent's agreement)

issuing of Premier Partner Award(s)

issuing of Partner voucher benefits (details subject to Tencent's agreement)

joint customer development with Tencent's sales team (details subject to Tencent's agreement)

rebate of order amount

assigning a dedicated partner manager for support

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*



The retention period will follow the data retention policy as set out in the Privacy Policy on the Tencent website.

*For transfer to (sub-)processors, also specify subject matter, nature and duration of the processing*

N/A

*Identify the competent supervisory authority/ies in accordance with Clause 13 of Schedules D, E and F*

The Netherlands

## SCHEDULE C: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Where applicable this Schedule C also forms part of the Standard Contractual Clauses.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. **Data security.** The data importer shall design and implement the following measures to protect customer's data against unauthorized access:

standards for data categorisation and classification;

a set of authentication and access control capabilities at the physical, network, system and application levels; and  
a mechanism for detecting big data-based abnormal behaviour.

2. **Network security.** The data importer shall implement stringent rules on internal network isolation to achieve access control and border protection for internal networks (including office networks, development networks, testing networks and production networks) by way of physical and logical isolation.

3. **Physical and environmental security.** Stringent infrastructure and environment access controls shall be implemented for data centers based on relevant regional security requirements. An access control matrix is established, based on the types of data center personnel and their respective access privileges, to ensure effective management and control of access and operations by data center personnel.

4. **Incident management.** The data importer shall operate active and real-time service monitoring, combined with a rapid response and handling mechanism, that enables prompt detection and handling of security incidents.

5. **Compliance with standards.** The data importer shall comply with the standards listed in Tencent's Compliance Center page, and as updated from time to time.

## SCHEDULE D-1: STANDARD CONTRACTUAL CLAUSES

# MODULE 1: CONTROLLER TO CONTROLLER TRANSFER

## Section I

### Clause 1: Purpose and scope

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- b. The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

### Clause 2: Effect and invariability of the Clauses

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### Clause 3: Third-party beneficiaries

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

- ii. Clause 8 - Clause 8.5 (e) and Clause 8.9(b);
  - iii. Clause 12 - Clause 12(a) and (d);
  - iv. Clause 13;
  - v. Clause 15.1(c), (d) and (e);
  - vi. Clause 16(e);
  - vii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### **Clause 4: Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **Section II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- i. where it has obtained the data subject's prior consent;
- ii. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iii. where necessary in order to protect the vital interests of the data subject or of another natural person.

## 8.2 Transparency

a. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

- i. of its identity and contact details;
- ii. of the categories of personal data processed;
- iii. of the right to obtain a copy of these Clauses;
- iv. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

b. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

c. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

d. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

## 8.3 Accuracy and data minimisation

a. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

b. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

c. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

## 8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

### 8.5 Security of processing

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- b. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- c. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- d. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- e. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- f. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- g. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

### 8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural

person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

### 8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- i. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

### 8.9 Documentation and compliance

- a. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- b. The data importer shall make such documentation available to the competent supervisory authority on request.

### Clause 9: Use of sub-processors Clause 10: Data subject rights

- a. The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her

rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

b. In particular, upon request by the data subject the data importer shall, free of charge:

i. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

ii. rectify inaccurate or incomplete data concerning the data subject;

iii. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

c. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

d. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the law of the country of destination, provided that such law lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

i. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

ii. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

e. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

f. The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

g. If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

## **Clause 11: Redress**



- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**Clause 12: Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

**Clause 13: Supervision**

- a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.



Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### **Clause 14: Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## 15.2 Review of legality and data minimisation

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## Section IV – FINAL PROVISIONS

### Clause 16: Non-compliance with the Clauses and termination

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - ii. the data importer is in substantial or persistent breach of these Clauses; or
  - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data

importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17: Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands (*specify Member State*).

#### **Clause 18: Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of The Netherlands (*specify Member State*).
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

### **APPENDIX TO SCHEDULE D-1 (SCCS MODULE 1)**

#### **ANNEX I**

##### **A. LIST OF PARTIES**

See Schedule A to the DPA

##### **B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA

##### **C. COMPETENT SUPERVISORY AUTHORITY**

See Schedule B to the DPA

#### **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

See Schedule C to the DPA

## **SCHEDULE D-2: INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES**

This Addendum has been issued by the UK Information Commissioner's Office for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## PART 1: TABLES

TABLE 1: PARTIES

Start date	See effective date of the DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	See Schedule A of the DPA	
Key Contact	See Schedule A of the DPA	

TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

AddendumEU SCCs	The Approved EU SCCs, including the Appendix Information, set out in Schedule D-1, Schedule E or Schedule F to the DPA, as applicable
-----------------	---

TABLE 3: APPENDIX INFORMATION

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

	Annex 1A: List of Parties: <b>See Schedule A to the DPA</b>
--	---

Annex 1B: Description of Transfer: <b>See Schedule B to the DPA</b>
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: <b>See Schedule C to the DPA</b>
Annex III: List of Sub processors (Modules 2 and 3 only): <b>N/A</b>

TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Neither Party
---	---

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

<b>Addendum</b>	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
<b>Addendum EU SCCs</b>	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
<b>Appendix Information</b>	As set out in Table 3.
<b>Appropriate Safeguards</b>	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
<b>Approved Addendum</b>	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022.
<b>Approved EU SCCs</b>	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
<b>ICO</b>	The Information Commissioner.
<b>Restricted Transfer</b>	A transfer which is covered by Chapter V of the UK GDPR.
<b>UK</b>	The United Kingdom of Great Britain and Northern Ireland.
<b>UK Data Protection Laws</b>	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
<b>UK GDPR</b>	As defined in section 3 of the Data Protection Act 2018.

4.This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5.If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6.If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7.If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8.ny references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

#### **Hierarchy**

9..Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10.Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11.Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

#### **Incorporation of and changes to the EU SCCs**

12.This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13.Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14.No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.



15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
- a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
  - b. In Clause 2, delete the words:  
“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;
  - c. Clause 6 (Description of the transfer(s)) is replaced with:  
“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
  - d. Clause 8.7(i) of Module A is replaced with:  
“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
  - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:  
“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
  - f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
  - g. References to Regulation (EU) 2018/1725 are removed;
  - h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
  - i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
  - j. Clause 13(a) and Part C of Annex I are not used;
  - k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
  - l. In Clause 16(e), subsection (i) is replaced with:  
“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
  - m. Clause 17 is replaced with:  
“These Clauses are governed by the laws of England and Wales.”;
  - n. Clause 18 is replaced with:  
“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
  - o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.



#### Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a. its direct costs of performing its obligations under the Addendum; and/or
- b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

## SCHEDULE E: STANDARD CONTRACTUAL CLAUSES

### MODULE 2: CONTROLLER TO PROCESSOR TRANSFER

#### Section I

##### Clause 1: Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

- i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
  - d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## **Clause 2: Effect and invariability of the Clauses**

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

## **Clause 3: Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - iii. Clause 9 - Clause 9(a), (c), (d) and (e);
  - iv. Clause 12 - Clause 12(a), (d) and (f);
  - v. Clause 13;
  - vi. Clause 15.1(c), (d) and (e);
  - vii. Clause 16(e);
  - viii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

## **Clause 4: Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **Section II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Instructions**

- a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

##### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

##### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may

redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised

to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

- a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

#### **Clause 9: Use of sub-processors**

- a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least twenty business days' in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### **Clause 10: Data subject rights**

- a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **Clause 11: Redress**

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### **Clause 12: Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.



- d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13: Supervision**

a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

### **Clause 14: Local laws and practices affecting compliance with the Clauses**

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a



democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

- i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
- ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **15.2 Review of legality and data minimisation**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **Section IV – FINAL PROVISIONS**

##### **Clause 16: Non-compliance with the Clauses and termination**

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17: Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands.

#### **Clause 18: Choice of forum and jurisdiction**

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of The Netherlands (specify Member State).

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

## APPENDIX TO SCHEDULE E (SCCS MODULE B)

### ANNEX I

#### A. LIST OF PARTIES

See Schedule A to the DPA

#### B. DESCRIPTION OF TRANSFER

See Schedule B to the DPA

#### C. COMPETENT SUPERVISORY AUTHORITY

See Schedule B to the DPA

### ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Schedule C to the DPA

## SCHEDULE F: STANDARD CONTRACTUAL CLAUSES

## MODULE 4: PROCESSOR TO CONTROLLER TRANSFER

### Section I

#### Clause 1: Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

- i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### Clause 2: Effect and invariability of the Clauses

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### **Clause 3: Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8 - Clause 8.1 (b) and Clause 8.3(b);
  - iii. Clause 15.1(c), (d) and (e);
  - iv. Clause 16(e);
  - v. Clause 18.
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### **Clause 4: Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **Section II – OBLIGATIONS OF THE PARTIES**

### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### **8.1 Instructions**

- a. The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- b. The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- c. The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- d. After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

#### **8.2 Security of processing**

- a. The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- b. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- c. The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

#### **8.3 Documentation and compliance**

- a. The Parties shall be able to demonstrate compliance with these Clauses.
- b. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

**Clause 9: Use of sub-processors Clause 10: Data subject rights**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

**Clause 11: Redress**

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

**Clause 12: Liability**

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

**Clause 13: Supervision****Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES****Clause 14: Local laws and practices affecting compliance with the Clauses**

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;



- ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
- iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.



- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **Section IV – FINAL PROVISIONS**

### **Clause 16: Non-compliance with the Clauses and termination**

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- ii. the data importer is in substantial or persistent breach of these Clauses; or
- iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17: Governing law**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands (*specify country*).

#### **Clause 18: Choice of forum and jurisdiction**

Any dispute arising from these Clauses shall be resolved by the courts of The Netherlands (*specify country*).

### **APPENDIX TO SCHEDULE F (SCCS MODULE 4)**

#### **ANNEX I**

##### **A. LIST OF PARTIES**

See Schedule A to the DPA

##### **B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA

If you have (a) registered as a Partner under the Tencent Cloud Distributor Agreement and (b) entered into a distributor arrangement (whether or not involving integration services) with us under a Distributor Agreement, this

Data Processing Agreement (“**DPA**”) applies to any processing of Personal Data in connection with such Distributor Agreement. In the event of any conflict between this DPA, the Distributor Agreement, Console Documentation and Purchase Order, this DPA shall prevail to the extent of the inconsistency. References to “Partner” and “Tencent” in this DPA have the same meaning as set out in the Distributor Agreement.

**Now it is hereby agreed** as follows:

## 1. Definitions

**1.1** Capitalised terms shall have the meaning given to them in the Distributor Agreement, unless otherwise defined below:

“**Personal Data**”, “**Special Categories of Data/Sensitive Data**”, “**Process/Processing**”, “**Controller**”, “**Processor**”, and “**Data Subject**” shall have the same meaning as in the relevant Applicable Data Protection Laws. “**Applicable Data Protection Law**” shall mean:

- a. the General Data Protection Regulation 2016/679 (the “**GDPR**”);
- b. the Privacy and Electronic Communications Directive 2002/58/EC;
- c. the UK Data Protection Act 2018 (“**DPA**”), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (“**UK GDPR**”), and the Privacy and Electronic Communications Regulations 2003;
- d. the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq. as amended by the California Privacy Rights Act of 2020, Cal. Civil Code § 1798.100 et seq. (collectively, “**CCPA**”), the Virginia Consumer Data Protection Act (“**VCDPA**”), the Colorado Privacy Act (“**CPA**”), Connecticut Data Privacy Act (“**CDPA**”), Utah Consumer Privacy Act (“**UCPA**”), Iowa Consumer Data Protection Act (“**ICDPA**”), Indiana Consumer Data Protection Act (“**INCDPA**”), Montana Consumer Data Privacy Act (“**MCDPA**”), Tennessee Information Protection Act (“**TIPA**”), Texas Data Privacy and Security Act (“**TDPSA**”), Oregon Consumer Privacy Act (“**OCPA**”), Florida Digital Bill of Rights (“**FDBR**”) (collectively, “**Applicable US Data Protection Law**”); and
- e. any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

“**Data Discloser**” means the Party who transfers Personal Data to the other Party.

“**Data Receiver**” means the Party who receives Personal Data from the Data Discloser for Processing in accordance with the terms of this Agreement.

“**Distributor Agreement**” means the Tencent Cloud Distributor Agreement in place between Tencent and the Partner.

“**Lawful Export Measure**” means a method allowing for the lawful transfer of Personal Data from a data exporter to a data importer, as may be stipulated by Applicable Data Protection Law or a Regulator from time to time, which may include (depending upon the Applicable Data Protection Laws) model transfer terms prescribed by Applicable Data Protection Laws; or prior registration, licensing or permission from a Regulator.

“**Party**” means a party to this DPA.

“**Partner Console**” means the area designated as console in the Tencent Cloud portal at

<http://www.tencentcloud.com>.

“**Personal Data Breach**” means any improper, unauthorised or unlawful access to, use of, or disclosure of, or any other compromise which affects the availability, integrity or confidentiality of Personal Data.

“**Member State**” means the member states of the European Union from time to time.

“**Regulator**” means the data protection supervisory authority which has jurisdiction over a Party's Processing of Personal Data.

“**Relevant Data Export**” means:

a. a transfer of Personal Data:

- i. from a Party which is subject to Applicable Data Protection Law in respect of that Personal Data;
- ii. to another Party that is in a Third Country or a territory which otherwise (but for the operation of this DPA) does not offer an adequate level of protection as required by Applicable Data Protection Law; and
- iii. which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law; and

b. the onward transfer of Personal Data pursuant to (a) to a Third Country or a territory which otherwise (but for the operation of this DPA) does not offer an adequate level of protection as required by Applicable Data Protection Law and which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law.

“**Security Standards**” shall mean the technical and organisational security measures set out in Schedule C.

“**Standard Contractual Clauses**” means:

- a. in the case of transfers of Personal Data relating to Data Subjects in the European Economic Area (“**EEA**”), the standard contractual clauses for the transfer of Personal Data to data processors established in third countries set out in the Commission Decision of 4 June 2021 (C(2021) 3972), as amended and restated from time to time;
- b. in relation to transfers of Personal Data from the UK, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, and in each case as amended, updated or replaced from time to time, as attached to and incorporated into this DPA to cover Personal Data transfers to Controllers or Processors as applicable established in Third Countries which do not ensure an adequate level of data protection; and
- c. in each case, as amended, updated or replaced from time to time, as attached to and incorporated into this DPA to cover Personal Data transfers to Controllers or Processors, as applicable, established in Third Countries which do not ensure an adequate level of data protection.

“**Third Country**” means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time; and (iii) in relation to Personal Data transfers from any other jurisdiction, any country other than those approved as providing adequate protection for Personal Data by the relevant competent authority of such country from time to time.

- 1.2 References to a statutory provision include any subordinate legislation made from time to time under that provision.
- 1.3 References to this DPA include the Schedules.
- 1.4 Headings shall be ignored in construing this DPA.
- 1.5 If a word or phrase is defined, its other grammatical forms have a corresponding meaning.
- 1.6 The words “include”, “includes” and “including”, and any succeeding words shall be construed without limitation to the generality of any preceding words or concepts.
- 1.7 If there is any inconsistency between the Clauses and Schedules to this DPA the Clauses shall take precedence.

## SCOPE OF THIS AGREEMENT

### 2. General

- 2.1 This DPA governs the transfer of Personal Data between Tencent and Partner. This DPA is divided into the following sections:
- a. Module A (Transfers between Controllers) sets forth the terms governing any transfer (including a Relevant Data Export) between the Parties, each acting as an independent Data Controller;
  - b. Module B (Transfers from a Data Controller to a Data Processor) sets forth the terms governing any transfer (including a Relevant Data Export) from Partner (acting as a Data Controller) to Tencent (acting as a Data Processor); and
  - c. Module C (Transfers from a Data Processor to a Data Controller) sets forth the terms governing any transfer (including a Relevant Data Export) from Partner (acting as a Data Processor) to Tencent (acting as a Data Controller).

## MODULE A – TRANSFERS BETWEEN DATA CONTROLLERS

### 3. APPLICATION OF THIS MODULE A

- 3.1 The Parties agree that this Module A applies in each case and only where Personal Data is transferred from Data Discloser to Data Receiver, in circumstances where each Party is acting as an independent Data Controller.
- 3.2 The details of the transfers covered by this Module A are specified in Schedule B which forms an integral part of this Module A.

**3.3** In the case of a Relevant Data Export to a Third Country, clause 7 shall govern the terms of the transfer and clauses 4, 5 and 6 shall not apply.

## 4. OBLIGATIONS OF BOTH PARTIES

**4.1** Each Party shall:

- a. Process Personal Data fairly and lawfully;
- b. ensure that Personal Data is accurate and up to date, and inform the other without undue delay if it becomes aware that any of the Personal Data is inaccurate or out of date;
- c. provide reasonable assistance as necessary to the other to enable them to comply with subject access requests and to respond to any other queries or complaints from Data Subjects;
- d. carry out any reasonable request from the other to amend, transfer or delete any Personal Data (to the extent applicable); and
- e. notify the other promptly about any enquiries from a Regulator in relation to Personal Data and cooperate promptly and thoroughly with such Regulator, to the extent required under Applicable Data Protection Law.

## 5. OBLIGATIONS OF DATA DISCLOSER

**5.1** The Data Discloser warrants and undertakes that:

- a. Personal Data have been collected, Processed, and transferred in accordance with Applicable Data Protection Laws, as applicable to the Data Discloser;
- b. it has obtained all consents, authorizations, approvals and rights and provided all notices necessary, including as required by Applicable Data Protection Law, to provide the Personal Data to the Data Receiver and permit the Data Receiver to use the Personal Data in accordance with this DPA;
- c. it has used reasonable efforts to determine that the Data Receiver is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Module A;
- d. it has taken all steps required by Applicable Data Protection Law to avoid “selling” Personal Data to Data Receiver under this Module A (as defined in such laws), including transferring Personal Data at the direction of the relevant individual, or otherwise taken all steps required to comply with obligations relating to “selling” under such Applicable Data Protection Law; and
- e. the Data Discloser shall provide a copy of this Module A and associated Schedules to the Regulator where required.

## 6. OBLIGATIONS OF DATA RECEIVER

**6.1** Data Receiver warrants and undertakes that:

- a. it will comply with all relevant obligations of Applicable Data Protection Law, including by providing the same level of privacy protections required of controllers and businesses by Applicable Data Protection Law;
- b. it will have in place appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the data to be protected including those in the Security Standards, and shall ensure that those measures continue to provide an appropriate level of security;
- c. in the event of a Personal Data Breach, it shall take appropriate measures to address the Personal Data Breach, and shall (if the breach is likely to result in a risk to individuals) notify the Data Discloser and cooperate with the Data Discloser in relation to any required notifications to the Regulator and/ or to relevant Data Subjects.
- d. it will have in place procedures so that any third party it authorises to have access to Personal Data, including Data Processors, will respect and maintain the confidentiality and security of Personal Data. Any person acting under the authority of the Data Receiver, including a Data Processor, shall be obligated to Process Personal Data only on instructions from the Data Receiver. This provision does not apply to persons authorised or required by law or regulation to have access to Personal Data;
- e. it shall notify the Data Receiver promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The Data Receiver shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. The Data Receiver will provide relevant information about disclosure requests to the Data Discloser, including in relation to its legality review and any challenges to the request;
- f. it will inform the Data Discloser if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Module A;
- g. it will Process Personal Data for purposes described in Schedule B (*Description of Transfer*), and has the legal authority to give the warranties and fulfil the undertakings set out in this Module A;
- h. it shall put in place appropriate technical or organisational measures in order to retain Personal Data for no longer than necessary for the purposes for which it is processed; and
- i. it will keep appropriate documentation of the Processing it carries out under this Module A, and shall make such documentation available to the relevant Regulator(s).

## 7. EXPORT OF PERSONAL DATA

**7.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 1: Controller to Controller, set out in Schedule D-1, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser, who shall comply with the data exporter's obligations set out in Schedule D-1, and the



applicable Data Receiver, who shall comply with the data importer's obligations set out in Schedule D-1, for that particular transfer of Personal Data for that particular transfer of Personal Data. In relation to any onward transfer of such Personal Data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 1: Controller to Controller set out in Schedule D-1; or (ii) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E, in respect of that Personal Data.

**7.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser. In relation to any onward transfer of such Personal Data by the Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the obligations set out in the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses set out in Schedule D-2, in respect of that Personal Data.

**7.3** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure,. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply mutatis mutandis for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another data importer, the receiving data importer shall comply with the same data importer obligations.

## MODULE B – TRANSFERS FROM DATA CONTROLLER TO DATA PROCESSOR

### 8. APPLICATION OF THIS MODULE B

**8.1** The Parties agree that this Module B applies in each case and only where Personal Data is transferred from Partner (acting as a Data Controller) to Tencent (acting as a Data Processor).

**8.2** The details of the transfers (as well as the Personal Data) covered by this Module B are specified in Schedule B which form an integral part of this Module B.



**8.3** In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, as relevant, clause 12 shall govern the terms of the transfer and clauses 9, 10 and 11 shall not apply.

**8.4** Nothing in this DPA shall relieve Partner or Tencent of liabilities imposed by virtue of their roles in the Processing relationship.

## 9. OBLIGATIONS OF DISTRIBUTOR

**9.1** Partner agrees and warrants that:

- a. it has used reasonable efforts to determine that Tencent is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Module B;
- b. it has obtained all consents, authorizations, approvals and rights and provided all notices necessary, including as required by Applicable US Data Protection Law, to provide the Personal Data to Tencent and permit Tencent to use the Personal Data in accordance with this DPA;
- c. it has disclosed the Personal Data to Tencent for the limited purposes set forth in Schedule B; and
- d. the Processing, including the transfer itself, of Personal Data has been and will continue to be carried out in accordance with the relevant provisions of Applicable Data Protection Law (and, where applicable, has been notified to the relevant authorities of the country in which Partner is established).

**9.2** Partner warrants that it has no reason to believe that any applicable local laws, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent Tencent from fulfilling its obligations under this Module B.

## 10. OBLIGATIONS OF TENCENT

**10.1** Tencent agrees and warrants that it will:

- a. Process Personal Data only on documented instructions of Partner and this DPA for the limited purposes set forth in Schedule B and in compliance with Applicable US Data Protection Law;
- b. not retain, use or disclose Personal Data (i) outside of the direct business relationship between Partner and Tencent or as otherwise permitted by Applicable Data Protection Law, or (ii) for any purpose other than for the limited purposes set forth in Schedule B;
- c. not combine Personal Data received from or on behalf of Partner with any Personal Data that may be collected from Tencent's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Applicable Data Protection Law;
- d. ensure that persons authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- e. take all technical and organisational security measures required by Applicable Data Protection Law relating to data security, and shall ensure that those measures continue to provide an appropriate level of security;

- f. taking into account the nature of the Processing, assist Partner by implementing appropriate technical and organisational measures, insofar as this is practicable, for the fulfilment of Partner's obligation to respond to requests for exercising the Data Subject's rights laid down in Applicable Data Protection Law;
- g. notify (as applicable) and assist Partner in ensuring compliance with data security, Personal Data Breach, data protection impact assessments, and engaging in other consultations, pursuant to Applicable Data Protection Law, taking into account the nature of Processing and the information available to Tencent;
- h. inform Partner if it becomes aware that any of Personal Data is inaccurate or out of date, and cooperate with Partner to erase or rectify the relevant Personal Data;
- i. notify Partner promptly if Tencent makes a determination that it can no longer meet its obligations under Applicable US Data Protection Law;
- j. permit Partner to take reasonable and appropriate steps to help ensure that Tencent uses Personal Data in a manner consistent with Partner's obligations under Applicable US Data Protection Law and to stop and remediate any unauthorized use of Personal Data;
- k. notify Partner promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. Tencent shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. Tencent will provide relevant information about disclosure requests to Partner, including in relation to its legality review and any challenges to the request;
- l. inform Partner if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Module B; and
- m. keep appropriate documentation of the Processing it carries out under this Module B, and make available to Partner (and any relevant Regulator) information sufficient to demonstrate compliance with Applicable Data Protection Law and allow for and contribute to audits, including inspections, conducted by Partner.

## 11. SUB-CONTRACTING

**11.1** Tencent may authorize any sub-processor to Process the Personal Data on its behalf provided that, where (and to the extent) required by Applicable Data Protection Laws, Tencent enters into a written agreement with the sub-processor containing terms which are substantially the same as those contained in this DPA. Partner hereby grants Tencent general written authorisation to engage sub-processors listed at <https://www.tencentcloud.com/services/thirdParties>. Tencent shall, to the extent required by Applicable Data Protection Laws, inform Partner of any intended changes concerning the addition or replacement of the sub-processors. In such a case, Partner will have fourteen (14) days from the date of receipt of the notice to approve or reject the change. In the event of no response from Partner, the sub-processor will be deemed accepted. If Partner rejects the replacement sub-processor, Tencent may terminate the DPA with immediate effect on written notice to

Partner. Tencent shall remain fully responsible to Partner for the performance of any sub-processor's obligations under its contract with the Partner.

## 12. EXPORT OF PERSONAL DATA

**12.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**12.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**12.3** In relation to any onward transfer of the Personal Data by Tencent to another party, Tencent shall comply with the relevant obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E; or (ii) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2.

**12.4** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations.

## MODULE C – TRANSFERS FROM A DATA PROCESSOR TO A DATA CONTROLLER

### 13. APPLICATION OF THIS MODULE C

**13.1** The Parties agree that this Module C applies in each case and only where Personal Data is transferred from Partner (acting as a Data Processor) to Tencent (acting as a Data Controller).

**13.2** The details of the transfers (as well as Personal Data) covered by this Module C are specified in Schedule B which form an integral part of this Module C.

**13.3** In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, clause 15 shall govern the terms of the transfer and clause 14 shall not apply.

## 14. OBLIGATIONS OF PARTNER

**14.1** Partner shall comply with the terms of clause 10 of Module B, and references to “Tencent” shall be read as a reference to “Partner”, and references to “Partner” shall be read as references to “Tencent”, for such purposes, in relation to any such Processing.

**14.2** Before Processing Personal Data, Partner shall implement, and ensure that its authorised personnel comply with, appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as well as ensuring that those measures continue to provide an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing as set out in Schedule C, or otherwise agreed and documented between Tencent and Partner from time to time, and shall continue to comply with them during the term of this DPA. Such measures shall include, as appropriate to the risk:

- a. the pseudonymisation and encryption of Personal Data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

**14.3** In the event that Partner directly receives a request from a Data Subject regarding Data Subject's Personal Data, or for the rectification or erasure of such Personal Data, or any other request or query from a Data Subject relating to its own Personal Data (including Data Subjects' exercising rights under Applicable Data Protection Laws, such as rights of objection, restriction of processing, data portability or the right not to be subject to automated decision making) (a “**Data Subject Request**”), Partner will:

- a. notify Tencent immediately of the Data Subject Request (without responding to that Data Subject Request, unless it has been otherwise authorised by Tencent to do so);
- b. provide details of the Data Subject Request (and any other relevant information Tencent may reasonably request) to Tencent within 3 business days of receipt of the Data Subject Request; and
- c. provide such assistance to Tencent as Tencent may require for the purposes of responding to the Data Subject Request and to enable Tencent to comply with all obligations which arise as a result thereof.

**14.4** In the event there is, or Partner reasonably believes that there is, any Personal Data Breach in respect of Personal Data which is Processed by Partner under or in connection with this DPA, then upon becoming aware of such Personal Data Breach, Partner shall:

- a. immediately notify Tencent in writing of all known details of the Personal Data Breach relating to the Personal Data, including:
  - i. a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects and records concerned;
  - ii. the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - iii. a description of the likely consequences of the Personal Data Breach; and
  - iv. a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;
- b. provide Tencent with regular status updates on any Personal Data Breach (including actions taken to resolve the incident) and share additional information related to the breach as soon as more details become available;
- c. mitigate any harmful effect that is known to Partner of a use or disclosure of the Personal Data in violation of this DPA or in connection with a Personal Data Breach;
- d. assist Tencent in remediating or mitigating any potential damage from a Personal Data Breach.
- e. within 4 weeks of closure of the incident, provide Tencent a written report describing the Personal Data Breach, the root cause analysis, actions taken by Partner during its response and Partner's plans for future actions to prevent a similar Personal Data Breach from occurring;
- f. not disclose to third parties (including Regulators) any information about a Personal Data Breach involving the Personal Data without prior written and express permission from Tencent for such disclosure; and
- g. assist Tencent with notifying the Personal Data Breach to any Regulator or the Data Subject in accordance with, and in the timeframe required by, the Applicable Data Protection Laws.

**14.5** Partner shall not subcontract to any third party any of its obligations to Process Personal Data under this Module C unless all of the following provisions of this clause have first been complied with:

- a. Partner has supplied to Tencent such information as Tencent may require to ascertain that such subcontractor has the ability to comply with Partner's obligations set out in this DPA and with Tencent's instructions;
- b. Partner has obtained the prior written consent of Tencent; and
- c. the proposed subcontractor has entered into a contract with Partner which requires the subcontractor to take adequate technical and organisational measures to safeguard the security and integrity of the relevant Personal Data and only Process data in accordance with the documented instructions of Tencent (including as set out in such contract with the proposed subcontractor), and which contains obligations on the relevant subcontractor which are no less onerous than the obligations on the Partner in, and which is no less protective of the Personal Data than, the terms of this DPA. The Partner shall provide, at Tencent's request, a copy of such subcontractor contract, and subsequent amendments, to Tencent.

**14.6** In the event that Tencent consents to subcontracting the Processing of Personal Data, Partner remains liable for the Processing under the terms of this DPA. The Partner shall notify Tencent of any failure by a subcontractor to fulfil

its obligations under the relevant subcontractor contract.

**14.7** Partner will not, without the consent of Tencent, either:

- a. Process Personal Data in any Third Country; or
- b. permit any third party including its subcontractors to Process Personal Data in any Third Country.

**14.8** Partner shall permit Tencent at any time upon seven (7) days' notice, to be given in writing, to have access to the appropriate part of Partner's premises, systems, equipment, and other materials and data Processing facilities to enable Tencent (or its designated representative) to inspect or audit the same for the purposes of monitoring compliance with Partner's obligations under this DPA. Such inspection shall:

- a. be carried out by Tencent or an inspection body composed of independent members and in possession of the required professional qualifications and bound by a duty of confidentiality, selected by Tencent, where applicable, in agreement with the Regulator; and
- b. not relieve Partner of any of its obligations under this DPA.

## 15. EXPORT OF PERSONAL DATA

**15.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 4 : Processor to Controller set out in Schedule F, which incorporate the provisions of Schedule B, and which together will form contractual terms between Tencent and Partner for that particular transfer of Personal Data.

**15.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**15.3** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations.

# MISCELLANEOUS (APPLICABLE TO ALL MODULES)

## 16. COOPERATION WITH REGULATORS

**16.1** The Parties agree that they shall and, where applicable, shall procure that their representatives shall cooperate, on request, with any relevant Regulator in the performance of its tasks pursuant to Applicable Data Protection Law.

## 17. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR A REGULATOR

In respect of any action or omission under this DPA:

- a. in the event of a dispute or claim brought by a Data Subject or a Regulator concerning the Processing of Personal Data against Tencent, Partner will inform Tencent about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion;
- b. Partner agrees to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by a Regulator. If they do participate in the proceedings, Partner may elect to do so remotely (such as by telephone or other electronic means); and
- c. each Party shall abide by a decision, as applicable, of a competent court of Tencent's country of establishment; of a competent court of the relevant Data Subject's country of habitual residence; or of the Regulator which is final and against which no further appeal is possible.

## 18. LIABILITY

**18.1** Without prejudice to any other rights or remedies that Tencent may have, Partner hereby acknowledges and agrees that a person with rights under this DPA may be irreparably harmed by any breach of its terms and that damages alone may not be an adequate remedy. Accordingly, a person bringing a claim under this DPA shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this DPA.

**18.2** Partner agrees that it will (in addition to, and without affecting, any other rights or remedies that Tencent may have whether under statute, common law or otherwise) indemnify, defend and hold harmless Tencent, its affiliates,



and their respective employees, officers and directors (the “Tencent Parties”), on demand from and against all claims, liabilities, costs, expenses, loss or damage incurred by a Tencent Party (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) arising directly or indirectly from a breach of Applicable Data Protection Law or this DPA by Partner or enforcement of any rights under it.

## 19. TERMINATION

**19.1** Termination of this DPA shall be governed by the applicable provisions in the relevant provisions in the Distributor Agreement.

**19.2** Upon termination of this DPA:

- a. each Party shall, except to the extent it acts as a Data Controller of such Personal Data, at the other Party’s option, either forthwith:
  - i. return all of the Personal Data and any copies thereof which it is Processing or has Processed upon behalf of that Party. The return of the Personal Data shall result in the full deletion of the Personal Data existent in the IT equipment and systems used by the Party; or
  - ii. destroy all of the Personal Data and any copies thereof which it has Processed on behalf of that Party promptly and in any case within 14 days of being requested to do so by that Party. The Party shall certify the deletion of such data in writing to the other Party; and
  - iii. cease Processing Personal Data on behalf of the other Party under this DPA.

## 20. MISCELLANEOUS

Applicable clauses in relation to Assignment, Variation, Further Assurance, Invalidity, Waiver and Notices of the applicable Distributor Agreement shall apply *mutatis mutandis* to this DPA.

## 21. ENTIRE AGREEMENT

These terms are the final and complete expression of all agreements between Partner and Tencent regarding Processing of Personal Data and supersede all prior oral and written agreements regarding these matter. In the event of any conflict between this DPA or the Distributor Agreement, this DPA shall prevail to the extent of the inconsistency solely to the extent such inconsistency relates to the Processing of Personal Data or any Applicable Data Protection Law.

## 22. COUNTERPARTS



This DPA may be entered into in any number of counterparts, all of which taken together shall constitute one and the same instrument.

## 23. GOVERNING LAW

**23.1** Subject to clause 24.2, this DPA shall be governed by Singapore law.

**23.2** The law governing Module A (Transfers between Data Controllers), 2 (Transfers from a Data Controller to a Data Processor), in respect of each transfer, be the law of the country in which the Data Discloser is established. The law governing Section 3 (Transfers from a Processor to a Controller) of this DPA shall, in respect of each transfer, be the law of the country in which the Data Receiver is established.

**23.3** Any dispute shall be referred to, and finally resolved by, arbitration administered by the Singapore International Arbitration Centre in accordance with the Arbitration Rules of the Singapore International Arbitration Centre for the time being in force when the notice of arbitration is submitted. The tribunal shall consist of one arbitrator. The seat of arbitration shall be Singapore and the language to be used in the arbitral proceedings shall be English.

## SCHEDULE A: LIST OF PARTIES

### Module A (Transfers between Controllers)

#### Data Exporter and Importer(s) - Tencent:

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Contact: cloudlegalnotices@tencent.com

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor):  
Controller

#### Data Exporter and Importer(s) – Partner:

Name: The relevant entity that entered into the Distributor Agreement with Tencent.

Address: The address provided to Tencent when signing up to act as a distributor of Tencent cloud services. Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Distributor of Tencent Role (controller/processor):  
Controller

## Module B (Transfers from a Data Controller (Partner) to a Data Processor (Tencent))

### Data exporter(s) –Partner:

Name: The relevant Party that entered into the Distributor Agreement with Tencent.

Address: The address provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Partner of Tencent

Role (controller/processor): Controller

### Data importer(s) –Tencent:

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Contact: cloudlegalnotices@tencent.com

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor):  
Processor

## Module C (Transfers from a Data Processor (Partner) to a Data Controller (Tencent))

### Data exporter(s) –Partner:

Name: The relevant Party that entered into the Distributor Agreement with Tencent.

Address: The address provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a distributor of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Partner of Tencent Role (controller/processor):

Processor

### Data importer(s) –Tencent:

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor):  
Controller

## SCHEDULE B: DESCRIPTION OF TRANSFERS

*Categories of data subjects whose personal data is transferred*

Individuals employed by or representing the Partner

End Users(s), End Customers

Individuals employed by or representing the Second-Level Reseller

Categories of personal data transferred

**Individuals employed by or representing the Partner:** name, job title, mobile phone, email address

**End User(s), End Customer(s):** Name, Email address, address, business registration number (and photo), job title, mobile number, payment details (bank name, account name, bank account, swift code), invoice information (Payer Account ID, Owner Account ID, Operator Account ID), and any other personal data made available by or on behalf of Partner/Partner's End User(s), or otherwise accessible directly or indirectly via the Partner Console.

**Individuals employed by or representing the Second-Level Reseller:** [name, job title, mobile phone, email address]

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strictpurpose limitation, accessrestrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

*No sensitive personal data transferred*

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

For the duration of the DPA

---

*Nature of the processing*

Partner will act as a distributor of Tencent cloud services for certain End Users and to Second-Level Resellers who Resell Tencent cloud services to End Users. Partner shall administer and manage Resell activities relating to its End Users and Second-Level Resellers through the functions and tools provided through Partner Console or via other processes authorized or designated by Tencent and this will involve processing personal data.

*Purpose(s) of the data transfer and further processing*

To facilitate the Reselling of Tencent Services by the Partner, including (without limitation and in each case to the extent the relevant services, features, support or functions are provided):

making available or accessible, directly or indirectly, Personal Data via the Partner Console

provision of integrated / value-added services by the Partner to its customers (if applicable)

customer account creation via email invite sent by Partner on the Tencent Cloud console

placement of orders / Purchase Orders for Tencent Services

fulfilment of orders / Purchase Orders (i.e. performance of Tencent Services)

billing (for Tencent to issue invoices to Partner)

payment by Partner to Tencent

for Tencent to respond to requests for and to provide after-sales customer support

access to online training materials and support from Tencent

access to dedicated online documents and support from Tencent

provision of certification training by Tencent

provision of certification vouchers by Tencent

assigning dedicated solution architect(s) for support

usage of Tencent's Partner Badge by Partner

Partner company listing in Tencent's Partner Directory

Usage of logo featured on Tencent's Partner Portal

participation in Tencent's marketing activities (details subject to Tencent's approval)

joint case study opportunities (details subject to Tencent's agreement)

joint press release development (details subject to Tencent's agreement)

opportunities for co-branding and co-marketing activities

marketing development fund (details subject to Tencent's agreement)

issuing of Premier Partner Award(s)

issuing of Partner voucher benefits (details subject to Tencent's agreement)

joint customer development with Tencent's sales team (details subject to Tencent's agreement)

rebate of order amount

assigning a dedicated partner manager for support

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

The retention period will follow the data retention policy as set out in the Privacy Policy on the Tencent website.

*For transfer to (sub-)processors, also specify subject matter, nature and duration of the processing*

N/A

*Identify the competent supervisory authority/ies in accordance with Clause 13 of Schedules D, E and F*

The Netherlands

## SCHEDULE C: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Where applicable this Schedule C also forms part of the Standard Contractual Clauses.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. **Data security.** The data importer shall design and implement the following measures to protect customer's data against unauthorized access:

standards for data categorisation and classification;

a set of authentication and access control capabilities at the physical, network, system and application levels; and  
a mechanism for detecting big data-based abnormal behaviour.

2. **Network security.** The data importer shall implement stringent rules on internal network isolation to achieve access control and border protection for internal networks (including office networks, development networks, testing networks and production networks) by way of physical and logical isolation.

3. **Physical and environmental security.** Stringent infrastructure and environment access controls shall be implemented for data centers based on relevant regional security requirements. An access control matrix is established, based on the types of data center personnel and their respective access privileges, to ensure effective management and control of access and operations by data center personnel.

4. **Incident management.** The data importer shall operate active and real-time service monitoring, combined with a rapid response and handling mechanism, that enables prompt detection and handling of security incidents.

5. **Compliance with standards.** The data importer shall comply with the standards listed in Tencent's Compliance Center page, and as updated from time to time.

## SCHEDULE D-1: STANDARD CONTRACTUAL CLAUSES

## MODULE 1: CONTROLLER TO CONTROLLER TRANSFER

### Section I

#### Clause 1: Purpose and scope

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- b. The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## **Clause 2: Effect and invariability of the Clauses**

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

## **Clause 3: Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8 - Clause 8.5 (e) and Clause 8.9(b);
  - iii. Clause 12 - Clause 12(a) and (d);
  - iv. Clause 13;
  - v. Clause 15.1(c), (d) and (e);
  - vi. Clause 16(e);
  - vii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

## **Clause 4: Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **Section II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- i. where it has obtained the data subject's prior consent;
- ii. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iii. where necessary in order to protect the vital interests of the data subject or of another natural person.

##### **8.2 Transparency**

- a. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:



- i. of its identity and contact details;
  - ii. of the categories of personal data processed;
  - iii. of the right to obtain a copy of these Clauses;
  - iv. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- b. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- c. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- d. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### 8.3 Accuracy and data minimisation

- a. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- b. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- c. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

### 8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

### 8.5 Security of processing

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the

- processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- b. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- c. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- d. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- e. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- f. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- g. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

## 8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

## 8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or

agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- i. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### **8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

#### **8.9 Documentation and compliance**

- a. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- b. The data importer shall make such documentation available to the competent supervisory authority on request.

#### **Clause 9: Use of sub-processors Clause 10: Data subject rights**

- a. The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- b. In particular, upon request by the data subject the data importer shall, free of charge:
  - i. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view

to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

ii. rectify inaccurate or incomplete data concerning the data subject;

iii. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

c. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

d. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the law of the country of destination, provided that such law lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

i. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

ii. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

e. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

f. The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

g. If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

#### **Clause 11: Redress**

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

- i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### **Clause 12: Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

#### **Clause 13: Supervision**

- a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to

respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### **Clause 14: Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted



by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### **15.2 Review of legality and data minimisation**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has

decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **Section IV – FINAL PROVISIONS**

##### **Clause 16: Non-compliance with the Clauses and termination**

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.



**Clause 17: Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands (*specify Member State*).

**Clause 18: Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of The Netherlands (*specify Member State*).
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX TO SCHEDULE D-1 (SCCS MODULE 1)****ANNEX I****A. LIST OF PARTIES**

See Schedule A to the DPA

**B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA

**C. COMPETENT SUPERVISORY AUTHORITY**

See Schedule B to the DPA

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

See Schedule C to the DPA

## SCHEDULE D-2:INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the UK Information Commissioner's Office for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

**PART 1: TABLES****TABLE 1: PARTIES**

Start date	See effective date of the DPA	

The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	See Schedule A of the DPA	
Key Contact	See Schedule A of the DPA	

**TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES**

AddendumEU SCCs	The Approved EU SCCs, including the Appendix Information, set out in Schedule D-1, Schedule E or Schedule F to the DPA, as applicable
-----------------	---

**TABLE 3: APPENDIX INFORMATION**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

	Annex 1A: List of Parties: <b>See Schedule A to the DPA</b>
--	---

Annex 1B: Description of Transfer: <b>See Schedule B to the DPA</b>
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: <b>See Schedule C to the DPA</b>
Annex III: List of Sub processors (Modules 2 and 3 only): <b>N/A</b>

**TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES**

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Neither Party
---	---

## Part 2: Mandatory Clauses

### Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on

the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

#### Interpretation of this Addendum

3.Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

<b>Addendum</b>	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
<b>AddendumEU SCCs</b>	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
<b>Appendix Information</b>	As set out in Table 3.
<b>Appropriate Safeguards</b>	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
<b>Approved Addendum</b>	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022.
<b>ApprovedEU SCCs</b>	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
<b>ICO</b>	The Information Commissioner.
<b>Restricted Transfer</b>	A transfer which is covered by Chapter V of the UK GDPR.
<b>UK</b>	The United Kingdom of Great Britain and Northern Ireland.
<b>UK Data Protection Laws</b>	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
<b>UK GDPR</b>	As defined in section 3 of the Data Protection Act 2018.

4.This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5.If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6.If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7.If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8.ny references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

#### **Hierarchy**

9..Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10.Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11.Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

#### **Incorporation of and changes to the EU SCCs**

12.This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13.Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14.No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15.The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

- a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
- b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

- c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

d. Clause 8.7(i) of Module A is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

#### **Amendments to this Addendum**

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a. its direct costs of performing its obligations under the Addendum; and/or
- b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

## SCHEDULE E: STANDARD CONTRACTUAL CLAUSES

### MODULE 2: CONTROLLER TO PROCESSOR TRANSFER

#### Section I

##### Clause 1: Purpose and scope

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- b. The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

**Clause 2: Effect and invariability of the Clauses**

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

**Clause 3: Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - iii. Clause 9 - Clause 9(a), (c), (d) and (e);
  - iv. Clause 12 - Clause 12(a), (d) and (f);
  - v. Clause 13;
  - vi. Clause 15.1(c), (d) and (e);
  - vii. Clause 16(e);
  - viii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4: Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **Section II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Instructions**

- a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

##### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

##### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

##### **8.4 Accuracy**



If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data

subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

- a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance.

In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

#### **Clause 9: Use of sub-processors**

a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least twenty business days' in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).

The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### **Clause 10: Data subject rights**

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **Clause 11: Redress**

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

ii. refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### **Clause 12: Liability**

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

- f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13: Supervision**

a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

### **Clause 14: Local laws and practices affecting compliance with the Clauses**

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the

categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the



importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **Section IV – FINAL PROVISIONS**

### **Clause 16: Non-compliance with the Clauses and termination**

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- ii. the data importer is in substantial or persistent breach of these Clauses; or
- iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17: Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands.

#### **Clause 18: Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of The Netherlands (specify Member State).
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

## **APPENDIX TO SCHEDULE E (SCCS MODULE B)**

### **ANNEX I**

#### **A.LIST OF PARTIES**

See Schedule A to the DPA



## B. DESCRIPTION OF TRANSFER

See Schedule B to the DPA

## C. COMPETENT SUPERVISORY AUTHORITY

See Schedule B to the DPA

## ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Schedule C to the DPA

# SCHEDULE F: STANDARD CONTRACTUAL CLAUSES

## MODULE 4: PROCESSOR TO CONTROLLER TRANSFER

### Section I

#### Clause 1: Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

- i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### Clause 2: Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional

safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### **Clause 3: Third-party beneficiaries**

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- ii. Clause 8 - Clause 8.1 (b) and Clause 8.3(b);
- iii. Clause 15.1(c), (d) and (e);
- iv. Clause 16(e);
- v. Clause 18.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### **Clause 4: Interpretation**

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### **Clause 7: Docking clause**

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **Section II – OBLIGATIONS OF THE PARTIES**

### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### 8.1 Instructions

- a. The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- b. The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- c. The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- d. After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

### 8.2 Security of processing

- a. The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- b. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- c. The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 8.3 Documentation and compliance

- a. The Parties shall be able to demonstrate compliance with these Clauses.
- b. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

### Clause 9: Use of sub-processors Clause 10: Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

### Clause 11: Redress

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it

receives from a data subject.

#### **Clause 12: Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

#### **Clause 13: Supervision**

### **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### **Clause 14: Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the

requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **Section IV – FINAL PROVISIONS**

### **Clause 16: Non-compliance with the Clauses and termination**

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17: Governing law**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands (*specify country*).

#### **Clause 18: Choice of forum and jurisdiction**

Any dispute arising from these Clauses shall be resolved by the courts of The Netherlands (*specify country*).

### **APPENDIX TO SCHEDULE F (SCCS MODULE 4)**

#### **ANNEX I**

##### **A. LIST OF PARTIES**

See Schedule A to the DPA

##### **B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA



# 二级经销商

## 受邀注册为二级经销商

最近更新时间：2023-12-07 11:29:34

### 1. 账号注册

第一步：点击一级经销商的邀请链接，进入注册页面，填写注册信息。（必须通过邀请链接进入）

**Register Tencent Cloud Sub Reseller**

Choose the account type

**Enterprise account**  
For your company, school, or organization

Country/Region  
Please select a country/region

Business email address  
Please enter your email address

Password  
Please enter your login password

Confirm password  
Please confirm your login password

Verification code  
Enter the verification code [Send code](#)

☐ I confirm that I have read and acknowledge the [Privacy Policy](#), [Data Processing and Security Agreement](#), [Tencent Cloud Terms of Service](#)

[Sign up](#)

Tencent  
Copyright © 2015-2023 Tencent Cloud. All Rights Reserved.

[Privacy Policy](#) | [Legal](#) | [Cookie Policy](#)

第二步：完善账号信息，填写企业名称、地址、手机号等，提交信息后，进入下一步。

**Complete information**

Before using Tencent Cloud service, please improve account information

Company name  
Enter your company name

Company address  
Street/apt, suite, unit, building, floor, etc.  
City State Postal code

Industry  
Select

Mobile number  
+86 Enter your phone number

Verification code  
Send code

☐ I want to receive news and promotional offers by email

☐ I want to receive news and promotional offers by SMS

☐ I want to receive news and promotional offers by phone call

[Submit](#)

**Promotions**

**Promotions**  
A wealth of vouchers, discounts and rebate activities, and a variety of free products for you to experience. Explore more about Tencent Cloud special offers, benefits, and incentives!

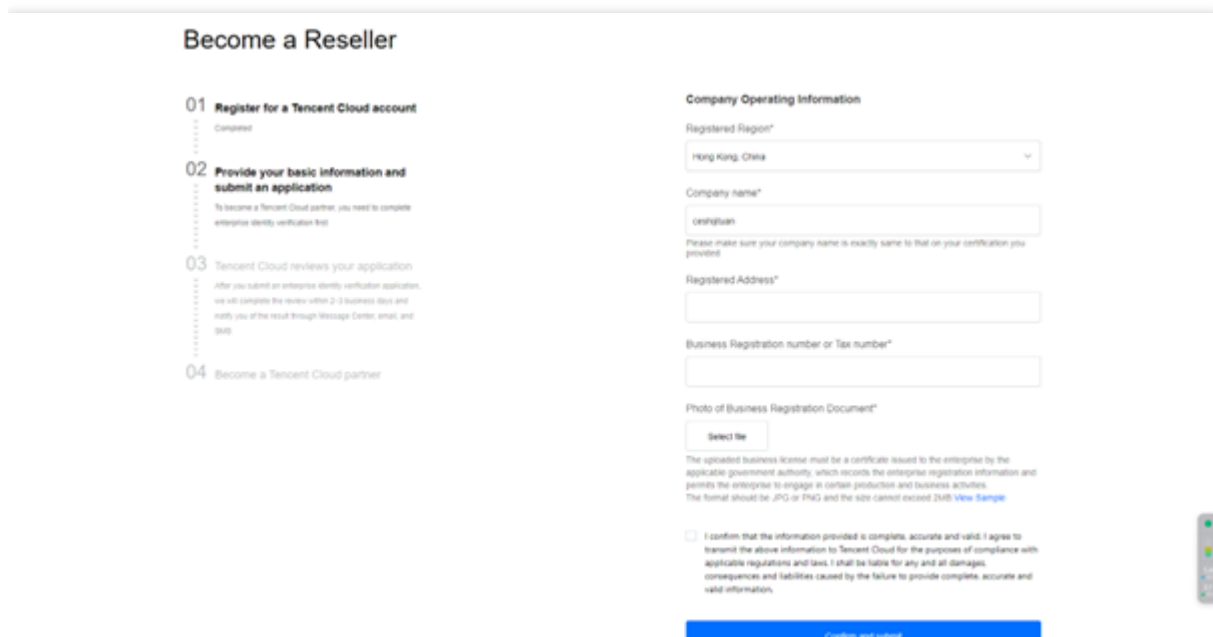
**Tencent Real-Time Communication (TRTC)**  
Run a demo within one minute and build solutions for audio/video calls or interactive live streaming within 30 minutes.

**Chat**  
Provides globally interconnected chat APIs, multi-platform SDKs, and CRM components to help you quickly bring messaging capabilities to your applications and websites.

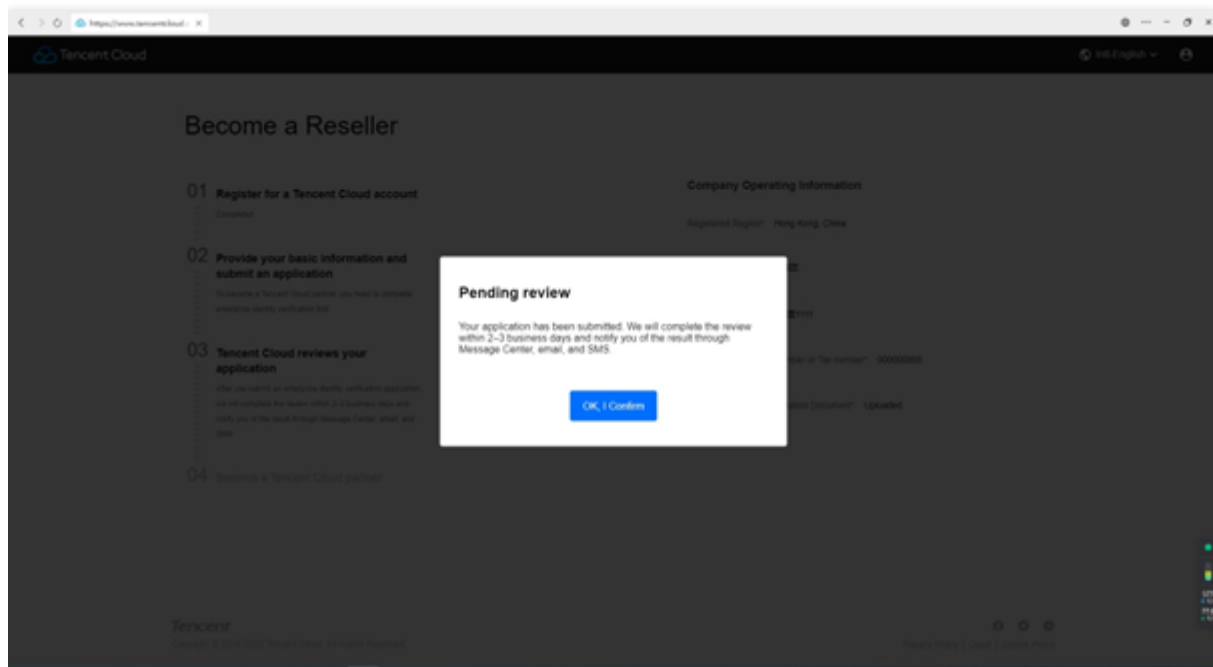


## 2.企业实名认证

第一步：填写企业认证相关信息，包括企业营业执照等（注：营业执照是指由政府机构颁发的、允许公司在政府的地域管辖范围内开展业务的许可证。）



第二步：提交信息后，等待审核完成，审核通常需要2-3个工作日。实名认证成功后您会通过邮件、短信以及站内信的方式收到通知。



## 3.资质审核

第一步：企业实名认证审核完成后，请再次登录官网或点击邀请链接，进入资质审核环节，填写资质审核所需信息。

**Become a Reseller**

**01 Enter the enterprise information**  
The enterprise information will be used for the business cooperation between the partner and Tencent Cloud, including qualification review, contract signing, and capital transactions.

**02 Pending review**  
After you submit your enterprise information, we will complete the review within 2-3 business days and notify you of the result through Message Center, email, and SMS.

**03 Become a Tencent Cloud partner**

**Contact information**

**Name\***  
First Name Last Name

**Role/job Title\***  
Role/job Title

**Mobile Phone\***  
+86 Number

**Email\***  
123456789@qq.com

☐ I confirm that the information provided is complete, accurate and valid. I agree to transmit the above information to Tencent Cloud for the purposes of compliance with applicable regulations and laws. I shall be liable for any and all damages, consequences and liabilities caused by the failure to provide complete, accurate and valid information.

☐ I have read and agreed to the [Tencent Cloud Second-Level Reseller Terms and Conditions](#).

**Confirm and submit**

第二步：提交资质审核信息，等待一级经销商审核，审核资质生效后可以登录伙伴控制台。

**Become a Reseller**

**01 Enter the enterprise information**  
The enterprise information will be used for the business cooperation between the partner and Tencent Cloud, including qualification review, contract signing, and capital transactions.

**02 Pending review**  
After you submit your enterprise information, we will complete the review within 2-3 business days and notify you of the result through Message Center, email, and SMS.

**03 Become a Tencent Cloud partner**

**Contact information**

**Name\***  
First Name Last Name

**Role/job Title\***  
Role/job Title

**Mobile Phone\***  
+86 Number

**Email\***  
123456789@qq.com

☐ I confirm that the information provided is complete, accurate and valid. I agree to transmit the above information to Tencent Cloud for the purposes of compliance with applicable regulations and laws. I shall be liable for any and all damages, consequences and liabilities caused by the failure to provide complete, accurate and valid information.

☐ I have read and agreed to the [Tencent Cloud Second-Level Reseller Terms and Conditions](#).

**Confirm and submit**

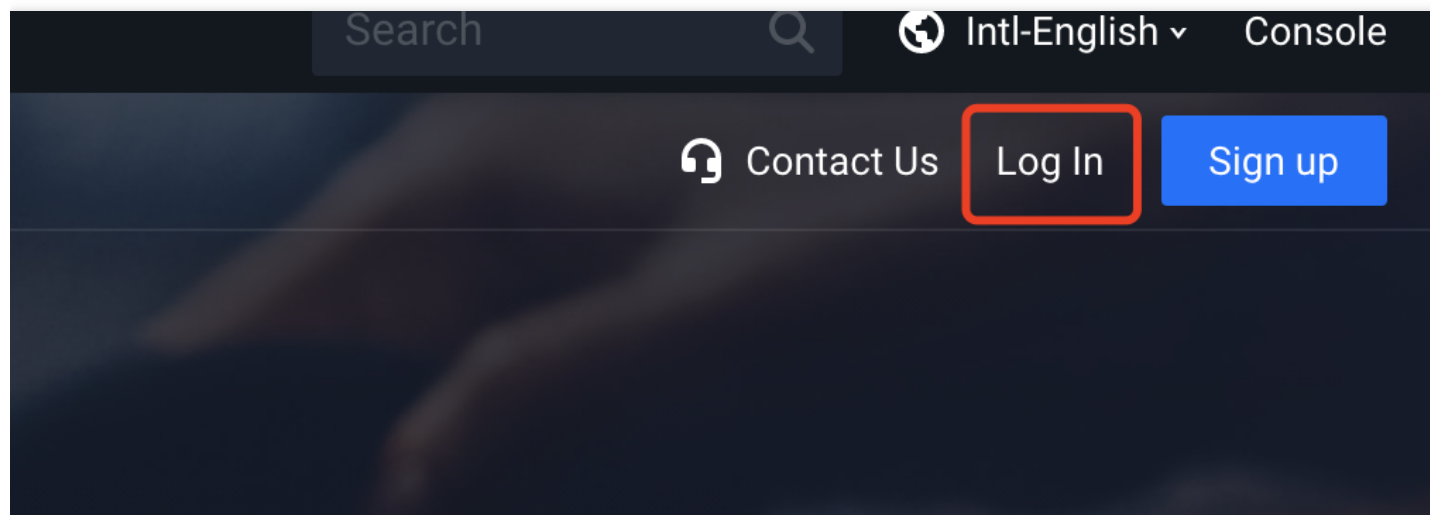
**Pending review**  
Your application has been submitted. We will complete the review within 2-3 business days and notify you of the result through Message Center, email, and SMS.

**OK, I Confirm**

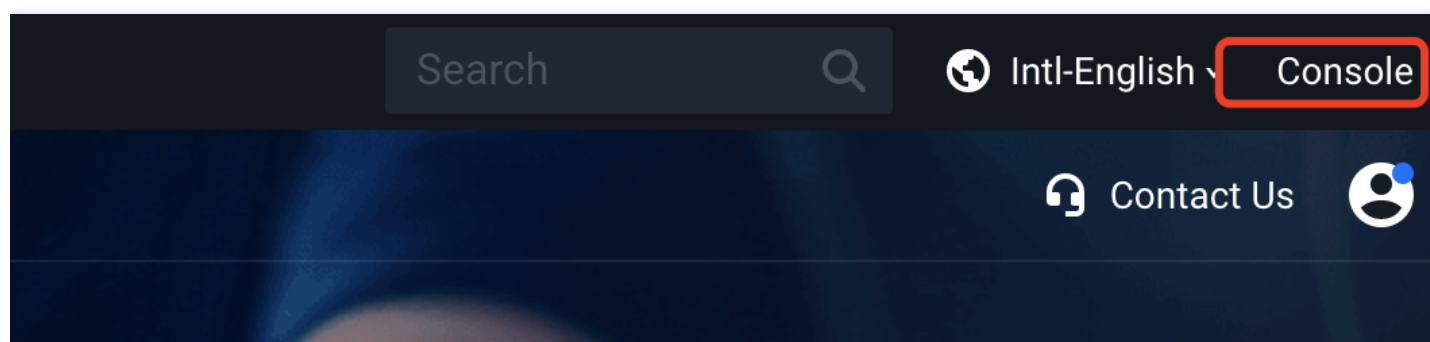
# 登录伙伴中心

最近更新时间：2022-11-17 16:49:20

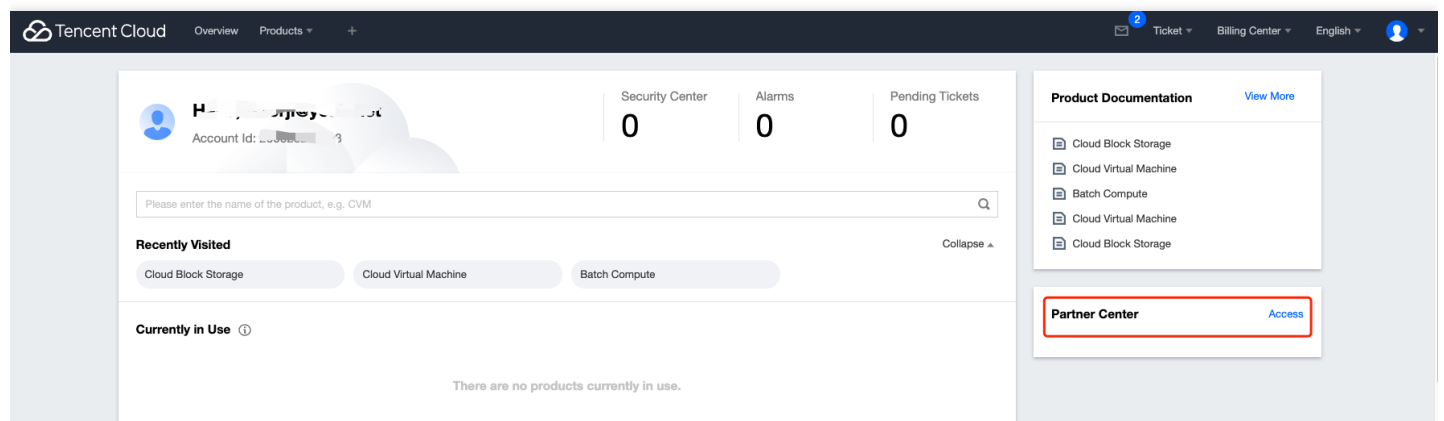
第一步：登录[经销商账号](#)。



第二步：登录成功后，点击右上角【控制台】。



第三步：点击【伙伴中心】，进入渠道控制台。



# 员工管理

最近更新时间：2023-03-09 11:33:46

员工管理可参考文档[员工管理](#)。

最近更新时间：2022-11-17 16:49:20

- 1、客户绑定：仅支持新注册客户绑定，不可绑定存量账号；
- 2、客户解绑：暂不支持线上解绑，如您的客户有解绑需求，请联系销售进行线下解绑处理。

点击【客户管理-邀请客户】，可发送邀请链接给客户，绑定成为经销商的客户。

**Tencent Cloud**

Overview Products +

**Partner Center**

- Company Information
- Customer Business
- Overview
- Customer Management**
- Customer Bills
- Customer Orders
- Voucher Management
- Bills Management

### Customer Management

+ Invite Customer

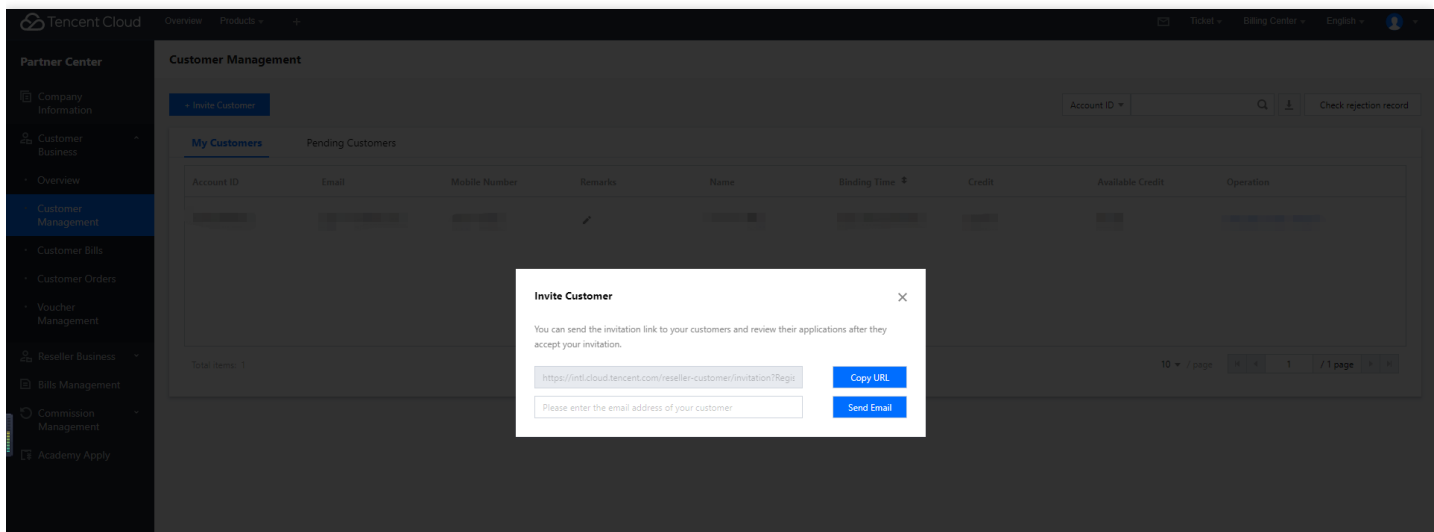
Account ID [ ] Q Check rejection record

**My Customers** Pending Customers

Account ID	Email	Mobile Number	Remarks	Name	Binding Time ↕	Credit	Available Credit	Operation
[REDACTED]	I*****2@yeah.net			11122233	2022-11-02 20:13:38	\$[REDACTED]	\$[REDACTED]	<a href="#">Allocate Credit</a> <a href="#">More ▾</a>
[REDACTED]	I****t@yeah.net	11		[REDACTED]	2022-11-02 15:23:23	\$[REDACTED]	\$[REDACTED]	<a href="#">Allocate Credit</a> <a href="#">More ▾</a>

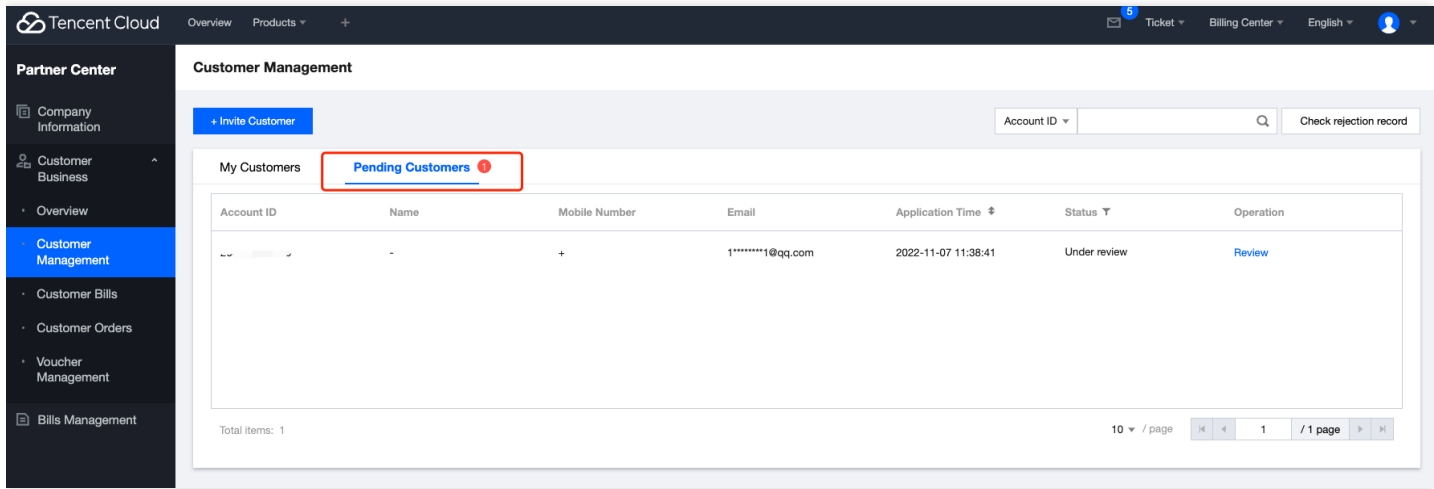
Total items: 2      10 / page    1 / 1 page

邀请链接发送方式，可邮件直接发送邀请链接，同时可复制邀请链接，线下通过其他方式发送。



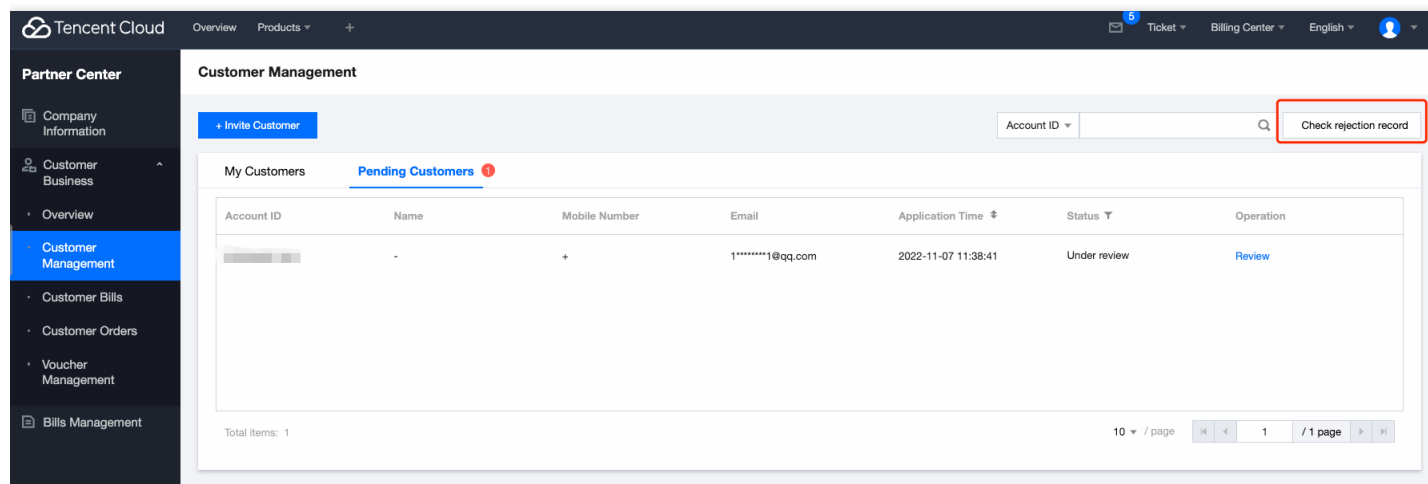
## 2、审核客户

客户提交绑定申请后，需经销商经销审核，确认是否可绑定。



## 3、驳回记录

客户提交绑定申请后，如经销商驳回，可查看所有驳回记录。



**Customer Management**

+ Invite Customer

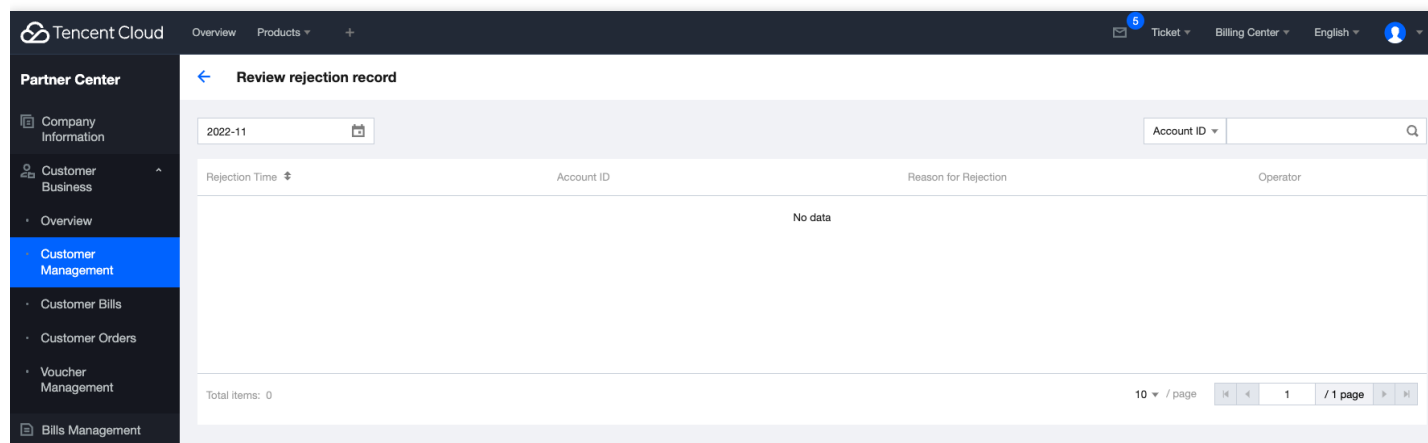
Account ID  [Check rejection record](#)

**My Customers** **Pending Customers** 1

Account ID	Name	Mobile Number	Email	Application Time	Status	Operation
[REDACTED]	-	+	1*****1@qq.com	2022-11-07 11:38:41	Under review	<a href="#">Review</a>

Total items: 1

10 / page 1 / 1 page



**Review rejection record**

2022-11

Account ID

Rejection Time	Account ID	Reason for Rejection	Operator
No data			

Total items: 0

10 / page 1 / 1 page



# 查询客户

最近更新时间：2022-11-17 16:49:20

合作伙伴可以查询其名下所有的子客，以及查看子客的基本信息、可用信用额度等。

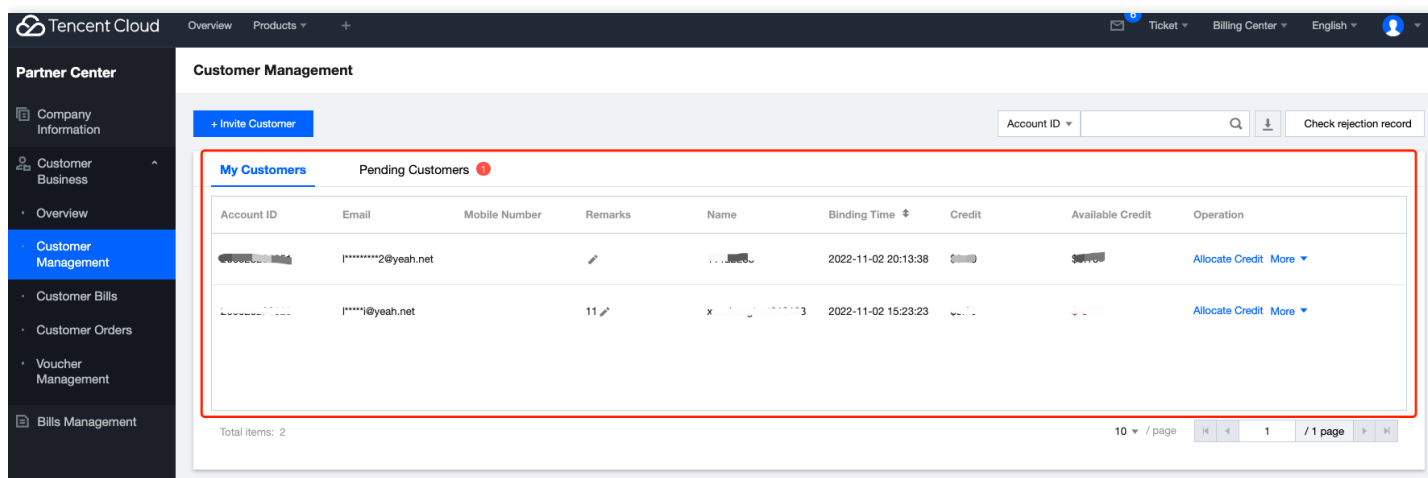
第一步：使用合作伙伴账号登录腾讯云，进入[伙伴中心](#)。

第二步：左侧导航栏中选择【客户管理】。

第三步：管理客户。

## 1、查询客户

伙伴可根据账号ID、名称、邮箱、备注等查询客户。

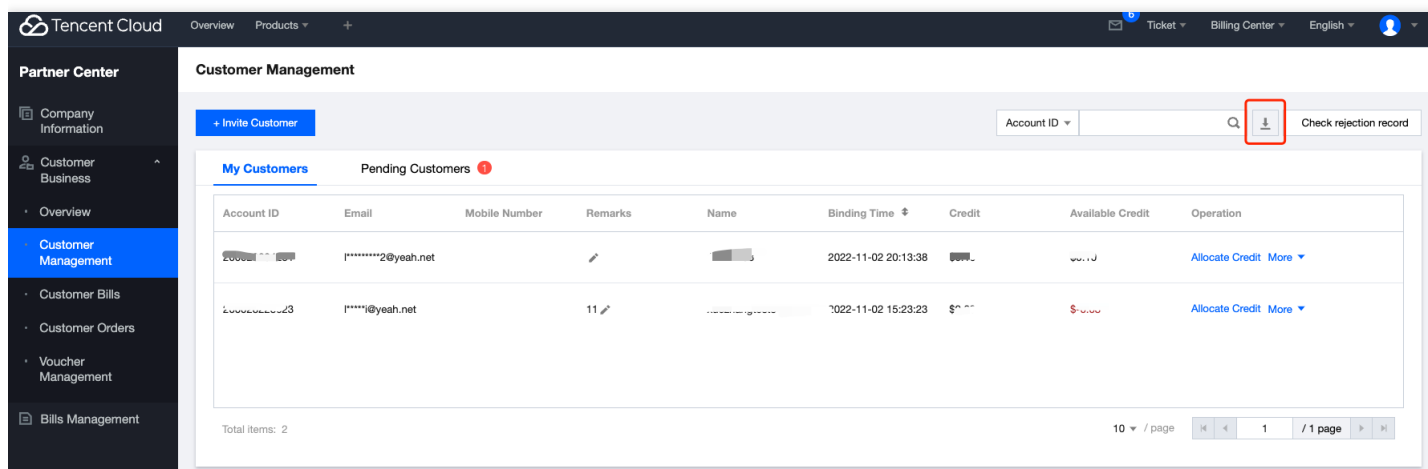


The screenshot shows the 'Customer Management' interface in the Tencent Cloud Partner Center. The left sidebar contains navigation options like 'Company Information', 'Customer Business', 'Overview', 'Customer Management' (selected), 'Customer Bills', 'Customer Orders', 'Voucher Management', and 'Bills Management'. The main content area displays a table of customers. The table has the following columns: Account ID, Email, Mobile Number, Remarks, Name, Binding Time, Credit, Available Credit, and Operation. Two customers are listed in the table. The 'Operation' column for each customer has links for 'Allocate Credit' and 'More'. A red box highlights the table area.

Account ID	Email	Mobile Number	Remarks	Name	Binding Time	Credit	Available Credit	Operation
20000000000000000000	*****2@yeah.net				2022-11-02 20:13:38			<a href="#">Allocate Credit</a> <a href="#">More</a>
20000000000000000000	*****i@yeah.net	11		x	2022-11-02 15:23:23			<a href="#">Allocate Credit</a> <a href="#">More</a>

## 2、导出客户

伙伴可导出全部客户。



The screenshot shows the 'Customer Management' interface in the Tencent Cloud Partner Center. The left sidebar contains navigation options like 'Company Information', 'Customer Business', 'Overview', 'Customer Management' (selected), 'Customer Bills', 'Customer Orders', 'Voucher Management', and 'Bills Management'. The main content area displays a table of customers. The table has the following columns: Account ID, Email, Mobile Number, Remarks, Name, Binding Time, Credit, Available Credit, and Operation. Two customers are listed in the table. The 'Operation' column for each customer has links for 'Allocate Credit' and 'More'. A red box highlights the 'Check rejection record' button in the top right corner of the table area.

Account ID	Email	Mobile Number	Remarks	Name	Binding Time	Credit	Available Credit	Operation
20000000000000000000	*****2@yeah.net				2022-11-02 20:13:38			<a href="#">Allocate Credit</a> <a href="#">More</a>
20000000000000000000	*****i@yeah.net	11		x	2022-11-02 15:23:23			<a href="#">Allocate Credit</a> <a href="#">More</a>

# 子客账户冻结

最近更新时间：2022-12-01 16:06:42

子客账户冻结操作目前仍需开白使用，请联系总经销商向腾讯侧申请开通。总经销商开通后，二级经销商默认可以使用。

子客账户冻结可参考文档[子客账户冻结](#)。

# 为客户分配信用

最近更新时间：2022-11-17 17:45:28

经销商可以查询其名下所有的客户，以及查看客户的基本信息、可用信用额度等。

第一步：线下联系您的销售经理，申请给客户分配的信用额度。（注：该信用额度区别于经销商的自用额度，请联系销售经理申请时说明申请信用额度为客户信用额度分配使用）

第二步：使用经销商账号登录[腾讯云](#)，进入[伙伴中心](#)。

第三步：左侧导航栏中选择【客户管理】，选择【我的客户】页签，在客户列表为客户分配信用。

Credit Allocation

×

Account name:

Account ID:

Available credit:

\$0.00

Total credit:

\$0.00

Used credit:

\$0.00

Notes:

1. The credit is the credit limit available to a customer. It is calculated as published at the Tencent Cloud official website and excludes deductions from vouchers.

2. Credit control is only a tool provided by Tencent Cloud for partners to control the approximate amount of credit available to customers. Due to the different billing modes and settlement cycles of Tencent Cloud services, there may be delays and differences in the monitoring of the fees incurred by customers.

3. We will send alarm notifications to you when a customer has used more than 75%, 90%, and 100% of their credit.

4. In the reseller mode, all fees incurred by customers are paid by the partner, so caution should be exercised.

5. A credit will immediately take effect once set.

Allocable credit: \$1,000.01

\* Allocated amount: (USD)

Available credit: \$0.00

Confirm

Close

Allocation Record

第四步：为客户调整信用。

## 1、分配信用

版权所有：腾讯云计算（北京）有限责任公司

第144 共442页

- (1) 在客户列表中，选中一条客户记录，单击操作列的【信用分配】，进入分配信用页面。
- (2) 设置【信用额度】，点击【确认】，系统提示分配成功信息。

Credit Allocation

Account name:1722203

Account ID:200000204251

Available credit:\$0.10

Total credit:\$0.10

Used credit:\$0.00

Notes:

1. The credit is the credit limit available to a customer. It is calculated as published at the Tencent Cloud official website and excludes deductions from vouchers.

2. Credit control is only a tool provided by Tencent Cloud for partners to control the approximate amount of credit available to customers. Due to the different billing modes and settlement cycles of Tencent Cloud services, there may be delays and differences in the monitoring of the fees incurred by customers.

3. We will send alarm notifications to you when a customer has used more than 75%, 90%, and 100% of their credit.

4. In the reseller mode, all fees incurred by customers are paid by the partner, so caution should be exercised.

5. A credit will immediately take effect once set.

Allocable credit: \$10.01

\* Allocated amount: (USD)

Available credit: \$0.10

Confirm

Close

Allocation Record

说明：

- 1、信用额度，为客户消费信用限额，按腾讯云官网计算，不包含代金券已抵扣部分；
- 2、信用管控只是腾讯云为伙伴提供了一种控制客户大概消费额度的工具，因云服务计费模式、结算周期等特点，客户消费监控会存在延时和误差；
- 3、如果客户的已使用信用额度比例超过75%、90%、100%，我们将发送预警通知给您；
- 4、经销模式下，客户消费最终由经销商负责还款，请谨慎操作；
- 5、信用额度设置完成后，即时生效。

## 2、回收信用

如果分配客户的信用额度较高，您可输入负值，回收客户可用信用额度。最高【可回收客户信用额度】≤【客户可用信用额度】。

### Credit Allocation



Account name:

Account ID:

Available credit:

**\$0.03**

Total credit:

\$4.90

Used credit:

\$4.87

Notes:

1. The credit is the credit limit available to a customer. It is calculated as published at the Tencent Cloud official website and excludes deductions from vouchers.

2. Credit control is only a tool provided by Tencent Cloud for partners to control the approximate amount of credit available to customers. Due to the different billing modes and settlement cycles of Tencent Cloud services, there may be delays and differences in the monitoring of the fees incurred by customers.

3. We will send alarm notifications to you when a customer has used more than 75%, 90%, and 100% of their credit.
4. In the reseller mode, all fees incurred by customers are paid by the partner, so caution should be exercised.
5. A credit will immediately take effect once set.
6. You can contact your channel manager to add you to the allowlist of the customer service suspension rule to shorten the service suspension period. For details, see [Customer Service Suspension Rules](#).

**Allocable credit: \$184.67**

\* Allocated amount: (USD)

-0.02



Available credit: \$0.01

Confirm

Close

[Allocation Record](#)

说明：

- 1、当客户可用信用额度为0时，不会触发客户停服，也不会影响客户新购产品。账户资产（信用+代金券）对新购和停服的影响，请查看[账户资产对新购&停服影响](#)。
- 2、联系您的总经销商，可申请开通客户欠费停服规则缩短停服期，具体规则请参考[子客欠费停服规则](#)说明。

### 3、分配记录

点击【信用分配页面-分配记录】，可查询经销商对客户全部的信用分配记录。

#### Credit Allocation



Account name:

1111111111

Account ID:

20111111111111

**Available credit:** \$0.00

Total credit: \$0.00

Used credit: \$0.00

#### Notes:

1. The credit is the credit limit available to a customer. It is calculated as published at the Tencent Cloud official website and excludes deductions from vouchers.
2. Credit control is only a tool provided by Tencent Cloud for partners to control the approximate amount of credit available to customers. Due to the different billing modes and settlement cycles of Tencent Cloud services, there may be delays and differences in the monitoring of the fees incurred by customers.
3. We will send alarm notifications to you when a customer has used more than 75%, 90%, and 100% of their credit.
4. In the reseller mode, all fees incurred by customers are paid by the partner, so caution should be exercised.
5. A credit will immediately take effect once set.

**Allocable credit:** \$0.00

\* Allocated amount: (USD)

Available credit: \$0.00

Confirm

Close

Allocation Record



Tencent Cloud

OverviewProducts+

TicketBilling CenterEnglish

Partner Center

Company Information

Customer Business

Overview

Customer Management

Customer Bills

Customer Orders

Voucher Management

Bills Management

Allocation Record (200028234251)

Allocation Time	Current Allocated Credit	Total Allocated Credit	Operator
2022-11-02 20:13:53	\$0.10	\$0.10	

Total items: 1

1 / 1 page

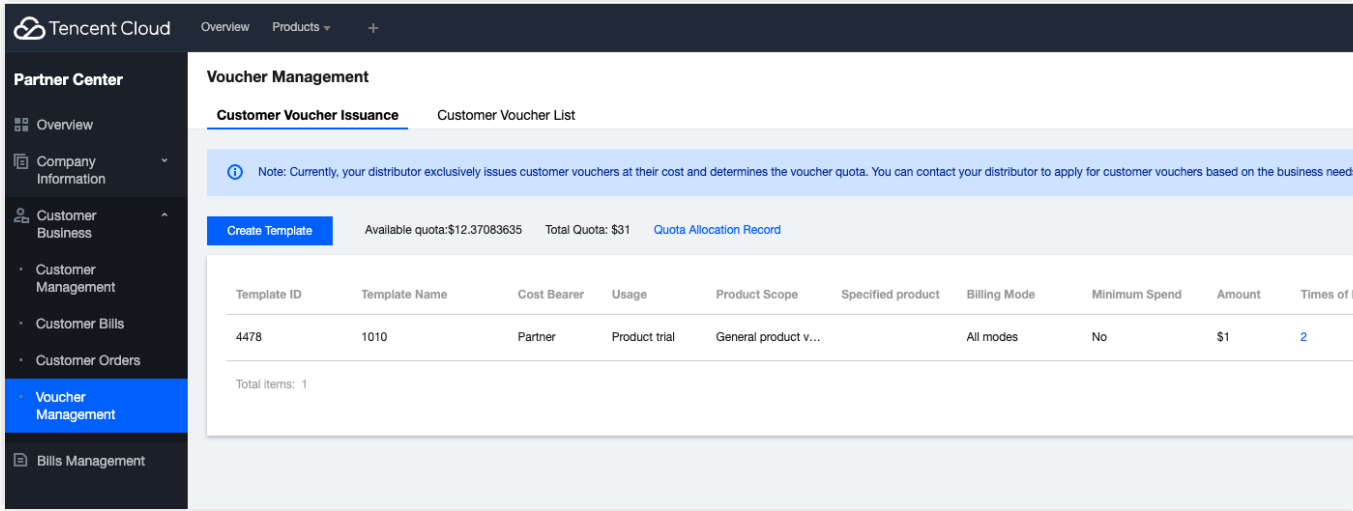
#### 4、信用通知

当您的客户已使用信用额度比例，超过75%、90%、100%，系统将给您和您的客户发送邮件、短信、站内信通知，请及时调根据客户情况调整额度，避免造成客户产品使用影响。

# 为客户分配代金券

最近更新时间：2024-06-14 15:18:27

- 第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。
- 第二步：点击[客户业务](#) > [代金券管理](#)菜单进入代金券发放页面。



- 第三步：点击[创建代金券模板](#)，填写代金券规则。

## Create Template

Template Name \*

Cost Bearer \*

☒ Partner

Usage \*

☒ Product trial ☐ Customer offer

Product Scope \*

☒ Specific Product Blacklist Voucher ☐ Specified product voucher ☐ General pr

Specified product \*

☐ One-Click Selection for the blacklist products corresponding to Manufacturer Vouche

Billing Mode \*

☒ All modes ☐ Prepaid ☐ Postpaid

Minimum Spend \*

☒ No

Voucher Type \*

☒ Balance deduction

Amount \*

USD

Available Quota: \$ 300

Validity Period \*

From the issuance date ▼

Please selec ▼

Month(s)

Description \*

0 / 1000

OK

Cancel

## 说明：

通用产品代金券：适用于可对客户任意产品的消耗费用进行抵扣。

指定产品代金券：适用于具体的单个或多个产品的产品测试场景申请，只对指定范围内的产品消耗费用进行抵扣。

一键选中“厂商代金券 - 通用产品代金券”对应的黑名单产品：自动选中一级经销商申请**厂商通用产品代金券**时，对应的黑名单产品列表，以代金券发放时为准。

第四步：确认填写内容后点击**确认**保存代金券模板。

**说明：**

代金券模板保存成功后，如未发放给实际客户，仍可以进行编辑，发放给客户后则模板无法继续编辑，可重新创建新的模板。

第五步：代金券模板创建完毕后，可以查看已创建的代金券模板，也支持按条件查询代金券模板。

Partner Center

Overview

Company Information

Customer Business

Customer Management

Customer Bills

Customer Orders

Voucher Management

Bills Management

Voucher Management

Customer Voucher Issuance

Customer Voucher List

Note: Currently, your distributor exclusively issues customer vouchers at their cost and determines the voucher quota. You can contact your distributor to apply for customer vouchers based on the business need.

Create Template

Available quota:\$12.37083635

Total Quota: \$31

Quota Allocation Record

Template ID	Template Name	Cost Bearer	Usage	Product Scope	Specified product	Billing Mode	Minimum Spend	Amount	Times o
4478	1010	Partner	Product trial	General product v...		All modes	No	\$1	2

Total items: 1

第六步：点击**发放**，可将代金券发放给具体的某一客户。

**说明：**

伙伴承担费用的客户代金券无需审批，伙伴确认发放后，子客即可收到代金券进行下单使用。

### Voucher Issuance

×

Template Name	1
Validity Period	3 month from the issuance date
Product Scope	General product voucher <span>(Note)</span> / All modes
Usage	Product trial
Cost Bearer	Partner

Customer Account ID \*

Select the customer account ID

Customer Name \*

Amount \*

100

USD

Available Quota: \$ 300

Issuance Remarks \*

Up to 1,000 characters

0 / 1000

OK

Cancel

## 代金券清单查询

点击客户业务>代金券管理 菜单进入客户代金券清单页面。客户代金券确认发放给客户后、可在此页面查询代金券状态和使用情况，支持全量查询或输入具体条件查询代金券。

### 说明：

客户代金券发放后，点击 客户代金券清单 即可查询到此代金券记录。

客户代金券发放后，可以通过代金券余额、代金券状态查看客户使用情况。

客户代金券发放后，如子客未使用完该代金券，允许经销商撤回代金券。

Partner Center

Overview

Company Information

Customer Business

Customer Management

Customer Bills

Customer Orders

Voucher Management

Voucher Management

Customer Voucher Issuance

Customer Voucher List

Template Name	Voucher ID	Cost Bearer	Customer Account ID	Customer Email	Amount	Balance	Issuance Time
1010	3634	Partner			\$1	\$0.00	2023-10-27 17:12
1010	3633	Partner			\$1	\$1.00	2023-10-27 17:11

Total items: 2

# 客户账单管理

最近更新时间：2022-11-17 16:49:20

经销商客户账单管理，可点击左侧菜单【客户业务>客户账单】进入客户账单页面，具体操作可参考[子客账单管理](#)。

## 协议管理 业务相关

# Tencent Cloud Second-Level Reseller Terms and Conditions

最近更新时间：2023-08-17 14:54:38

## Tencent Cloud Second-Level Reseller Terms and Conditions

### PLEASE READ THESE TERMS CAREFULLY BEFORE AGREEING TO BECOME A TENCENT CLOUD SECOND-LEVEL RESELLER PARTNER

YOUR PARTICIPATION AS A TENCENT CLOUD SECOND-LEVEL RESELLER (I.E. A RESELLER APPOINTED BY A TENCENT CLOUD DISTRIBUTOR, AND REFERRED TO AS A “**SECOND-LEVEL RESELLER**” HEREIN) IS SUBJECT TO THESE TERMS AND CONDITIONS INCLUDING EXHIBITS, DOCUMENTS AND ADDENDUMS REFERENCED HEREIN (COLLECTIVELY, THESE “**TERMS**”). THESE TERMS ARE LEGALLY BINDING AND GOVERN THE SECOND-LEVEL RESELLER’S RESELLING OF TENCENT CLOUD SERVICES AND USE OF THE PARTNER CONSOLE. YOU ACKNOWLEDGE AND AGREE THAT TENCENT MAY AMEND THESE TERMS AT ANY TIME BY POSTING THE UPDATED TERMS ON THE PARTNER CONSOLE WHICH WILL BECOME EFFECTIVE NO EARLIER THAN 7 DAYS AFTER THE DATE OF POSTING. YOU ACKNOWLEDGE THAT THESE TERMS ARE SEPARATE FROM THE RESELLER AGREEMENT BETWEEN SECOND-LEVEL RESELLER AND THE AUTHORIZED TENCENT CLOUD DISTRIBUTOR WHICH GOVERN THEIR RIGHTS AND OBLIGATIONS WITH RESPECT TO EACH OTHER IN THEIR DISTRIBUTOR--RESELLER RELATIONSHIP.

BY CLICKING “AGREE” BUTTON BELOW, YOU REPRESENT AND WARRANT THAT (I) YOU HAVE READ AND UNDERSTOOD THESE TERMS; (II) YOU ARE DULY AUTHORISED TO ACT ON BEHALF OF THE ENTITY APPLYING TO BECOME A TENCENT CLOUD SECOND-LEVEL RESELLER; AND (III) YOU ARE AUTHORISED TO ENTER INTO THESE TERMS AND LEGALLY BIND THE SECOND-LEVEL RESELLER TO THESE TERMS. IF YOU ARE NOT AUTHORISED TO BIND THE ENTITY TO THESE TERMS OR YOU DO NOT AGREE TO THESE TERMS IN FULL, DO NOT CLICK THE “AGREE” BUTTON BELOW, AND YOU CANNOT ENGAGE IN TENCENT CLOUD RESELLER ACTIVITIES NOR REPRESENT YOURSELF AS A TENCENT CLOUD SECOND-LEVEL RESELLER.

### 1. DEFINITIONS



(a) “**Applicable Data Protection Laws**” means, in respect of a Party, any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument relating to the protection of Personal Data, in each case as amended, consolidated, re-enacted or replaced from time to time, including but not limited to, as applicable, the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”), the UK Data Protection Act 2018 (“**UK DPA**”), the UK General Data Protection Regulation as defined by the UK DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, and the Privacy and Electronic Communications Regulations 2003, the California Consumer Privacy Act (“**CCPA**”).

(b) “**Appointment**” means the confirmation of appointment of Second-Level Reseller set out in Section 2(a).

(c) “**Authorized Reseller Territory**” or “**Territory**” means the territory or territories where Second-Level Reseller is authorized to Resell Tencent Services, which shall be specified by Authorized Tencent Cloud Distributor and set in the Second-Level Reseller Account in the Partner Console.

(d) “**Authorized Tencent Cloud Distributor**” means an authorized distributor of Tencent Services from whom Second-Level Reseller have entered into a reseller agreement to enable Second-Level Reseller to Resell Tencent Services in the Authorized Reseller Territory.

(e) “**Console Documentation**” means the information relating to the user guides, pricing, operation, support, functions of Tencent Services and the Console that are made available via the Console.

(f) “**Data Processing Addendum**” means the then-current data processing agreement applicable insofar as any performance pursuant to these Terms constitutes the processing of any Personal Data and/or is otherwise subject to any applicable laws relating to the processing of Personal Data and data protection in general in effect in any relevant jurisdiction, as located at <https://www.tencentcloud.com/zh/document/product/1085/55684> and updated from time to time.

(g) “**End User**” means a purchaser who is a customer of Second-Level Reseller and subscribes to any Tencent Services under a Subscription Agreement from the Second-Level Reseller for such purchaser’s own internal use and not for resale, transfer, or distribution to third parties.

(h) “**End User Purchase**” means any purchase of Tencent Services by an End User.

(i) “**European Economic Area**” means the member countries of the European Union specified in the official website of the European Union ([https://europa.eu/european-union/about-eu/countries\\_en](https://europa.eu/european-union/about-eu/countries_en)).

(j) “**Existing Customer of Tencent Services**” means a customer who already has a Tencent Cloud CID (Tencent Cloud Account ID) and/or any person/entity who have been purchasing Tencent Services directly from either Tencent, an authorized distributor or an authorized reseller.

(k) “**North America**” means Canada and the United States of America.

(l) “**Partner Console**” means the area designated as Console in the Tencent Cloud portal at <http://www.tencentcloud.com>. The Partner Console will provide Second-Level Reseller with Console Documentation,

updates, and online tools to administer and manage Second-Level Reseller's reseller activities relating to these Terms.

(m) **"Personal Data"** shall have the meaning as set out in the Applicable Data Protection Laws, and where such term is not defined in Applicable Data Protection Laws such term shall be defined by reference to the materially analogous term in the Applicable Data Protection Laws, and in respect of Data Subjects located in the state of California, "Data Subject" shall have the meaning given to the term "Consumer" in the CCPA and "Personal Data" shall have the meaning given to the term "Personal Information" in the CCPA.

(n) **"Resell"** or **"Resale"** means with respect to any Tencent Service, any resale or distribution of such Tencent Service to any End User in the Territory.

(o) **"Second-Level Reseller Account"** means the Second-Level Reseller's own login account, which shall be tied to the Authorized Tencent Cloud Distributor's account, for accessing the Partner Console to administer and manage reseller activities relating to these Terms.

(p) **"Tencent Services"** means software, content, digital materials and other items and services made available as a service offering by Tencent, through an Authorized Tencent Cloud Distributor, to Second-Level Reseller under these Terms, including, without limitation, any such service offerings made available to Second-Level Reseller for purchase via the Tencent Cloud international portal at [intl.cloud.tencent.com](http://intl.cloud.tencent.com).

(q) **"Updates"** means periodic updates to Tencent Services that Tencent may provide from time to time.

## 2. CONFIRMATION OF APPOINTMENT AND GENERAL OBLIGATIONS

(a) Confirmation of Appointment. Subject to these Terms and as long as there is a valid legally binding Reseller Agreement between the Second-Level Reseller and its Authorized Tencent Cloud Distributor, Tencent confirms the appointment of Second-Level Reseller as a non-exclusive independent reseller to Resell, on a non-exclusive basis, subscriptions to Tencent Services to End Users for their own use solely in the Authorized Reseller Territory, on the condition that Second-Level Reseller may not resell to an Existing Customer of Tencent Services. Second-Level Reseller will use its best efforts to promote and market the Tencent Services and to increase sales of the Tencent Services in the Territory. Tencent reserves the right to (by itself or by authorizing a third party to) promote, market, Resell, and support the Tencent Services inside and outside of the Territory to any End User. For the avoidance of doubt, Second-Level Reseller shall not Resell any Tencent Services outside the Territory, unless otherwise agreed in writing by Tencent.

(b) Partner Console Management. Second-Level Reseller shall administer and manage Resell activities relating to End Users through the functions and tools provided through Partner Console or via other processes authorized or designated by Tencent. Second-Level Reseller shall create a Second-Level Reseller Account in Partner Console in order to access and use Partner Console, and comply with all applicable terms and conditions governing its use of Partner Console. Second-Level Reseller will be provided a special URL link to enable its End Users to create a Tencent Cloud account and to submit subscription orders to purchase Tencent Services. All such End Users' Tencent

Cloud accounts will be linked to the Second-Level Reseller account identifying the Second-Level Reseller being the reseller.

(c) Terms of Sale. The End Users of a Second-Level Reseller who make purchases of Tencent Services will be associated as a purchase from the Second-Level Reseller and all such End Users transactions will be identified as a reseller sales transaction. In the interest of limiting each party's liability to End Users and protecting certain rights, in connection with Second-Level Reseller's Sale of the Tencent Services, All End Users must accept all applicable terms and conditions relating to use of Tencent Services including, without limitation, the Tencent Cloud Reseller Customer Terms of Service, Acceptable Use Policy, Privacy Policy and other terms and conditions in the Tencent Cloud portal.

(d) Relationship. Second-Level Reseller is an independent contractor of Tencent under these Terms. All financial obligations associated with Second-Level Reseller's business are the responsibility of Second-Level Reseller. The parties acknowledge and agree that Second-Level Reseller will be the primary point of contact with End Users and will be solely responsible for maintaining the relationship with such End Users (including managing all respective End User accounts and related resources). However, Tencent may, in its sole discretion, contact any such End User to resolve issues or to comply with applicable laws. All sales and other agreements between Second-Level Reseller and its End Users are Second-Level Reseller's exclusive responsibility.

(e) Tencent Trademarks. Tencent hereby grants to Second-Level Reseller a non-exclusive, non-transferable, and non-sublicensable license in the Territory to use the trademarks, trade names, service marks, and logos of Tencent ("**Tencent Trademarks**"), during the Term and solely in the Territory and solely in connection with Second-Level Reseller's marketing, promotional, and sales of the Tencent Services in accordance with these Terms. Second-Level Reseller will ensure that its use of any Tencent Trademark complies with Tencent's then-current trademark use guidelines as may be changed by Tencent from time to time. Any use of Tencent's Trademarks by Second-Level Reseller will first be submitted to Tencent for approval. Second-Level Reseller will not alter or remove any Tencent Trademarks provided with or embedded in the Tencent Services. Other than otherwise expressly provided herein, nothing contained in these Terms will grant or will be deemed to grant to Second-Level Reseller any right, title, or interest in or to Tencent's Trademarks. All uses of Tencent's Trademarks and related goodwill will inure solely to Tencent. Second-Level Reseller may not register or attempt to register, directly or indirectly, within the Territory or elsewhere, any trademarks, service marks, or URLs that utilize, or that are confusingly similar to, a Tencent Trademark.

(f) Second-Level Reseller Trademarks. Second-Level Reseller hereby grants to Tencent a non-exclusive, non-transferable, and non-sublicensable license in the Territory to use the trademarks, trade names, service marks, and logos of Second-Level Reseller ("Second-Level Reseller Trademarks") that are provided by Second-Level Reseller and/or uploaded by Second-Level Reseller to the Partner Console, during the Term and solely in the Territory and solely in connection with Tencent's marketing and promotion of the Tencent Services involving Second-Level Reseller's participation as a reseller of Tencent Services in accordance with these Terms. Tencent will ensure that its use of any Second-Level Reseller Trademark complies with Second-Level Reseller's then-current trademark use guidelines as may be changed by Second-Level Reseller from time to time. Other than otherwise expressly provided

herein, nothing contained in these Terms will grant or will be deemed to grant to Tencent any right, title, or interest in or to Second-Level Reseller's Trademarks. All uses of Second-Level Reseller's Trademarks and related goodwill will inure solely to Second-Level Reseller. Tencent may not register or attempt to register, directly or indirectly, within the Territory or elsewhere, any trademarks, service marks, or URLs that utilize, or that are confusingly similar to, a Second-Level Reseller Trademark. For the avoidance of doubt, Tencent may identify Second-Level Reseller as a reseller/partner of the Tencent Services on its website and marketing and promotional materials.

### 3. RESALE OF TENCENT SERVICES

(a) Second-Level Reseller Orders. Second-Level Reseller shall submit a purchase order for Tencent Services through the standard ordering process on Tencent Cloud international portal, Partner Console or through an order form in a format designated by Authorized Tencent Cloud Distributor and Second-Level Reseller shall specify the purchase order details (e.g., such as applicable price to be paid, type and volume ordered, minimum commitment, product activation date, term, and End User identity, address and entity details)(**"Purchase Order"**). Second-Level Reseller shall pay all applicable fees to its Authorized Tencent Cloud Distributor for the Tencent Services purchased under the Purchase Order.

(b) Account Access. Once a Purchase Order is accepted, Second-Level Reseller will be responsible to arrange for its End User to set up a Tencent Cloud account (either as a separate End User account or a sub-account for End User under the Second-Level Reseller account through the Partner Console) so as to facilitate their access to the Tencent Services purchased by such End Users. For all such End Users accounts, they will be associated with their relevant Second-Level Reseller's account in the Partner Console so as to enable Second-Level Reseller to manage reseller activities related to its End Users' accounts.

(c) Subscription Agreement. Second-Level Reseller must require each End User to agree and enter into a valid and enforceable written agreement that meets all of the following requirements (a **"Subscription Agreement"**): (i) contains terms and conditions that are at least as restrictive and protective of Tencent as the Tencent Cloud Reseller Customer Terms of Service and applicable terms and conditions for that Tencent Service (which terms and conditions may be made available at intl.cloud.tencent.com and any supplemental URLs thereto and successor URLs thereof) (without limiting the generality of the foregoing, the Subscription Agreement must disclaim, to the maximum extent permitted by applicable laws, Tencent's liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Tencent Services, except for the express warranties made by Tencent in the applicable terms and conditions for that Tencent Service); (ii) does not make any representations, warranties, or guarantees concerning the Tencent Services that are inconsistent with or in addition to those made by Tencent in these Terms; (iii) names Tencent as an intended third party beneficiary with the right to enforce the terms of that Subscription Agreement; (iv) provides that, upon expiration or termination of these Terms, that Subscription Agreement will automatically terminate or provide Second-Level Reseller the right to assign that Subscription Agreement to Tencent or any of its affiliates without End User's consent; and (v) specifies that access to Tencent Services may be immediately suspended or terminated if the End User is in default. Second-Level Reseller will be responsible for collecting payment from each End User. Second-Level Reseller will use its best efforts to enforce each Subscription

Agreement with at least the same degree of diligence used in enforcing similar agreements governing others, which in any event will be sufficient to adequately enforce each Subscription Agreement. Second-Level Reseller will use its best efforts to protect Tencent's proprietary intellectual property rights, promptly notify Tencent of any breach of a material obligation under a Subscription Agreement affecting any part of a Tencent Service, and cooperate with Tencent in any legal action to prevent or stop unauthorized use of any Tencent Service. Second-Level Reseller will provide to Tencent copies of all executed Subscription Agreements upon request, and will cooperate with Tencent if Tencent elects to enforce a Subscription Agreement directly against an End User. Second-Level Reseller acknowledges that Tencent is a third party beneficiary of each Subscription Agreement.

(d) Service Provisioning. Depending on the Territory where the Tencent Services are provisioned, they shall be provisioned by the Tencent entity specified in the Tencent Cloud Terms of Service on the Tencent Cloud portal.

#### 4. SECOND-LEVEL RESELLER SUPPORT AND REFUND OBLIGATIONS

(a) Support. Second-Level Reseller and Tencent will provide support to End Users and Tencent will provide limited support to Second-Level Reseller as follows:

Support provided by Reseller to End Users	Support Level	Support provided by Tencent to Second Level Reseller
<ul style="list-style-type: none"> <li>• Troubleshooting for End Users</li> <li>• Setup and configuration assistance</li> </ul>	<b>Tier 1 Support</b>	N/A
<ul style="list-style-type: none"> <li>• Troubleshooting for End Users with assistance from Tencent</li> </ul>	<b>Tier 2 Support</b>	<ul style="list-style-type: none"> <li>• Resolution of issues that cannot be easily resolved by <b>Second-Level Reseller</b> alone</li> <li>• Unless expressly specified otherwise in a Purchase Order, support provided in accordance with the General Service Level Agreements (as further described at <a href="https://www.tencentcloud.com/document/product/301/12905">https://www.tencentcloud.com/document/product/301/12905</a>)</li> </ul>
<ul style="list-style-type: none"> <li>• Troubleshooting for End Users with assistance from Tencent</li> </ul>	<b>Tier 3 Support</b>	<ul style="list-style-type: none"> <li>• Resolution of material technical issues that cannot be resolved by Partner alone</li> </ul>

For the avoidance of doubt, Tencent may redirect any End Users requests for support to **Second-Level Reseller** as appropriate in accordance with the above conditions.

(b) End Users Refunds. If End User seeks to exercise its right to refund under applicable laws, Second-Level Reseller shall promptly notify its Authorized Tencent Cloud Distributor and provide all necessary information relating to the End

User's refund request. Tencent will, through the Authorized Tencent Cloud Distributor, review the request and, if required under applicable laws, process the refund request by providing a refund or service credit to Second-Level Reseller through the Authorized Tencent Cloud Distributor and in turn Second-Level Reseller shall promptly process the End User refund request and revert to the End User. If Tencent receives a refund request from End User directly, the refund request will be redirected to Second-Level Reseller to follow up on the relevant purchase order between Second-Level Reseller and End User.

## 5. TERM AND TERMINATION

(a) Term. The Appointment commences when the Second-Level Reseller creates a Second-Level Reseller account and click "Agree" to these Terms and shall continue in effect until terminated in accordance with this Section 5 ("Term").

(b) Termination without Cause. Tencent may terminate these Terms without cause upon 60 days prior written notice to Second-Level Reseller.

(c) Termination of Reseller Agreement with Authorized Tencent Cloud Distributor. The Appointment will be terminated automatically when the Tencent Cloud services reseller agreement between Authorized Tencent Cloud Distributor and the Second-Level Reseller is terminated.

(d) Termination for Cause. Either party may terminate the Appointment if the other party (i) commits a material breach of these Terms and fails to cure that material breach within 30 days following its receipt of notice regarding that material breach from the non-breaching party; (ii) becomes insolvent; or (iii) ceases, or threatens to cease, to carry on business. Tencent may terminate the Appointment when it is required to do so by applicable law, court order or requirements imposed by government bodies, or if Tencent otherwise determines that it is reasonable to do so in order to ensure that Tencent does not violate or risk violation of the same.

(e) Effects of Termination

(i) Upon termination of the Appointment, all rights granted to Second-Level Reseller shall be terminated immediately, Second-Level Reseller shall cease all Resell of Tencent Services and all use of the Tencent Trademarks as contemplated under these Terms. Tencent shall cease all use of the Second-Level Reseller Trademarks as contemplated under these Terms, both Tencent and Second-Level Reseller shall work in good faith for a transition of the End Users, including without limitation, whether to terminate or assign their subscription agreements to Tencent, one of its affiliates or to another reseller partner;

(ii) Second-Level Reseller will, at Tencent's direction, terminate Subscription Agreements or assign Subscription Agreements to Tencent or one of its affiliates or other reseller partner and provide contact and other reasonable information to Tencent about transferred End Users; and

(iii) Second-Level Reseller is responsible to pay its Authorized Tencent Cloud Distributor all amounts of outstanding and unpaid fees accepted prior to the date of termination.



(f) Survival. The following provisions will survive any expiration or termination of these Terms: Sections 1, 4(b), 5(e), 5(f), 6(d), 7 to 12. The termination or expiration of the Appointment and these Terms will not relieve Second-Level Reseller of: (i) the obligation to pay any fees that are due to its Authorized Tencent Cloud Distributor; or (ii) Second-Level Reseller's obligation to indemnify Tencent as specified in these Terms.

## 6. SUSPENSION RIGHTS

(a) Suspension of Second-Level Reseller's access to Tencent Services by Tencent. Tencent retains the right to immediately upon written notice suspend Second-Level Reseller's access to any or all Tencent Services resold by Second-Level Reseller if (i) Authorized Tencent Cloud Distributor informs Tencent that Second-Level Reseller has failed to make any payment of agreed price for Tencent Services purchased under a Purchase Order when due, (ii) Second-Level Reseller has breached any terms of these Terms, or (iii) the resale of Tencent Services by Second-Level Reseller will violate any applicable laws or regulations, and Tencent may continue to impose the suspension indefinitely until the aforesaid issues have been rectified to the satisfaction of Tencent.

(b) Suspension of End User's access to Tencent Services by Tencent. Tencent retains the right to immediately upon written notice suspend an End User's access to any or all Tencent Services purchased from Reseller if (i) any conditions in Section 6(a) apply; (ii) such End User fails to make any payment of fees for Tencent Services purchased from Reseller when due; (iii) the credit balance allocated by Second-Level Reseller in relation to such End User's Tencent Cloud account falls to 0 (zero) or below; (iv) such End User has breached any terms and conditions applicable to the use of the relevant Tencent Services and/or the Subscription Agreement, or (v) the provision of Tencent Services to End User will violate any applicable laws or regulations, and Tencent may continue to impose the suspension indefinitely until the aforesaid issues have been rectified to the satisfaction of Tencent.

(c) Suspension of End User's access to Tencent Services by Second-Level Reseller. Second-Level Reseller. Subject to prior approval by Tencent, Second-Level Reseller may also exercise the right to suspend its End User's access to any or all of Tencent Services resold by Second-Level Reseller if (i) such End User has breached any terms and conditions applicable to the use of the relevant Tencent Services and/or the Subscription Agreement; (ii) such End User fails to make any payment of fees for Tencent Services purchased from Second-Level Reseller when due; or (iii) the resale of Tencent Services by Second-Level Reseller to End User will violate any applicable laws and regulations.

(d) Suspension Override by. Second-Level Reseller. For selected End Users which are determined by Second-Level Reseller and configured through the Partner Console, Second-Level Reseller may override the suspension of the End User's access to Tencent Services even if the credit balance allocated by Second-Level Reseller in relation to such End User's Tencent Cloud account falls to 0 (zero) or below provided always that Second-Level Reseller shall be responsible to repay and indemnify Tencent of all additional fees that are incurred by such End User after their credit balance falls to 0.

## 7. INTELLECTUAL PROPERTY AND PROPRIETARY RIGHTS NOTICES

(a) Intellectual Property. All right, title, and interest in and to the Tencent Services and any derivative work thereof, including all intellectual property rights therein, are and will remain exclusively with Tencent. Second-Level Reseller

has no right or license with respect to any Tencent Services, except as expressly set forth in these Terms. Second-Level Reseller may not act to jeopardize, limit, or interfere in any manner with Tencent's ownership of and rights with respect to the Tencent Services.

(b) Proprietary Rights Notices. Second-Level Reseller may not remove or alter any trademark, trade name, copyright, patent, patent pending, or other proprietary notices, legends, symbols, or labels appearing on or with the Tencent Services or related documentation provided by Tencent

## 8. WARRANTIES; DISCLAIMER

(a) Warranties. Unless expressly specified otherwise in a Purchase Order, Tencent represents and warrants that each Tencent Service will be provided consistently with, and will meet, the applicable General Service Level Agreement (as further described at <https://www.tencentcloud.com/document/product/301/12905>) (each, an "**SLA**"). With respect to Tencent's failure to meet the applicable SLA for a Tencent Service, Second-Level Reseller's sole and exclusive remedy, and Tencent's sole and exclusive liability, will be service credits provided pursuant to the terms of the applicable SLA. Second-Level Reseller represents and warrants that (a) it has the full legal power and authority to enter into and perform its obligations under these Terms, (b) the performance of its obligations under these Terms will not violate any other agreement to which it is a party, and (c) it will comply with all applicable laws when performing its obligations under these Terms.

(b) Disclaimer. EXCEPT FOR THE WARRANTIES SET FORTH IN SECTION 8(a), TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TENCENT DISCLAIMS ALL WARRANTIES WITH REGARD TO THE TENCENT SERVICES. ALL TENCENT SERVICES ARE PROVIDED "AS IS". TENCENT MAKES NO ADDITIONAL REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS, IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), OR STATUTORY, AS TO ANY MATTER WHATSOEVER. TENCENT EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, ACCURACY, INFRINGEMENT AND TITLE. TENCENT DOES NOT WARRANT AGAINST INTERFERENCE WITH THE ENJOYMENT OF THE TENCENT SERVICES OR AGAINST INFRINGEMENT. TENCENT DOES NOT WARRANT THAT THE TENCENT SERVICES ARE ERROR-FREE OR THAT OPERATION OF THE TENCENT SERVICES WILL BE SECURE OR UNINTERRUPTED. SECOND-LEVEL RESELLER WILL NOT HAVE THE RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTIES ON BEHALF OF TENCENT TO ANY OTHER THIRD PARTY. USE OF ANY INFORMATION OR DATA OBTAINED THROUGH THE TENCENT SERVICES IS AT SECOND-LEVEL RESELLER'S AND EACH END USER'S SOLE RISK. THE PARTIES AGREE THAT TENCENT WILL BEAR NO RESPONSIBILITY FOR THE ACCURACY OR QUALITY OF INFORMATION OR DATA OBTAINED THROUGH THE TENCENT SERVICES.

## 9. INDEMNIFICATION

(a) (a) Indemnification by Second-Level Reseller. Second-Level Reseller hereby indemnifies, defends, and holds harmless of Tencent and its affiliates and their respective employees, directors, agents, and representatives ("**Tencent Indemnified Parties**") from and against any and all third party claims, demands, suits, actions,



judgments, damages, costs, losses, expenses (including attorneys' fees) and other liabilities (each, a "**Claim**") arising from or relating to: (i) any actual or alleged breach of any of the representations, warranties, or covenants made by Second-Level Reseller under these Terms; (ii) any actual or alleged breach of any agreement between Second-Level Reseller and End User; (iii) any violation of or non-compliance with any applicable law; (iv) any unauthorized use or violation of a Tencent Service by an End User; or (v) Second-Level Reseller's negligence or willful misconduct.

(b) Indemnification Procedures. Tencent will promptly give Second-Level Reseller written notice of the Claim and will grant to Second-Level Reseller control over the defense and settlement of the Claim. Upon reasonable request by Second-Level Reseller, Tencent will provide assistance in connection with the defense and settlement of the Claim. However, Tencent's failure to comply with one or more of the obligations in the preceding sentence will not relieve Second-Level Reseller of its obligations under this Section 9 except and solely to the extent that such failure materially prejudices Second-Level Reseller's defense of the Claim. Second-Level Reseller may not settle any Claim without Tencent's prior written consent.

## 10. PRIVACY AND END USERS DATA

(a) Data Privacy Compliance. Second-Level Reseller shall comply with all applicable laws and regulations relating to privacy and data protection, and where applicable, provide all necessary notices to and obtain sufficient consents and authorizations from End Users and any other persons providing Personal Data to Second-Level Reseller and Tencent in connection with the processing of Personal Data by Second-Level Reseller, Tencent and its affiliates pursuant to these Terms. Tencent is entitled to collect, use, transfer and process End Users' data in accordance with the Tencent Cloud Terms of Service, Acceptable Use Policy, Privacy Policy and other terms and conditions in the Tencent Cloud portal.

(b) Data Processing Addendum. Second-Level Reseller shall comply with all applicable laws and regulations relating to privacy and data protection, and where applicable, provide all necessary notices to and obtain sufficient consents and authorizations from End Users and any other persons providing Personal Data to Second-Level Reseller and Tencent in connection with the processing of Personal Data by Second-Level Reseller, Tencent and its affiliates pursuant to these Terms. Tencent is entitled to collect, use, transfer and process End Users' data in accordance with the Tencent Cloud Terms of Service, Acceptable Use Policy, Privacy Policy and other terms and conditions in the Tencent Cloud portal.

(c) End Users' Data. Second-Level Reseller shall only use End Users' data solely for the purpose of providing End Users with the Tencent Services and support services in accordance with these Terms and to provide assistance to the End Users as well as managing and administering the End Users' records relating to their use and purchase of Tencent Services. If Second-Level Reseller receives a request for End Users' data from law enforcement authorities, then Second-Level Reseller shall redirect the authorities to request that data directly from the End Users. If compelled to disclose End Users' data to law enforcement authorities, Second-Level Reseller shall promptly notify End Users together with a copy of the official notice from the law enforcement authorities, unless it is illegal to do so. If Tencent is compelled to disclose End Users' data and related information to law enforcement authorities, Second-Level Reseller shall co-operate fully with Tencent to satisfy all requests from the law enforcement authorities including, without

limitation, to obtain all necessary consents from such End User(s) to give full force and effect to this Section to provide such End User(s)'s data and related information to the law enforcement authorities.

## 11. LIMITATION OF LIABILITY

(a) DISCLAIMER OF DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THESE TERMS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TENCENT WILL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO SECOND-LEVEL RESELLER OR END USERS FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE TRANSACTION CONTEMPLATED UNDER THESE TERMS, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS, LOSS OF GOODWILL, LOSS OF, OR DAMAGE TO, DATA OR CONTENT AND LOSS OF BUSINESS, EVEN IF TENCENT IS APPRISED OF THE LIKELIHOOD OF SUCH DAMAGES OCCURRING.

(b) CAP ON LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, UNDER NO CIRCUMSTANCES WILL TENCENT'S TOTAL LIABILITY OF ALL KINDS ARISING OUT OF OR RELATED TO THESE TERMS (INCLUDING WARRANTY CLAIMS), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT, OR OTHERWISE, EXCEED THE TOTAL AMOUNT OF THE PRICE OF THE TENCENT SERVICES SUPPLIED TO PARTNER UNDER THESE TERMS DURING THE 12 MONTHS PRECEDING THE CLAIM (DETERMINED AS OF THE DATE OF ANY FINAL JUDGMENT IN AN ACTION).

(c) INDEPENDENT ALLOCATIONS OF RISK. EACH PROVISION OF THESE TERMS THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES IS TO ALLOCATE THE RISKS OF THESE TERMS BETWEEN THE PARTIES. THIS ALLOCATION IS REFLECTED IN THE COMMISSION OFFERED BY TENCENT TO SECOND-LEVEL RESELLER AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THESE TERMS, AND EACH OF THESE PROVISIONS WILL APPLY EVEN IF THE WARRANTIES IN THESE TERMS HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

## 12. GENERAL

(a) Independent Contractors. The relationship of the parties established by these Terms is that of independent contractors, and nothing contained in these Terms should be construed to give either party the power to (i) act as an agent or (ii) direct or control the day-to-day activities of the other. Financial and other obligations associated with each party's business are the sole responsibility of that party.

(b) Non-Assignability and Binding Effect. Neither party will assign its rights and obligations under these Terms without the written consent of the other party, except: (i) that Tencent may assign these Terms to a successor to its business (including a successor by way of merger, acquisition, sale of all or substantially all of its assets, or operation of law); and (ii) Tencent may freely assign these Terms to its affiliates. Subject to the foregoing, these Terms will be binding upon and inure to the benefit of the parties and their successors and assigns.

(c) Non-solicitation. During the Term and for a period of one year thereafter, Partner may not, directly or indirectly, employ or solicit the employment or services of a Tencent employee or independent contractor without the prior written consent of Tencent.

(d) Notices. Except for provisions that expressly allow for email notice, any notice required or permitted to be given under these Terms will be effective if it is in writing and sent by certified or registered mail, or insured courier, return receipt requested, to the Partner at the physical address specified by Partner in the Partner Account and with the appropriate postage affixed. Notices are deemed given two business days following the date of mailing or one business day following delivery to a courier. For any notice sent to Tencent, copies of the notice will also need to be sent to Tengyun Building, Tower A, No. 397 Tianlin Road, Xuhui District, Shanghai, 200233, China (Attn: International Business Legal Center) and by email to IBLCLegalnotice@tencent.com.

(e) Force Majeure. Nonperformance of either party will be excused to the extent that performance is rendered impossible by strike, fire, flood, governmental acts, orders or restrictions, pandemic or any other reason where failure to perform is beyond the control and not caused by the negligence of the non-performing party.

(f) Export Control and Sanctions. Partner hereby represents and warrants to Tencent that at the time of entering into these Terms and throughout the Term neither Partner, its subsidiaries, nor any of Partner or Partner's subsidiaries' officers, directors, shareholders, agents or employees, are:

(a) listed in any list of designated persons maintained by the United States (including, without limitation, the list of "Specially Designated Nationals" as maintained by the Office of Foreign Assets Control of the U.S. Treasury Department, the United Nations Security Council, the United Kingdom (including the Consolidated List of Financial Sanctions Targets as maintained by His Majesty's Treasury), the European Union and any Member State thereof (including the Consolidated List of Persons, Groups and Entities Subject to Financial Sanctions), or any other list of restricted persons maintained by any authority with jurisdiction over Partner (any person so listed being a "**Restricted Person**"));

(b) organized under the laws of, operating from or located or resident in a country or territory that is the target of comprehensive sanctions (as of the date of these Terms, Iran, Cuba, North Korea, Syria and the Crimea/Sevastopol region and the so-called Donetsk and Luhansk People's Republics (collectively, "**Sanctioned Territories**")); or

(c) controlled or owned 50 percent or more (directly or indirectly) in the aggregate, by one or more Restricted Persons. In connection with Partner's performance of its obligations under these Terms, Partner will comply with all applicable export controls and economic sanctions laws and regulations of the United Nations, PRC, United States, European Union, including its member states; and other applicable government authorities, including without limitation, the U.S Export Administration Regulations ("**EAR**") and the economic sanctions rules and regulations implemented under statutory authority and/or the U.S. President's Executive Orders and administered by the U.S. Treasury Department's Office of Foreign Assets Control (collectively, "**Trade Laws**"). Partner agrees not to engage in any activities in connection with the performance of its obligations that would violate Trade Laws or that would risk placing Tencent in breach of any Trade Laws and Partner is solely responsible for compliance with Trade Laws

related to the manner in which Partner performs its obligations including: (a) Partner's transfer and processing of End User's data; (b) the provision of End User's data to End Users; and (c) accurately specifying the Territory in which any of the foregoing occur. For the avoidance of doubt, Partner is solely responsible for compliance with applicable laws (including the Trade Laws) relating to the use of the Tencent Services by the Partner and End Users.

(g) Relevant Actions. If at any time during the term of these Terms, (a) provision of the Tencent Services becomes otherwise restricted or prohibited as a consequence of the imposition of sanctions or by operation of Trade Laws; (b) Tencent reasonably believes a breach of Section 12(f) has occurred or is at risk of occurring; (c) Tencent reasonably believes that Partner or Partner's subsidiaries are in violation of Trade Laws or are engaging in activities that would risk placing Tencent in breach of any Trade Laws, Tencent shall not be obliged to perform any of its obligations under these Terms or continue to provide the Tencent Services and shall be entitled, in its sole discretion, to terminate these Terms, or any relevant Purchase Orders, and the provision of the Tencent Services with immediate effect and without any liability. Tencent is also entitled to take any other actions against Partner as it deems appropriate in the circumstances, including but not limited to, requesting Partner to remove any content that is subject to export control.

(h) Governing Law and Resolution of Disputes. (h) Governing Law and Resolution of Disputes. These Terms shall be governed by and interpreted in accordance with the laws as follows: If Second-Level Reseller is located in Europe Economic Area, UK and Switzerland, these Terms are governed by and interpreted in accordance with English laws. Any claims for equitable relief may be brought in any court of competent jurisdiction even if the parties have chosen an exclusive venue below. Any dispute or difference between the parties arising out of or in connection with these Terms, its interpretation or subject-matter, shall be referred to and finally resolved by arbitration under the London Court of International Arbitration (LCIA) Rules, which rules are deemed to be incorporated by reference into this Section. The seat of arbitration shall be London, the United Kingdom. The language to be used in the arbitral proceedings shall be English; If Second-Level Reseller is located in North America, these Terms are governed by and interpreted in accordance with the laws of the State of California, USA, without giving effect to provisions related to choice of laws or conflict of laws. Any claims for equitable relief may be brought in any court of competent jurisdiction and for all claims arising out of or relating to these Terms or the Services. Any dispute or difference between the parties arising out of or in connection with these Terms will be settled by binding arbitration in Santa Clara County, California under the auspices of the American Arbitration Association (the "**Association**") and under the rules of the Association in force at the commencement of such arbitration proceedings. Judgment upon the award rendered by the arbitrators may be entered in any court of competent jurisdiction; and If Second-Level Reseller is located in the rest of the world except People's Republic of China, these Terms is governed by and interpreted in accordance with the laws of Singapore. Except for the right of either party to apply to any court of competent jurisdiction for a temporary restraining order, a preliminary injunction, or other equitable relief to preserve the status quo or prevent irreparable harm, any dispute as to the interpretation, enforcement, breach, or termination of these Terms will be settled by binding arbitration under the Rules of Singapore International Arbitration Center ("SIAC Rules") by three arbitrators appointed in accordance with the SIAC Rules. The place of arbitration shall be Singapore. The language of proceedings shall be English. Judgment upon the award rendered by the arbitrators may be entered in any court of competent jurisdiction. The prevailing party

will be entitled to receive from the other party its reasonable attorneys' fees and costs incurred in connection with any arbitration or litigation instituted in connection with these Terms.

(i) Remedies Cumulative. The remedies provided to the parties under these Terms are cumulative and will not exclude any other remedies to which a party may be lawfully entitled.

(j) Waiver and Severability. The waiver by either party of any breach of these Terms does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation under these Terms will not be a waiver of such party's right to demand strict compliance in the future, nor will the same be construed as a novation of these Terms. If any part of these Terms is unenforceable, the remaining portions of these Terms will remain in full force and effect.

(k) Entire Agreement. These Terms are the final and complete expression of all agreements between these parties and supersedes all previous oral and written agreements regarding these matters.

(l) No Third Party Rights. No one other than a party to these Terms, their successors and permitted assignees, will have any right to enforce any of its terms.

(m) Costs. Partner will bear the entire cost, taxes, and expense incurred in connection with its performance of these Terms.

# Tencent Cloud International Data Processing Agreement (with Second-Level Resellers)

最近更新时间：2024-03-04 16:08:18

If you have (a) registered as a Second-Level Reseller under the Tencent Cloud Second-Level Reseller Terms (“**Tencent Cloud Reseller Terms**”) and Conditions and (b) entered into a Reseller Agreement with the Authorized Tencent Cloud Distributor (whether or not involving integration services), this Data Processing Agreement (“**DPA**”) applies to any processing of Personal Data in connection with such Tencent Cloud Reseller Terms. In the event of any conflict between this DPA, the Tencent Cloud Reseller, Reseller Agreement, Console Documentation and Purchase Order, this DPA shall prevail to the extent of the inconsistency. References to “Second-Level Reseller” and “Tencent” in this DPA have the same meaning as set out in the Tencent Cloud Reseller Terms.

**Now it is hereby agreed** as follows:

## 1. Definitions

**1.1** Capitalised terms shall have the meaning given to them in the Tencent Cloud Reseller Terms, unless otherwise defined below:

“**Personal Data**”, “**Special Categories of Data/Sensitive Data**”, “**Process/Processing**”, “**Controller**”, “**Processor**”, and “**Data Subject**” shall have the same meaning as in the relevant Applicable Data Protection Laws. “**Applicable Data Protection Law**” shall mean:

- a. the General Data Protection Regulation 2016/679 (the “**GDPR**”);
- b. the Privacy and Electronic Communications Directive 2002/58/EC;
- c. the UK Data Protection Act 2018 (“**DPA**”), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (“**UK GDPR**”), and the Privacy and Electronic Communications Regulations 2003;
- d. the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq. as amended by the California Privacy Rights Act of 2020, Cal. Civil Code § 1798.100 et seq. (collectively, “**CCPA**”), the Virginia Consumer Data Protection Act (“**VCDPA**”), the Colorado Privacy Act (“**CPA**”), Connecticut Data Privacy Act (“**CDPA**”), Utah Consumer Privacy Act (“**UCPA**”), Iowa Consumer Data Protection Act (“**ICDPA**”), Indiana Consumer Data Protection Act (“**INCDPA**”), Montana Consumer Data Privacy Act (“**MCDPA**”), Tennessee Information Protection Act (“**TIPA**”), Texas Data Privacy and Security Act (“**TDPSA**”), Oregon Consumer Privacy Act (“**OCPA**”), Florida Digital Bill of Rights (“**FDBR**”) (collectively, “**Applicable US Data Protection Law**”); and
- e. any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

“**Data Discloser**” means the Party who transfers Personal Data to the other Party.

**“Data Receiver”** means the Party who receives Personal Data from the Data Discloser for Processing in accordance with the terms of this Agreement.

**“Lawful Export Measure”** means a method allowing for the lawful transfer of Personal Data from a data exporter to a data importer, as may be stipulated by Applicable Data Protection Law or a Regulator from time to time, which may include (depending upon the Applicable Data Protection Laws) model transfer terms prescribed by Applicable Data Protection Laws; or prior registration, licensing or permission from a Regulator.

**“Party”** means a party to this DPA.

**“Partner Console”** means the area designated as console in the Tencent Cloud portal at <http://www.tencentcloud.com>.

**“Personal Data Breach”** means any improper, unauthorised or unlawful access to, use of, or disclosure of, or any other compromise which affects the availability, integrity or confidentiality of Personal Data.

**“Member State”** means the member states of the European Union from time to time.

**“Regulator”** means the data protection supervisory authority which has jurisdiction over a Party's Processing of Personal Data.

**“Relevant Data Export”** means:

- a. a transfer of Personal Data:
  - i. from a Party which is subject to Applicable Data Protection Law in respect of that Personal Data;
  - ii. to another Party that is in a Third Country or a territory which otherwise (but for the operation of this DPA) does not offer an adequate level of protection as required by Applicable Data Protection Law; and
  - iii. which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law; and
- b. the onward transfer of Personal Data pursuant to (a) to a Third Country or a territory which otherwise (but for the operation of this DPA) does not offer an adequate level of protection as required by Applicable Data Protection Law and which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law.

**“Security Standards”** shall mean the technical and organisational security measures set out in Schedule C.

**“Standard Contractual Clauses”** means:

- a. in the case of transfers of Personal Data relating to Data Subjects in the European Economic Area (“EEA”), the standard contractual clauses for the transfer of Personal Data to data processors established in third countries set out in the Commission Decision of 4 June 2021 (C(2021) 3972), as amended and restated from time to time;
- b. in relation to transfers of Personal Data from the UK, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, and in each case as amended, updated or replaced from time to time, as attached to and incorporated into this DPA to cover Personal Data transfers to Controllers or Processors as applicable established in Third Countries which do not ensure an adequate level of data protection; and
- c. in each case, as amended, updated or replaced from time to time, as attached and incorporated into this DPA to cover Personal Data transfers to Controllers or Processors, as applicable, established in Third Countries which do not ensure an adequate level of data protection.



“**Tencent Cloud Reseller Terms**” means the Tencent Cloud Second-Level Reseller Terms and Conditions in place between Tencent and the Second-Level Reseller.

“**Third Country**” means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time; and (iii) in relation to Personal Data transfers from any other jurisdiction, any country other than those approved as providing adequate protection for Personal Data by the relevant competent authority of such country from time to time.

**1.2** References to a statutory provision include any subordinate legislation made from time to time under that provision.

**1.3** References to this DPA include the Schedules.

**1.4** Headings shall be ignored in construing this DPA.

**1.5** If a word or phrase is defined, its other grammatical forms have a corresponding meaning.

**1.6** The words “include”, “includes” and “including”, and any succeeding words shall be construed without limitation to the generality of any preceding words or concepts.

**1.7** If there is any inconsistency between the Clauses and Schedules to this DPA the Clauses shall take precedence.

# SCOPE OF THIS AGREEMENT

## 2. General

**2.1** This DPA governs the transfer of Personal Data between Tencent and Second-Level Reseller. This DPA is divided into the following sections:

- a. Module A (Transfers between Controllers) sets forth the terms governing any transfer (including a Relevant Data Export) between the Parties, each acting as an independent Data Controller;
- b. Module B (Transfers from a Data Controller to a Data Processor) sets forth the terms governing any transfer (including a Relevant Data Export) from Second-Level Reseller (acting as a Data Controller) to Tencent (acting as a Data Processor);
- c. Module C (Transfers from a Data Processor to a Data Controller) sets forth the terms governing any transfer (including a Relevant Data Export) from Second-Level Reseller (acting as a Data Processor) to Tencent (acting as a Data Controller).



# MODULE A – TRANSFERS BETWEEN DATA CONTROLLERS

## 3. APPLICATION OF THIS MODULE A

**3.1** The Parties agree that this Module A applies in each case and only where Personal Data is transferred from Data Discloser to Data Receiver, in circumstances where each Party is acting as an independent Data Controller.

**3.2** The details of the transfers covered by this Module A are specified in Schedule B which forms an integral part of this Module A.

**3.3** In the case of a Relevant Data Export to a Third Country, clause 7 shall govern the terms of the transfer and clauses 4, 5 and 6 shall not apply.

## 4. OBLIGATIONS OF BOTH PARTIES

**4.1** Each Party shall:

- a. Process Personal Data fairly and lawfully;
- b. ensure that Personal Data is accurate and up to date, and inform the other without undue delay if it becomes aware that any of the Personal Data is inaccurate or out of date;
- c. provide reasonable assistance as necessary to the other to enable them to comply with subject access requests and to respond to any other queries or complaints from Data Subjects;
- d. carry out any reasonable request from the other to amend, transfer or delete any Personal Data (to the extent applicable); and
- e. notify the other promptly about any enquiries from a Regulator in relation to Personal Data and cooperate promptly and thoroughly with such Regulator, to the extent required under Applicable Data Protection Law.

## 5. OBLIGATIONS OF DATA DISCLOSER

**5.1** The Data Discloser warrants and undertakes that:

- a. Personal Data have been collected, Processed, and transferred in accordance with Applicable Data Protection Laws, as applicable to the Data Discloser;
- b. it has obtained all consents, authorizations, approvals and rights and provided all notices necessary, including as required by Applicable Data Protection Law, to provide the Personal Data to the Data Receiver and permit the Data Receiver to use the Personal Data in accordance with this DPA;

- c. it has used reasonable efforts to determine that the Data Receiver is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Module A;
- d. it has taken all steps required by Applicable Data Protection Law to avoid “selling” Personal Data to Data Receiver under this Module A (as defined in such laws), including transferring Personal Data at the direction of the relevant individual, or otherwise taken all steps required to comply with obligations relating to “selling” under such Applicable Data Protection Law;
- e. the Data Discloser shall provide a copy of this Module A and associated Schedules to the Regulator where required.

## 6. OBLIGATIONS OF DATA RECEIVER

### 6.1 Data Receiver warrants and undertakes that:

- a. it will comply with all relevant obligations of Applicable Data Protection Law, including by providing the same level of privacy protections required of controllers and businesses by Applicable Data Protection Law;
- b. it will have in place appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the data to be protected including those in the Security Standards, and shall ensure that those measures continue to provide an appropriate level of security;
- c. in the event of a Personal Data Breach, it shall take appropriate measures to address the Personal Data Breach, and shall (if the breach is likely to result in a risk to individuals) notify the Data Discloser and cooperate with the Data Discloser in relation to any required notifications to the Regulator and/ or to relevant Data Subjects.
- d. it will have in place procedures so that any third party it authorises to have access to Personal Data, including Data Processors, will respect and maintain the confidentiality and security of Personal Data. Any person acting under the authority of the Data Receiver, including a Data Processor, shall be obligated to Process Personal Data only on instructions from the Data Receiver. This provision does not apply to persons authorised or required by law or regulation to have access to Personal Data;
- e. it shall notify the Data Receiver promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The Data Receiver shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. The Data Receiver will provide relevant information about disclosure requests to the Data Discloser, including in relation to its legality review and any challenges to the request;
- f. it will inform the Data Discloser if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Module A;
- g. it will Process Personal Data for purposes described in Schedule B (*Description of Transfer*), and has the legal authority to give the warranties and fulfil the undertakings set out in this Module A;

- h. it shall put in place appropriate technical or organisational measures in order to retain Personal Data for no longer than necessary for the purposes for which it is processed; and
- i. it will keep appropriate documentation of the Processing it carries out under this Module A, and shall make such documentation available to the relevant Regulator(s).

## 7. EXPORT OF PERSONAL DATA

**7.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 1: Controller to Controller, set out in Schedule D-1, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser, who shall comply with the data exporter’s obligations set out in Schedule D-1, and the applicable Data Receiver, who shall comply with the data importer’s obligations set out in Schedule D-1, for that particular transfer of Personal Data for that particular transfer of Personal Data. In relation to any onward transfer of such Personal Data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 1: Controller to Controller set out in Schedule D-1; or (ii) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E, in respect of that Personal Data.

**7.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser. In relation to any onward transfer of such Personal Data by the Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the obligations set out in the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses set out in Schedule D-2, in respect of that Personal Data.

**7.3** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure,. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply mutatis mutandis for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another data importer, the receiving data importer shall comply with the same data importer obligations.

# MODULE B – TRANSFERS FROM DATA CONTROLLER TO DATA PROCESSOR

## 8. APPLICATION OF THIS MODULE B

**8.1** The Parties agree that this Module B applies in each case and only where Personal Data is transferred from Second-Level Reseller (acting as a Data Controller) to Tencent (acting as a Data Processor).

**8.2** The details of the transfers (as well as the Personal Data) covered by this Module B are specified in Schedule B which form an integral part of this Module B.

**8.3** In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, as relevant, clause 12 shall govern the terms of the transfer and clauses 9, 10 and 11 shall not apply.

**8.4** Nothing in this DPA shall relieve Second-Level Reseller or Tencent of liabilities imposed by virtue of their roles in the Processing relationship.

## 9. OBLIGATIONS OF SECOND-LEVEL RESELLER

**9.1** Second-Level Reseller agrees and warrants that:

- a. it has used reasonable efforts to determine that Tencent is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Module B;
- b. it has obtained all consents, authorizations, approvals and rights and provided all notices necessary, including as required by Applicable US Data Protection Law, to provide the Personal Data to Tencent and permit Tencent to use the Personal Data in accordance with this DPA;
- c. it has disclosed Personal Data to Tencent for the limited purposes set forth in Schedule B; and
- d. the Processing, including the transfer itself, of Personal Data has been and will continue to be carried out in accordance with the relevant provisions of Applicable Data Protection Law (and, where applicable, has been notified to the relevant authorities of the country in which Second-Level Reseller is established).

**9.2** Second-Level Reseller warrants that it has no reason to believe that any applicable local laws, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent Tencent from fulfilling its obligations under this Module B.

## 10. OBLIGATIONS OF TENCENT

**10.1** Tencent agrees and warrants that it will:

- a. Process Personal Data only on documented instructions of Second-Level Reseller and this DPA for the limited purposes set forth in Schedule B and in compliance with Applicable US Data Protection Law;
- b. not retain, use or disclose Personal Data (i) outside of the direct business relationship between Second-Level Reseller and Tencent or as otherwise permitted by Applicable Data Protection Law, or (ii) for any purpose other than for the limited purposes set forth in Schedule B;
- c. not combine Personal Data received from or on behalf of Second-Level Reseller with any Personal Data that may be collected from Tencent's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Applicable Data Protection Law;
- d. ensure that persons authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- e. take all technical and organisational security measures required by Applicable Data Protection Law relating to data security, and shall ensure that those measures continue to provide an appropriate level of security;
- f. taking into account the nature of the Processing, assist Second-Level Reseller by implementing appropriate technical and organisational measures, insofar as this is practicable, for the fulfilment of Second-Level Reseller's obligation to respond to requests for exercising the Data Subject's rights laid down in Applicable Data Protection Law;
- g. notify (as applicable) and assist Second-Level Reseller in ensuring compliance with data security, Personal Data Breach, data protection impact assessments, and engaging in other consultations, pursuant to Applicable Data Protection Law, taking into account the nature of Processing and the information available to Tencent;
- h. inform Second-Level Reseller if it becomes aware that any of Personal Data is inaccurate or out of date, and cooperate with Second-Level Reseller to erase or rectify the relevant Personal Data;
- i. notify Second-Level Reseller promptly if Tencent makes a determination that it can no longer meet its obligations under Applicable US Data Protection Law;
- j. permit Second-Level Reseller to take reasonable and appropriate steps to help ensure that Tencent uses Personal Data in a manner consistent with Second-Level Reseller's obligations under Applicable US Data Protection Law and stop and remediate any unauthorized use of Personal Data;
- k. notify Second-Level Reseller promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. Tencent shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. Tencent will provide relevant information about disclosure requests to Second-Level Reseller, including in relation to its legality review and any challenges to the request;
- l. inform Second-Level Reseller if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Module B; and
- m. keep appropriate documentation of the Processing it carries out under this Module B, and make available to Second-Level Reseller (and any relevant Regulator) information sufficient to demonstrate compliance with Applicable Data Protection Law and allow for and contribute to audits, including inspections, conducted by Second-Level Reseller.

## 11. SUB-CONTRACTING

**11.1** Tencent may authorize any sub-processor to Process the Personal Data on its behalf provided that, where (and to the extent) required by Applicable Data Protection Laws, Tencent enters into a written agreement with the sub-processor containing terms which are substantially the same as those contained in this DPA. Second-Level Reseller hereby grants Tencent general written authorisation to engage sub-processors listed at <https://www.tencentcloud.com/services/thirdParties>. Tencent shall, to the extent required by Applicable Data Protection Laws, inform Second-Level Reseller of any intended changes concerning the addition or replacement of the sub-processors. In such a case, Second-Level Reseller will have fourteen (14) days from the date of receipt of the notice to approve or reject the change. In the event of no response from Second-Level Reseller, the sub-processor will be deemed accepted. If Second-Level Reseller rejects the replacement sub-processor, Tencent may terminate the DPA with immediate effect on written notice to Second-Level Reseller. Tencent shall remain fully responsible to Second-Level Reseller for the performance of any sub-processor's obligations under its contract with the Second-Level Reseller.

## 12. EXPORT OF PERSONAL DATA

**12.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between Second-Level Reseller and Tencent for that particular transfer of Personal Data.

**12.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between Second-Level Reseller and Tencent for that particular transfer of Personal Data.

**12.3** In relation to any onward transfer of the Personal Data by Tencent to another party, Tencent shall comply with the relevant obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E; or (ii) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2.

**12.4** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in

Schedule C, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations.

## MODULE C – TRANSFERS FROM A DATA PROCESSOR TO A DATA CONTROLLER

### 13. APPLICATION OF THIS MODULE C

**13.1** The Parties agree that this Module C applies in each case and only where Personal Data is transferred from Second-Level Reseller (acting as a Data Processor) to Tencent (acting as a Data Controller).

**13.2** The details of the transfers (as well as Personal Data) covered by this Module C are specified in Schedule B which form an integral part of this Module C.

**13.3** In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, clause 15 shall govern the terms of the transfer and clause 14 shall not apply.

### 14. OBLIGATIONS OF SECOND-LEVEL RESELLER

**14.1** Second-Level Reseller shall comply with the terms of clause 10 of Module B, and references to “Tencent” shall be read as a reference to “Second-Level Reseller”, and references to “Second-Level Reseller” shall be read as references to “Tencent”, for such purposes, in relation to any such Processing.

**14.2** Before Processing Personal Data, Second-Level Reseller shall implement, and ensure that its authorised personnel comply with, appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as well as ensuring that those measures continue to provide an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing as set out in Schedule C, or otherwise agreed and documented between Tencent and Second-Level Reseller from time to time, and shall continue to comply with them during the term of this DPA. Such measures shall include, as appropriate to the risk:

- a. the pseudonymisation and encryption of Personal Data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and



d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

**14.3** In the event that Second-Level Reseller directly receives a request from a Data Subject regarding Data Subject's Personal Data, or for the rectification or erasure of such Personal Data, or any other request or query from a Data Subject relating to its own Personal Data (including Data Subjects' exercising rights under Applicable Data Protection Laws, such as rights of objection, restriction of processing, data portability or the right not to be subject to automated decision making) (a "**Data Subject Request**"), Second-Level Reseller will:

- a. notify Tencent immediately of the Data Subject Request (without responding to that Data Subject Request, unless it has been otherwise authorised by Tencent to do so);
- b. provide details of the Data Subject Request (and any other relevant information Tencent may reasonably request) to Tencent within 3 business days of receipt of the Data Subject Request; and
- c. provide such assistance to Tencent as Tencent may require for the purposes of responding to the Data Subject Request and to enable Tencent to comply with all obligations which arise as a result thereof.

**14.4** In the event there is, or Second-Level Reseller reasonably believes that there is, any Personal Data Breach in respect of Personal Data which is Processed by Second-Level Reseller under or in connection with this DPA, then upon becoming aware of such Personal Data Breach, Second-Level Reseller shall:

- a. immediately notify Tencent in writing of all known details of the Personal Data Breach relating to the Personal Data, including:
  - i. a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects and records concerned;
  - ii. the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - iii. a description of the likely consequences of the Personal Data Breach; and
  - iv. a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;
- b. provide Tencent with regular status updates on any Personal Data Breach (including actions taken to resolve the incident) and share additional information related to the breach as soon as more details become available;
- c. mitigate any harmful effect that is known to Second-Level Reseller of a use or disclosure of the Personal Data in violation of this DPA or in connection with a Personal Data Breach;
- d. assist Tencent in remediating or mitigating any potential damage from a Personal Data Breach.
- e. within 4 weeks of closure of the incident, provide Tencent a written report describing the Personal Data Breach, the root cause analysis, actions taken by Second-Level Reseller during its response and Second-Level Reseller's plans for future actions to prevent a similar Personal Data Breach from occurring;
- f. not disclose to third parties (including Regulators) any information about a Personal Data Breach involving the Personal Data without prior written and express permission from Tencent for such disclosure; and
- g. assist Tencent with notifying the Personal Data Breach to any Regulator or the Data Subject in accordance with, and in the timeframe required by, the Applicable Data Protection Laws.



**14.5** Second-Level Reseller shall not subcontract to any third party any of its obligations to Process Personal Data under this Module C unless all of the following provisions of this clause have first been complied with:

- a. Second-Level Reseller has supplied to Tencent such information as that Tencent may require to ascertain that such subcontractor has the ability to comply with Second-Level Reseller's obligations set out in this DPA and with Tencent's instructions;
- b. Second-Level Reseller has obtained the prior written consent of Tencent; and
- c. the proposed subcontractor has entered into a contract with Second-Level Reseller which requires the subcontractor to take adequate technical and organisational measures to safeguard the security and integrity of the relevant Personal Data and only Process data in accordance with the documented instructions of Tencent (including as set out in such contract with the proposed subcontractor), and which contains obligations on the relevant subcontractor which are no less onerous than the obligations on the Second-Level Reseller in, and which is no less protective of the Personal Data than, the terms of this DPA. The Second-Level Reseller shall provide, at Tencent's request, a copy of such subcontractor contract, and subsequent amendments, to Tencent.

**14.6** In the event that Tencent consents to subcontracting the Processing of Personal Data, Second-Level Reseller remains liable for the Processing under the terms of this DPA. The Second-Level Reseller shall notify Tencent of any failure by a subcontractor to fulfil its obligations under the relevant subcontractor contract.

**14.7** Second-Level Reseller will not, without the consent of Tencent, either:

- a. Process Personal Data in any Third Country; or
- b. permit any third party including its subcontractors to Process Personal Data in any Third Country.

**14.8** Second-Level Reseller shall permit Tencent at any time upon seven (7) days' notice, to be given in writing, to have access to the appropriate part of Second-Level Reseller's premises, systems, equipment, and other materials and data Processing facilities to enable Tencent (or its designated representative) to inspect or audit the same for the purposes of monitoring compliance with Second-Level Reseller's obligations under this DPA. Such inspection shall:

- a. be carried out by Tencent or an inspection body composed of independent members and in possession of the required professional qualifications and bound by a duty of confidentiality, selected by Tencent, where applicable, in agreement with the Regulator; and
- b. not relieve Second-Level Reseller of any of its obligations under this DPA.

## 15. EXPORT OF PERSONAL DATA

**15.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 4 : Processor to Controller set out in Schedule F, which incorporate the provisions of Schedule B, and which together will form contractual terms between Tencent and Second-Level Reseller for that particular transfer of Personal Data.

**15.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which

together will form contractual terms between Second-Level Reseller and Tencent for that particular transfer of Personal Data.

**15.3** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations.

## MISCELLANEOUS (APPLICABLE TO ALL MODULES)

### 16. COOPERATION WITH REGULATORS

**16.1** The Parties agree that they shall and, where applicable, shall procure that their representatives shall cooperate, on request, with any relevant Regulator in the performance of its tasks pursuant to Applicable Data Protection Law.

### 17. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR A REGULATOR

In respect of any action or omission under this DPA:

- a. in the event of a dispute or claim brought by a Data Subject or a Regulator concerning the Processing of Personal Data against Tencent, Second-Level Reseller will inform Tencent about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion;
- b. Second-Level Reseller agrees to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by a Regulator. If they do participate in the proceedings, Second-Level Reseller may elect to do so remotely (such as by telephone or other electronic means); and
- c. each Party shall abide by a decision, as applicable, of a competent court of Tencent's country of establishment; of a competent court of the relevant Data Subject's country of habitual residence; or of the Regulator which is final and

against which no further appeal is possible.

## 18. LIABILITY

**18.1** Without prejudice to any other rights or remedies that Tencent may have, Second-Level Reseller hereby acknowledges and agrees that a person with rights under this DPA may be irreparably harmed by any breach of its terms and that damages alone may not be an adequate remedy. Accordingly, a person bringing a claim under this DPA shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this DPA.

**18.2** Second-Level Reseller agrees that it will (in addition to, and without affecting, any other rights or remedies that Tencent may have whether under statute, common law or otherwise) indemnify, defend and hold harmless Tencent, its affiliates, and their respective employees, officers and directors (the "Tencent Parties") on demand from and against all claims, liabilities, costs, expenses, loss or damage incurred by a Tencent Party (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) arising directly or indirectly from a breach of Applicable Data Protection Law or this DPA by Second-Level Reseller or enforcement of any rights under it.

## 19. TERMINATION

**19.1** Termination of this DPA shall be governed by the applicable provisions in the relevant provisions in the Tencent Cloud Reseller Terms.

**19.2** Upon termination of this DPA:

- a. each Party shall, except to the extent it acts as a Data Controller of such Personal Data, at the other Party's option, either forthwith:
  - i. return all of the Personal Data and any copies thereof which it is Processing or has Processed upon behalf of that Party. The return of the Personal Data shall result in the full deletion of the Personal Data existent in the IT equipment and systems used by the Party; or
  - ii. destroy all of the Personal Data and any copies thereof which it has Processed on behalf of that Party promptly and in any case within 14 days of being requested to do so by that Party. The Party shall certify the deletion of such data in writing to the other Party; and
  - iii. cease Processing Personal Data on behalf of the other Party under this DPA.

## 20. MISCELLANEOUS

Applicable clauses in relation to Assignment, Variation, Further Assurance, Invalidity, Waiver and Notices of the applicable Tencent Cloud Reseller Terms shall apply *mutatis mutandis* to this DPA.

## 21. SERVICE-SPECIFIC TERMS

The Parties agree that certain Additional Terms may apply to certain services provided by or on behalf of Tencent from time to time in connection with the Tencent Cloud Reseller Terms, and that such Additional Terms shall be deemed to be incorporated into this DPA.

## 22. ENTIRE AGREEMENT

These terms are the final and complete expression of all agreements between Second-Level Reseller and Tencent regarding Processing of Personal Data and supersede all prior oral and written agreements regarding these matter. In the event of any conflict between this DPA or the Tencent Cloud Reseller Terms, this DPA shall prevail to the extent of the inconsistency solely to the extent such inconsistency relates to the Processing of Personal Data or any Applicable Data Protection Law.

## 23. COUNTERPARTS

This DPA may be entered into in any number of counterparts, all of which taken together shall constitute one and the same instrument.

## 24. GOVERNING LAW

**24.1** Subject to clause 24.2, this DPA shall be governed by Singapore law.

**24.2** The law governing Module A (Transfers between Data Controllers), 2 (Transfers from a Data Controller to a Data Processor), in respect of each transfer, be the law of the country in which the Data Discloser is established. The law governing Section 3 (Transfers from a Processor to a Controller) of this DPA shall, in respect of each transfer, be the law of the country in which the Data Receiver is established.

**24.3** Any dispute shall be referred to, and finally resolved by, arbitration administered by the Singapore International Arbitration Centre in accordance with the Arbitration Rules of the Singapore International Arbitration Centre for the time being in force when the notice of arbitration is submitted. The tribunal shall consist of one arbitrator. The seat of arbitration shall be Singapore and the language to be used in the arbitral proceedings shall be English.

## SCHEDULE A: LIST OF PARTIES

### Module A (Transfers between Controllers)

#### Data Exporter and Importer(s) - Tencent:

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Second-Level Reseller is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Second-Level Reseller is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Second-Level Reseller is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Second-Level Reseller is located in the rest of the world except People's Republic of China

Contact: cloudlegalnotices@tencent.com

Activities relevant to the data transferred under these Clauses: Cloud service provider Role

(controller/processor): Controller

#### Data Exporter and Importer(s) – Second-Level Reseller:

Name: The relevant entity that entered into the Tencent Cloud Reseller Terms with Tencent

Address: The address provided to Tencent when signing up to act as a reseller of Tencent cloud services. Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Reseller of Tencent Role (controller/processor): Controller

### Module B (Transfers from a Data Controller (Second-Level Reseller) to a Data Processor (Tencent))

#### Data exporter(s) –Second-Level Reseller:

Name: The relevant Party that entered into the Tencent Cloud Reseller Terms with Tencent, who acting as Data Controller transfers Personal Data to Tencent.

Address: The address provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Second-Level Reseller of Tencent Role (controller/processor): Controller

**Data importer(s) –Tencent:**

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Second-Level Reseller is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Second-Level Reseller is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Second-Level Reseller is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Second-Level Reseller is located in the rest of the world except People's Republic of China

Contact: cloudlegalnotices@tencent.com

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor): Processor

**Module C (Transfers from a Data Processor (Second-Level Reseller) to a Data Controller (Tencent))****Data exporter(s) –Second-Level Reseller:**

Name: The relevant Party that entered into the Tencent Cloud Reseller Terms with Tencent.

Address: The address provided to Tencent when signing up to act as a second-level reseller of Tencent cloud services.

Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Second-Level Reseller of Tencent

Role (controller/processor): Processor

**Data importer(s) –Tencent:**

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Second-Level Reseller is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Second-Level Reseller is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Second-Level Reseller is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Second-Level Reseller is located in the rest of the world except People's Republic of China

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor): Controller

## SCHEDULE B: DESCRIPTION OF TRANSFERS

*Categories of data subjects whose personal data is transferred*

Individuals employed by or representing the Second-Level Reseller

End Users(s), End Customers

*Categories of personal data transferred*

**Individuals employed by or representing the Second-Level Reseller:** name, job title, mobile phone, email address

**End Users(s), End Customers:** Name, Email address, address, country, business registration number (and photo), job title, mobile number, payment details (bank name, account name, bank account, swift code), invoice information (Payer Account ID, Owner Account ID, Operator Account ID), and any other personal data made available by or on behalf of Second-Level Reseller/Second-Level Reseller's End User(s), or otherwise accessible directly or indirectly via the Partner Console.

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

No sensitive personal data transferred

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

For the duration of the DPA

*Nature of the processing*

Second-Level Reseller will act as a reseller of Tencent cloud services for certain End Users. Second-Level Reseller shall administer and manage Resell activities relating to its End Users and Second-Level Resellers through the functions and tools provided through Partner Console or via other processes authorized or designated by Tencent and this will involve processing personal data.

*Purpose(s) of the data transfer and further processing*

To facilitate the Reselling of Tencent Services by the Second-Level Reseller, including (without limitation and in each case to the extent the relevant services, features, support or functions are provided):

making available or accessible, directly or indirectly, Personal Data via the Partner Console

provision of integrated / value-added services by the Second-Level Reseller to its customers (if applicable)

customer account creation via email invite sent by Second-Level Reseller on the Tencent Cloud console

placement of orders / Purchase Orders for Tencent Services

fulfilment of orders / Purchase Orders (i.e. performance of Tencent Services)

access to online training materials and support from Tencent

access to dedicated online documents and support from Tencent

assigning dedicated solution architect(s) for support

participation in Tencent's marketing activities (details subject to Tencent's approval)

joint case study opportunities (details subject to Tencent's agreement)

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

The retention period will follow the data retention policy as set out in the Privacy Policy on the Tencent website.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

N/A

*Identify the competent supervisory authority/ies in accordance with Clause 13 of Schedules D, E and F*

The Netherlands

## SCHEDULE C: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Where applicable this Schedule C also forms part of the Standard Contractual Clauses.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. **Data security.** The data importer shall design and implement the following measures to protect customer's data against unauthorized access:  
standards for data categorisation and classification;  
a set of authentication and access control capabilities at the physical, network, system and application levels; and  
a mechanism for detecting big data-based abnormal behaviour.
2. **Network security.** The data importer shall implement stringent rules on internal network isolation to achieve access control and border protection for internal networks (including office networks, development networks, testing networks and production networks) by way of physical and logical isolation.
3. **Physical and environmental security.** Stringent infrastructure and environment access controls shall be implemented for data centers based on relevant regional security requirements. An access control matrix is established, based on the types of data center personnel and their respective access privileges, to ensure effective management and control of access and operations by data center personnel.
4. **Incident management.** The data importer shall operate active and real-time service monitoring, combined with a rapid response and handling mechanism, that enables prompt detection and handling of security incidents.



**5. Compliance with standards.** The data importer shall comply with the standards listed in Tencent's Compliance Center page, and as updated from time to time.

## SCHEDULE D-1: STANDARD CONTRACTUAL CLAUSES

### MODULE 1: CONTROLLER TO CONTROLLER TRANSFER

#### Section I

##### Clause 1: Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### Clause 2: Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

##### Clause 3: Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

- ii. Clause 8 - Clause 8.5 (e) and Clause 8.9(b);
  - iii. Clause 12 - Clause 12(a) and (d);
  - iv. Clause 13;
  - v. Clause 15.1(c), (d) and (e);
  - vi. Clause 16(e);
  - vii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### **Clause 4: Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **Section II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- i. where it has obtained the data subject's prior consent;

- ii. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iii. where necessary in order to protect the vital interests of the data subject or of another natural person.

## 8.2 Transparency

- a. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
  - i. of its identity and contact details;
  - ii. of the categories of personal data processed;
  - iii. of the right to obtain a copy of these Clauses;
  - iv. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- b. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- c. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- d. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

## 8.3 Accuracy and data minimisation

- a. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- b. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- c. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

## 8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

## 8.5 Security of processing

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- b. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- c. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- d. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- e. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- f. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- g. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

## 8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter “sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted

to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

#### **8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- i. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### **8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

#### **8.9 Documentation and compliance**

- a. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- b. The data importer shall make such documentation available to the competent supervisory authority on request.

#### **Clause 9: Use of sub-processors Clause 10: Data subject rights**

- a. The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of

data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

b. In particular, upon request by the data subject the data importer shall, free of charge:

i. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

ii. rectify inaccurate or incomplete data concerning the data subject;

iii. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

c. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

d. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the law of the country of destination, provided that such law lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

i. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

ii. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

e. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

f. The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

g. If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

#### **Clause 11: Redress**

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
- i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

### **Clause 12: Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

### **Clause 13: Supervision**

- a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which



the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### **Clause 14: Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as



a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### **15.2 Review of legality and data minimisation**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **Section IV – FINAL PROVISIONS**

##### **Clause 16: Non-compliance with the Clauses and termination**

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - ii. the data importer is in substantial or persistent breach of these Clauses; or
  - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data

importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17: Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands (*specify Member State*).

#### **Clause 18: Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of The Netherlands (*specify Member State*).
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

### **APPENDIX TO SCHEDULE D-1 (SCCS MODULE 1)**

#### **ANNEX I**

##### **A. LIST OF PARTIES**

See Schedule A to the DPA

##### **B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA

##### **C. COMPETENT SUPERVISORY AUTHORITY**

See Schedule B to the DPA

#### **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

See Schedule C to the DPA

## **SCHEDULE D-2: INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES**

This Addendum has been issued by the UK Information Commissioner’s Office for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## PART 1: TABLES

**TABLE 1: PARTIES**

<b>Start date</b>	<b>See effective date of the DPA</b>	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties’ details</b>	<b>See Schedule A of the DPA</b>	
<b>Key Contact</b>	<b>See Schedule A of the DPA</b>	

**TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES**

<b>AddendumEU SCCs</b>	<b>The Approved EU SCCs, including the Appendix Information, set out in Schedule D-1, Schedule E or Schedule F to the DPA, as applicable</b>
------------------------	--

**TABLE 3: APPENDIX INFORMATION**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Schedule A to the DPA	
Annex 1B: Description of Transfer: See Schedule B to the DPA	
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: <b>See Schedule C to the DPA</b>	
Annex III: List of Sub processors (Modules 2 and 3 only): <b>N/A</b>	

**TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES**

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Neither Party
---	---

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

<b>Addendum</b>	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
<b>AddendumEU SCCs</b>	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
<b>Appendix Information</b>	As set out in Table 3.
<b>Appropriate Safeguards</b>	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
<b>Approved Addendum</b>	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022.
<b>ApprovedEU SCCs</b>	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
<b>ICO</b>	The Information Commissioner.
<b>Restricted Transfer</b>	A transfer which is covered by Chapter V of the UK GDPR.
<b>UK</b>	The United Kingdom of Great Britain and Northern Ireland.
<b>UK Data Protection Laws</b>	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
<b>UK GDPR</b>	As defined in section 3 of the Data Protection Act 2018.

4 .This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5 .If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6.If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7.If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8 .Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

#### **Hierarchy**

9 .Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10 .Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

#### **Incorporation of and changes to the EU SCCs**

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13.Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14.No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;

c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

d. Clause 8.7(i) of Module A is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.



#### Amendments to this Addendum

**16.**The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

**17.**If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

**18.**From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

**19.**If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a. its direct costs of performing its obligations under the Addendum; and/or
- b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

## SCHEDULE E: STANDARD CONTRACTUAL CLAUSES

### MODULE 2: CONTROLLER TO PROCESSOR TRANSFER

#### Section I

#### Clause 1: Purpose and scope



- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- b. The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## **Clause 2: Effect and invariability of the Clauses**

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

## **Clause 3: Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - iii. Clause 9 - Clause 9(a), (c), (d) and (e);
  - iv. Clause 12 - Clause 12(a), (d) and (f);
  - v. Clause 13;
  - vi. Clause 15.1(c), (d) and (e);
  - vii. Clause 16(e);
  - viii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

## **Clause 4: Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **Section II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Instructions**

- a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

##### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

##### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible

without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its

adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

- a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

#### **Clause 9: Use of sub-processors**

a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least twenty business days' in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### **Clause 10: Data subject rights**

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the

appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **Clause 11: Redress**

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

ii. refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### **Clause 12: Liability**

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an



action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13: Supervision**

a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

### **Clause 14: Local laws and practices affecting compliance with the Clauses**

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the

categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the



importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **Section IV – FINAL PROVISIONS**

### **Clause 16: Non-compliance with the Clauses and termination**

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- ii. the data importer is in substantial or persistent breach of these Clauses; or
- iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17: Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands.

#### **Clause 18: Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of The Netherlands (specify Member State).
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

## **APPENDIX TO SCHEDULE E (SCCS MODULE B)**

### **ANNEX I**

#### **A.LIST OF PARTIES**

See Schedule A to the DPA

## B. DESCRIPTION OF TRANSFER

See Schedule B to the DPA

## C. COMPETENT SUPERVISORY AUTHORITY

See Schedule B to the DPA

## ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Schedule C to the DPA

# SCHEDULE F: STANDARD CONTRACTUAL CLAUSES

## MODULE 4: PROCESSOR TO CONTROLLER TRANSFER

### Section I

#### Clause 1: Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

- i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### Clause 2: Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional

safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### **Clause 3: Third-party beneficiaries**

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- ii. Clause 8 - Clause 8.1 (b) and Clause 8.3(b);
- iii. Clause 15.1(c), (d) and (e);
- iv. Clause 16(e);
- v. Clause 18.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### **Clause 4: Interpretation**

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### **Clause 7: Docking clause**

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **Section II – OBLIGATIONS OF THE PARTIES**

### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### 8.1 Instructions

- a. The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- b. The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- c. The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- d. After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

### 8.2 Security of processing

- a. The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- b. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- c. The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 8.3 Documentation and compliance

- a. The Parties shall be able to demonstrate compliance with these Clauses.
- b. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

### **Clause 9: Use of sub-processors Clause 10: Data subject rights**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

### **Clause 11: Redress**

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it

receives from a data subject.

#### **Clause 12: Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

#### **Clause 13: Supervision**

### **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### **Clause 14: Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the



requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **Section IV – FINAL PROVISIONS**

### **Clause 16: Non-compliance with the Clauses and termination**

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.



In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17: Governing law**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands (*specify country*).

#### **Clause 18: Choice of forum and jurisdiction**

Any dispute arising from these Clauses shall be resolved by the courts of The Netherlands (*specify country*).

### **APPENDIX TO SCHEDULE F (SCCS MODULE 4)**

#### **ANNEX I**

##### **A. LIST OF PARTIES**

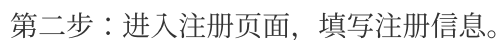
See Schedule A to the DPA

##### **B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA

最近更新时间：2022-03-29 16:10:05

第一步：进入腾讯云官网-[合作伙伴介绍页](#)，点击页面中【立即注册】按钮。



版权所有：腾讯云计算（北京）有限责任公司

第一步：登陆账号后，进入[企业实名认证流程](#)，填写企业认证相关信息，包括企业营业执照等。（注：营业执照是指由政府机构颁发的、允许公司在政府的地域管辖范围内开展业务的许可证。）

## Become a Tencent Cloud partner

### 01 Register for a Tencent Cloud account

Completed

### 02 Provide your basic information and submit an application

To become a Tencent Cloud partner, you need to complete enterprise identity verification first

### 03 Tencent Cloud reviews your application

After you submit an enterprise identity verification application, we will complete the review within 2–3 business days and notify you of the result through Message Center, email, and SMS

### 04 Become a Tencent Cloud partner

#### Company Operating Information

Registered Region \*

Albania

Company name \*

ZrCCCC

Please make sure your company name is exactly same to that on your certification you provided

Registered Address \*

Business Registration number or Tax number \*

Photo of Business Registration Document \*

Select file

The uploaded business license must be a certificate issued to the enterprise by the applicable government authority, which records the enterprise registration information and permits the enterprise to engage in certain production and business activities. The format should be JPG or PNG and the size cannot exceed 2MB.[View Sample](#)

☐ I confirm that the information provided is complete, accurate and valid. I agree to transmit the above information to Tencent Cloud for the purposes of compliance with applicable regulations and laws. I shall be liable for any and all damages, consequences and liabilities caused by the failure to provide complete, accurate and valid information.

Confirm and submit

第二步：等待审核完成，审核通常需要2-3个工作日。实名认证成功后您会通过到邮件、短信以及站内信的方式收到通知，并附带资质申请链接进入下一环节。

## 经销商资质申请

第一步：进入[经销商资质申请页](#)，按照要求填写公司信息，包括公司联系信息，公司运营信息，公司银行账户信息并需要上传有效银行开户证明文件。

## Become a Tencent Cloud partner

### 01 Enter the enterprise information

The enterprise information will be used for the business cooperation between the partner and Tencent Cloud, including qualification reviews, contract signing, and capital transactions.

### 02 Pending review

After you submit your enterprise information, we will complete the review within 2–3 business days and notify you of the result through Message Center, email, and SMS.

### 03 Become a Tencent Cloud partner

#### Contact Information

First Name \*

Last Name \*

Role/Job Title \*

Mobile Phone \*

Email \*

#### Company Operating Information

Company Name \*

Industry \*

Size of the Company \*

Company Introduction

Company Introduction

Company Website

Company Website

Company Bank Information

Bank Name \*

Bank Name

Account Name \*

ZrCCCC

Bank Account \*

Bank Account

The transaction currency is USD. Make sure that your bank account can receive transfers in USD.

SWIFT Code \*

SWIFT Code

Bank Statement \*

Select file

The uploaded document must be a certificate issued by your enterprise's bank or financial department proving that your enterprise has an account in the bank.

第二步：等待审核完成，审核通常需要2-3个工作日，资质生效后可以登录伙伴控制台。

# 企业注册文件示例

最近更新时间：2022-03-10 16:09:28

## 概述

营业执照是政府相关机构发给企业的记载企业注册，准许企业从事某项生产经营活动的凭证。

## 示例





Company numbe. [redacted]

Follow this company

File for this company

- Overview
- Filing history
- People
- Charges
- More

Registered office address



Company status

Active

Company type

Private limited Company

Incorporated on



Accounts

Next accounts made up to [redacted] . 2022  
due by [redacted] 2022

# 银行证明示例

最近更新时间：2023-07-27 16:48:15

## 概述

银行对账单必须是企业银行在给定期限内发生的金融交易的官方摘要。

银行对账单提供的账户信息包括

-收款人账户名称

-收款人账号

-收款银行名称

-收款行swift代码

-一年期的进出口交易，如提款、转账和存款。

根据您的银行和偏好，银行对账单可以是实物对账单，也可以是数字对账单。它们可以通过大多数银行应用程序或在线银行账户在线获得，也可以通过邮寄或电子邮件获得。

## 示例





# Incoming Wire Transfer Instructions (US Dollar only)

Please direct incoming US Dollar denominated wires to CB International Standard account through Signature bank with the following bank routing instructions:

Bank Name	
Swift (International Wires Only)*	
ABA	
Beneficiary Account Name	
Beneficiary Account Number	
For Further Credit to	

**Attention:** CB International Standard ("CBIS") account is a multi-functional account that combines a variety of traditional account categories. CB International Bank uses agent banks to process wire transfer through the Federal Reserve on behalf of CB International Bank. As a result, the name "CB International Bank" will appear on your remittance information as the beneficiary, and the agent bank as the beneficiary bank. Additionally, you will receive multiple incoming wire transfer instructions for e-commerce and trade proceeds collections, backed by our partner financial institutions. Under such circumstances, the beneficiary will be the name you applied, and the beneficiary bank will be the corresponding financial institution.

In addition, if your originating bank requests the address for CB International Bank and/or Signature Bank, please provide the address below:

**CB International Bank**  
St 330  
270 MunozRivera Ave  
San Juan, PR 00918

**Signature Bank**  
565 Fifth Avenue  
New York, NY 10017

#### ADDITIONAL HELP AND SUPPORT

If you have any additional questions or need assistance, please call the Client Service Center at **+86-400-022-9291** or send email to **Support@cbibank.com**

# 线上合同签署

最近更新时间：2022-06-02 14:40:06

说明：

- 经销商入驻审批通过后进入线上化签署流程。
- 新入驻的经销商必须完成合同签署后才能进入伙伴控制台。

## 合同签署流程

1. 进入合同管理页，伙伴首次入驻会自动推送待签约的合同，点**签约**按钮进入签约流程。

Partner Center		Contract management				
Contract management		Contract ID	Contract name	Tencent entity	Term	Operation
		CLM-INF-2022053119481576	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-05-31 2023-05-30	To be signed <a href="#">Sign</a>
		Total items: 1				10 / page 1 / 1 page

2. 信息确认及填写页，确认入驻时填写的伙伴信息是否准确（若不准确请联系您的渠道经理进行信息修改），需选择业务拓展国家（可多选），信息确认后点击**下一步**进入合同签署页。

Partner Center

Contract management

← Resale contract confirmation

1 Confirm contract info

2 Sign

3 Submit contract

Contract info

Please contact your channel manager if any information is incorrect.

Term

2023-05-29

Tencent entity

Name of Partner Entity

UIN (Tencent Cloud User ID)

Email address for Notice of Partner Entity

Registered business address of Partner Entity

Company registration/license no. of Partner Entity

Partner Account Manager Contact Name

Message to Partner:

Select "Tencent Cloud Reseller Agreement" if you wish to become a Tencent Cloud reseller only. However, if you wish to become a Tencent Cloud reseller and integration partner of Tencent Services, you are required to agree to our "Tencent Cloud Reseller and Integration Agreement" instead. The Tencent Cloud reseller and integration partner agreement enables you to, in addition to resell Tencent Cloud services, integrate our Tencent Cloud services into one or more of your products and services that you own or licenses from a third party, and then offer such integrated products/services to your own customers.

Type of agreement \*

Tencent Cloud Reseller Agreement

Business country/region \*

Algeria Argentina

Office address \*

Mailing address \*

Contact address \*

Next

3. 查看合同详情，勾选已阅读标示后，点击**签署**。

Partner Center

Contract management

← Resale contract confirmation

1 Confirm contract info

2 Sign

3 Submit contract

CLM-INF-2022053017034444

Tencent Cloud Reseller Agreement

Effective from: 30 May 2022

Thank you for your interest in becoming a Tencent Cloud Reseller!

PLEASE READ THESE TERMS CAREFULLY

THIS TENCENT CLOUD RESELLER AGREEMENT ( "AGREEMENT" ) IS ENTERED INTO BY AND BETWEEN THE RELEVANT TENCENT ENTITY (SEE BELOW) AND THE APPLICABLE RESELLER ( "PARTNER" OR "YOU" ) AS OF THE EFFECTIVE DATE. YOUR PARTICIPATION IN TENCENT CLOUD RESELLER ACTIVITIES IS SUBJECT TO THESE TERMS AND CONDITIONS (THESE "TERMS" ). YOU ARE NOT PERMITTED TO PARTICIAPTE IN TENCENT CLOUD RESELLER ACTIVITIES AND YOU SHALL NOT REPRESENT YOURSELF AS A TENCENT CLOUD RESELLER IF YOU DO NOT AGREE TO THESE TERMS IN FULL.

BY CLICKING "AGREE" BUTTON BELOW, YOU REPRESENT AND WARRANT THAT (I) YOU HAVE READ AND UNDERSTOOD THESE TERMS; (II) YOU ARE DULY AUTHORISED TO ACT ON BEHALF OF THE ENTITY APPLYING TO BECOME A TENCENT CLOUD RESELLER AS PART OF THE TENCENT CLOUD PARTNER PROGRAM; AND (III) YOU ARE AUTHORISED TO ENTER INTO THESE TERMS AND LEGALLY BIND THE

☐ I have read and agree to the "Tencent Cloud Reseller Agreement"

BackSign

Partner Center

Contract management

← Resale contract confirmation

1 Confirm contract info

2 Sign

3 Submit contract

Submitted successfully

The contract signing information has been submitted successfully. Please return to the list to check the signing result.

Return to contract list

4. 提交成功后可返回列表页面点击**刷新**查询合同签署状况（系统签约大约需要1分钟）。

Partner Center

Overview

Company Info

Customer Management

Bills Management

Voucher Management

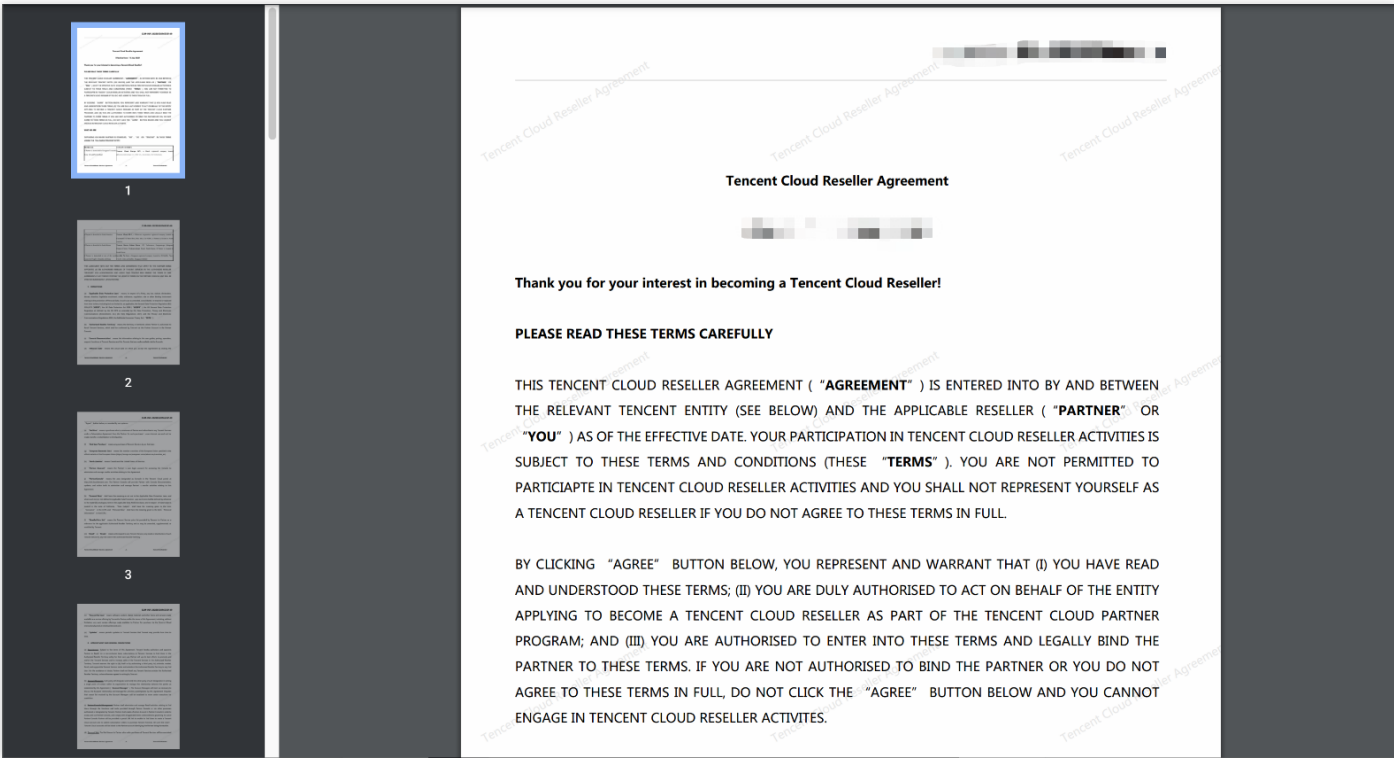
Contract management

Contract management

Submitted the application for contract termination


Contract ID	Contract name	Tencent entity	Term	Status	Operation
CLM-INF-2022053017034444	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-05-30 2023-05-29	Signed (non-renewal in review)	<a href="#">Refresh</a> <a href="#">View details</a>
CLM-INF-2022053019595640	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-05-30 2023-05-29	Signed	<a href="#">Not renew</a> <a href="#">View details</a>
CLM-INF-2022053016535149	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-05-22 2022-05-29	Expired	<a href="#">View details</a>
CLM-INF-2022053016362063	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2021-05-20 2022-05-21	Expired	<a href="#">View details</a>
CLM-INF-2022053016193926	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2020-05-26 2020-05-27	Expired	<a href="#">View details</a>
CLM-INF-2022053014082060	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2019-05-30 2020-05-25	Failed to sign	<a href="#">Sign</a>

5. 已签署的合同可以点击**查看详情**查看合同。



## 合同不续约

1. 合同签约成功后可进行**不续约**操作，确认当前合同信息。（注意：合同到期前**30**天内不可做不续约操作。）



### Contract non-renewal confirmation

Please confirm the contract information and expiration date. After you click "Confirm", the non-renewal approval process will start and cannot be canceled.

Contract type	Tencent Cloud Reseller Agreement
Contract ID	CLM-INF-2022053017034444
Cooperation expiration date	2023-05-29

ConfirmCancel

2. 提交成功后合同状态变化为**审批中**，可刷新获取审批状态。（审批详情请联系您的渠道经理。）

**Partner Center**

- Overview
- Company Info
- Customer Management
- Bills Management
- Voucher Management
- Contract management**

#### Contract management

Submitted the application for contract termination

Contract ID	Contract name	Tencent entity	Term	Status	Operation
CLM-INF-2022053017034444	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-05-30 2023-05-29	Signed (non-renewal in review)	<a href="#">Refresh</a> <a href="#">View details</a>
CLM-INF-2022053019595640	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-05-30 2023-05-29	Signed	<a href="#">Not renew</a> <a href="#">View details</a>
CLM-INF-2022053016535149	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-05-22 2022-05-29	Expired	<a href="#">View details</a>
CLM-INF-2022053016362063	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2021-05-20 2022-05-21	Expired	<a href="#">View details</a>
CLM-INF-2022053016193926	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2020-05-26 2020-05-27	Expired	<a href="#">View details</a>
CLM-INF-2022053014082060	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2019-05-30 2020-05-25	Failed to sign	<a href="#">Sign</a>

3. 审批通过后，在当前合同到期后系统不会对该合同进行续约合同的推送。

Contract management					
Contract ID	Contract name	Tencent entity	Term	Status	Operation
CLM-INF-2022053016535149	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-05-30 2022-07-14	Signed (non-renewal)	<a href="#">View details</a>
CLM-INF-2022053016362063	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2021-05-28 2022-05-29	Signed (renewal)	
CLM-INF-2022053016193926	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2020-05-26 2020-05-27	Signed (renewal)	
CLM-INF-2022053014082060	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2019-05-30 2020-05-25	Failed to sign	<a href="#">Sign</a>

## 合同续约

1. 在合同到期前45天，可进行合同续约操作，点击续约按钮进行合同续约。（您有15天时间可以进行合同续约，若在合同到期前30天未做操作则默认进行合同续约。）

CLM-INF-2022053020504198	Tencent Cloud Reseller Agreement	Aceville Pte. Ltd.	2022-01-01 2022-07-03	Signed	<a href="#">Not renew</a> <a href="#">Renew</a> <a href="#">View details</a>
--------------------------	----------------------------------	--------------------	--------------------------	--------	--

2. 确认续约后会进入续约合同的签署流程。（约合同的生效日期为当前合同的到期日期第二天）



## Contract renewal confirmation

After you click "Confirm", the new contract signing process will start.

Contract type	Tencent Cloud Reseller Agreement
Contract ID	CLM-INF-2022053020504198
Cooperation expiration date	2022-07-03

[Confirm](#)[Cancel](#)

← Resale contract confirmation

1 Confirm contract info > 2 Sign > 3 Submit contract

Contract info ⓘ Please contact your channel manager if any information is incorrect.

Term  
2023-07-03

Tencent entity  
Aceville Pte. Ltd.

Name of Partner Entity

UIN (Tencent Cloud User ID)  
200000103051

Email address for Notice of Partner Entity  
12345678@qq.com

Registered business address of Partner Entity

Company registration/license no. of Partner Entity  
13323

Partner Account Manager Contact Name

### Message to Partner:

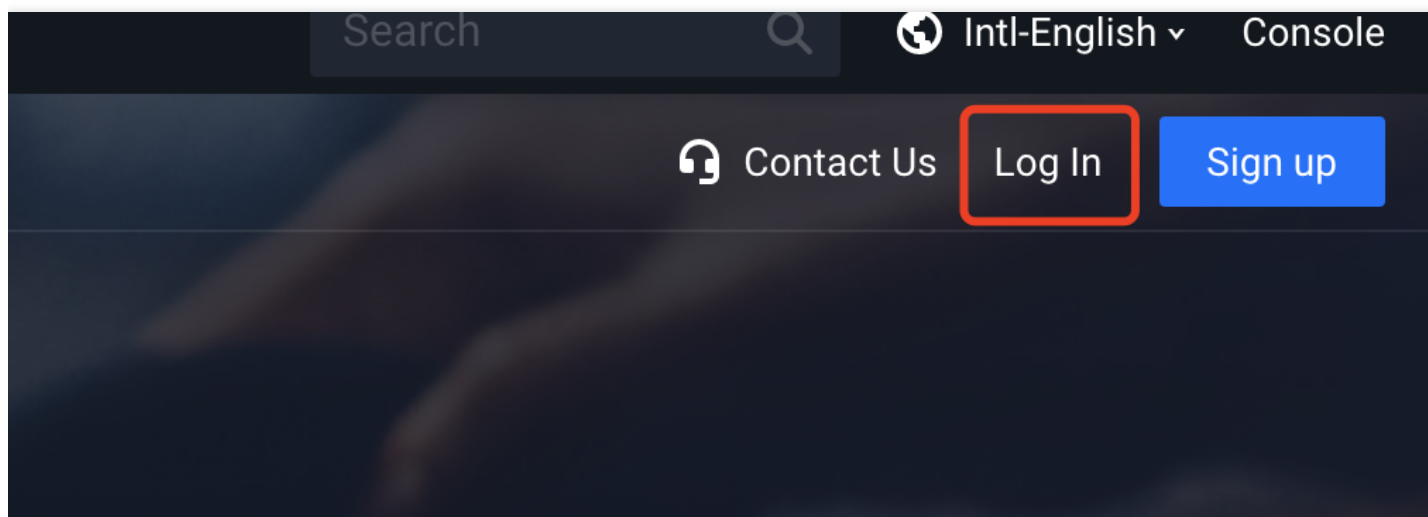
Select "Tencent Cloud Reseller Agreement" if you wish to become a Tencent Cloud reseller only. However, if you wish to become a Tencent Cloud reseller and integration partner of Tencent Services, you are required to agree to our "Tencent Cloud Reseller and Integration Agreement" instead. The Tencent Cloud reseller and integration partner agreement enables you to, in addition to resell Tencent Cloud services, integrate our Tencent Cloud services into one or more of your products and services that you own or licenses from a third party, and then offer such integrated products/services to your own customers.

# 登录伙伴中心

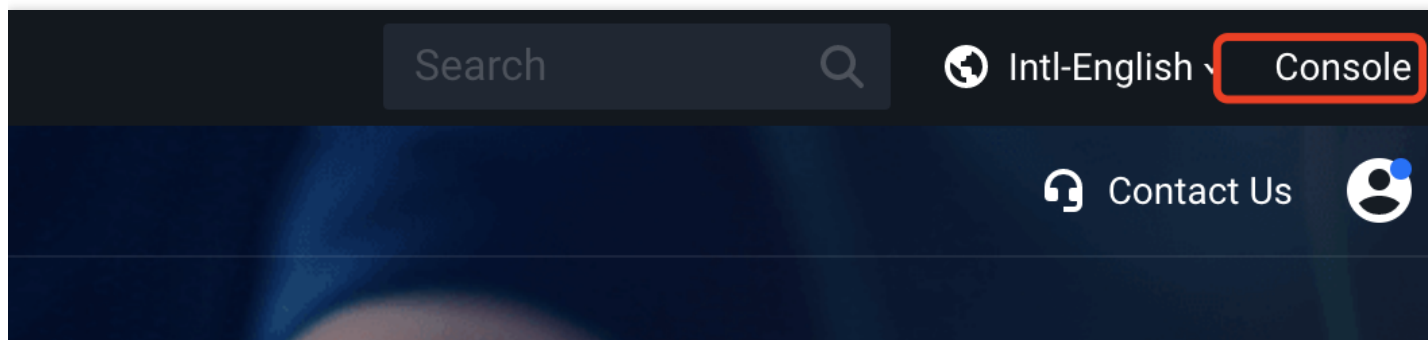
最近更新时间：2022-10-26 11:20:35

## 登录伙伴中心

第一步：登录[经销商账号](#)



第二步：登录成功后，点击右上角【控制台】。



第三步：鼠标悬浮在账号名称处，点击【渠道管理】，进入渠道控制台。



6

Ticket ▾

Billing Center ▾

English ▾

cloudpartner@tencent... ▾

Outstanding Balance (USD)

21.92

Transactions

Bills

Product Documentation

View M

Account Information

Security Settings

Access Management

Security Management

Channel Management

API Access Key

Log Out

版权所有：腾讯云计算（北京）有限责任公司

第237 共442页

# 账户管理

## 查询合作伙伴基础信息

最近更新时间：2022-11-22 16:42:45

### 合作伙伴信息管理

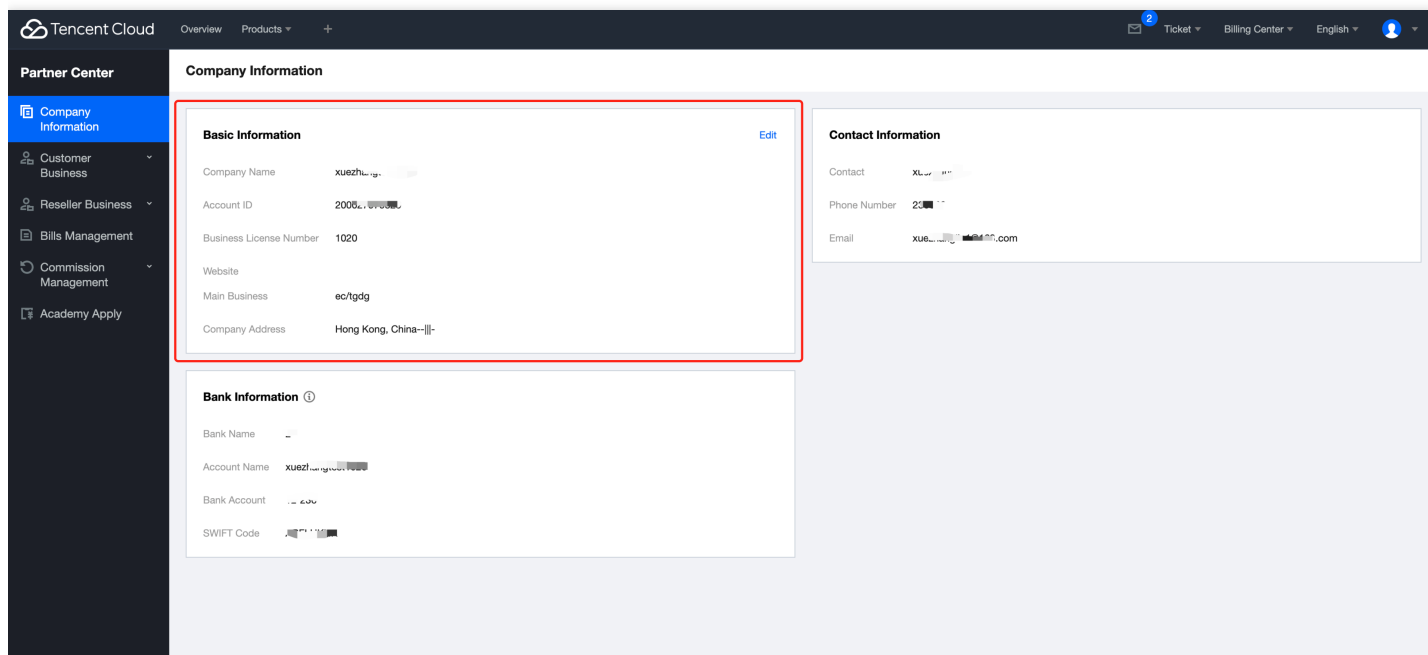
合作伙伴可以查询其信息，包含基础信息、银行信息、联系信息，且可对以上信息进行编辑。

第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。

第二步：左侧导航栏中选择【公司信息】。

#### 1、查询/编辑基础信息

单击【公司信息】，可查询公司基础信息。



单击基础信息的【编辑】，可编辑基础信息。

Tencent Cloud

OverviewProducts+

Ticket

Billing Center

English

Partner Center

Company Information

Customer Business

Reseller Business

Bills Management

Commission Management

Academy Apply

Company Information

Basic Information

Company Name

xuezhong

Account ID

20080100000000000000

Business License Number

1020

Website

Main Business

ec/fgdg

Company Address

Hong Kong, China--||-

Bank Information

Bank Name

Account Name

xuezhong

Bank Account

SWIFT Code

Contact Information

Contact

xuezhong

Phone Number

2008010000

Email

xuezhong@tencent.com

Basic Information

Edit

Company Name

xu

Account ID

20

Business License Number

132

Website

Website

Main Business

ec/tgdg

Company Address

Hong Kong, Chi

-

-||-

Save

Close

2、查询银行信息

单击【公司信息】，可查询公司银行信息。

Tencent Cloud

OverviewProducts+

2TicketBilling CenterEnglish

Partner Center

Company Information

Customer BusinessReseller BusinessBills ManagementCommission ManagementAcademy Apply

Company Information

Basic Information

Company Name

xuezh...

Account ID

2008...

Business License Number

1020

Website

Main Business

ec/tgdg

Company Address

Hong Kong, China--||-

Bank Information ⓘ

Bank Name

Account Name

xuezh...

Bank Account

SWIFT Code

Contact Information

Contact

XL...

Phone Number

23...

Email

xue...@tencent.com

说明：

银行信息暂不支持线上修改，如需修改请联系销售经理。

### 3、查询/编辑联系信息

单击【公司信息】，可查询公司联系信息。

Tencent Cloud

OverviewProducts+

2TicketBilling CenterEnglish

Partner Center

Company Information

Customer BusinessReseller BusinessBills ManagementCommission ManagementAcademy Apply

Company Information

Basic Information

Company Name

xuezh...

Account ID

2008...

Business License Number

1020

Website

Main Business

ec/tgdg

Company Address

Hong Kong, China--||-

Bank Information ⓘ

Bank Name

Account Name

xuezh...

Bank Account

SWIFT Code

Contact Information

Contact

XL...

Phone Number

23...

Email

xue...@tencent.com

## Contact Information

[Edit](#)

XLU

•

Please select

Phone Number

This field is required.

XL

Save

Close

# 员工管理

## 基本概念

最近更新时间：2023-02-27 15:19:18

## 基本概念

本文档介绍如何管理经销商的组织员工信息、新增人员和新增角色等。

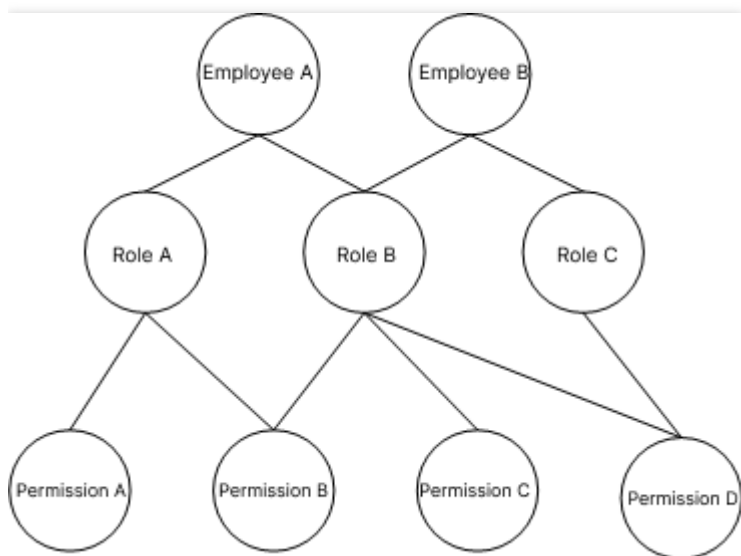
经销商可以创建拥有不同权限的组织员工账号，用来对经销商账号进行分权管理。

说明：

只有在经销商平台**公司信息 > 员工管理**页面新增员工并分配角色，才可以分权管理。请勿直接在**访问管理服务**中新增和删除用户，否则将与经销商平台员工管理权限冲突。

## 员工、角色和权限的关系

角色是权限的集合，可以自定义。一个员工可以拥有至多三个角色，每个角色拥有若干权限。



示例：

如果**员工A**分配角色为**客户经理(角色B)**，**客户经理(角色B)**拥有查看客户基础信息的权限(**客户查询权限B**)，说明**员工A**拥有**客户查询的权限B**。

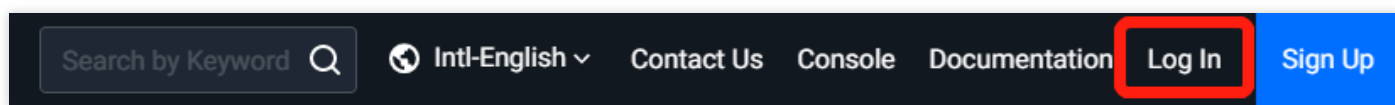
# 子账号登录经销商平台

最近更新时间：2023-02-27 15:09:44

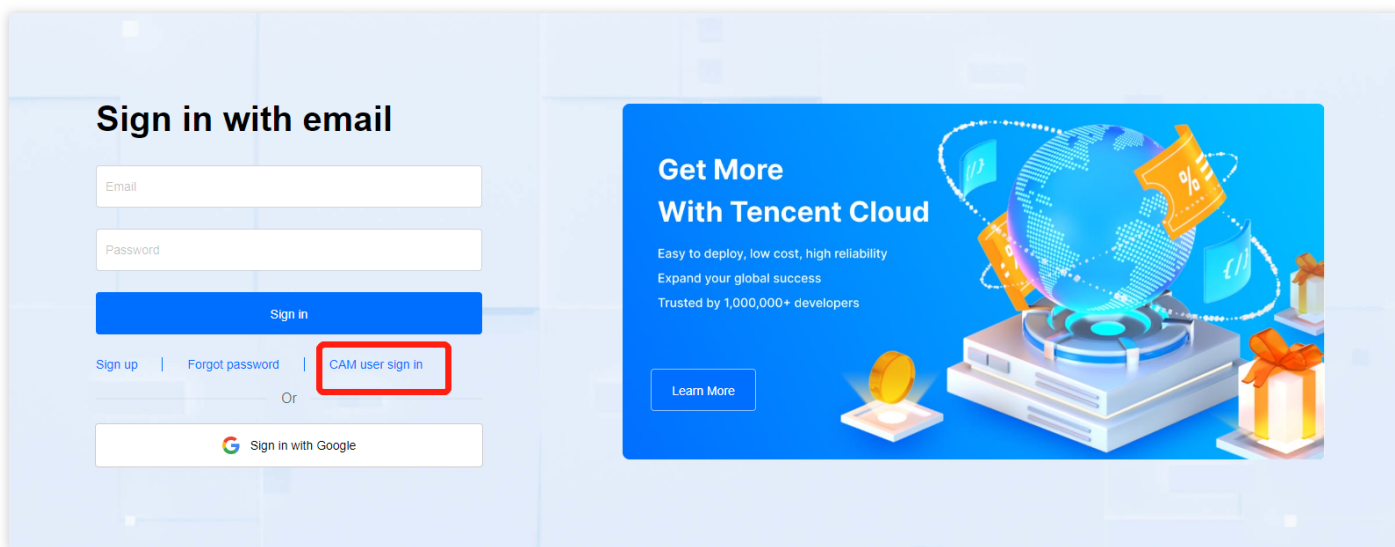
员工需要从**CAM用户登录**界面登录伙伴中心。如遇到登录访问失败，可联系主账号管理员。

## 操作步骤

1. 进入[腾讯云官网首页](#)。
2. 单击**登录**，进入登录页面。



3. 单击登录页面的**CAM用户登录**。





4. 输入登录信息后，单击**登录**。

# CAM user login

Root account ID

Sub-user name

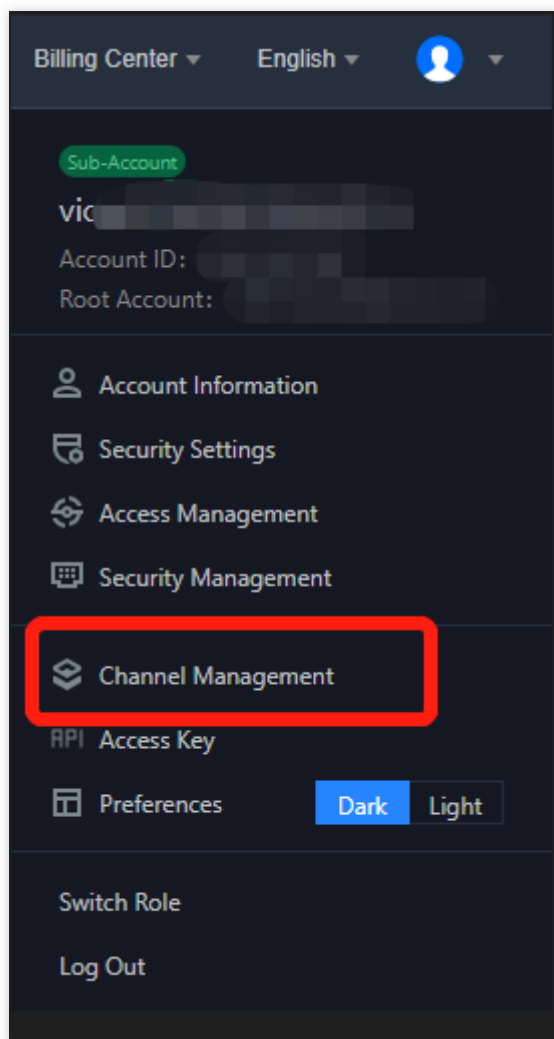
Password

Sign in

[← Login with root account](#)

参数	说明
主账号ID	输入合作伙伴的主账号ID。 经销商提供复制员工登录地址可直接填写主 账号ID。
CAM子账号名	输入员工账号名。 子账号名需要咨询经销商主账号管理员获取。
CAM用户密码	输入员工登录初始密码。 首次登录时， 需要根据页面提示修改密码。

5. 登录后找到控制台，点击**渠道管理**菜单入口访问经销商平台。



# 预设角色

最近更新时间：2023-02-27 15:10:00

## 预设角色

经销商选择员工关联的角色时，平台提供预设角色和权限供经销商使用。  
经销商进入平台后，预设角色和权限会自动完成初始化，未完成前员工管理将短暂不可用。

### 预设角色清单

预设角色	预设权限
系统管理员	包括所有经销商平台提供的功能
客户经理	二级经销商、客户邀请和管理，客户消费、佣金代金券、账单查看
财务管理	公司信息维护，二级经销商信用、代金券资产管理，账单对账
平台研发	平台邀请客户，信用管理API调用

# 新增角色

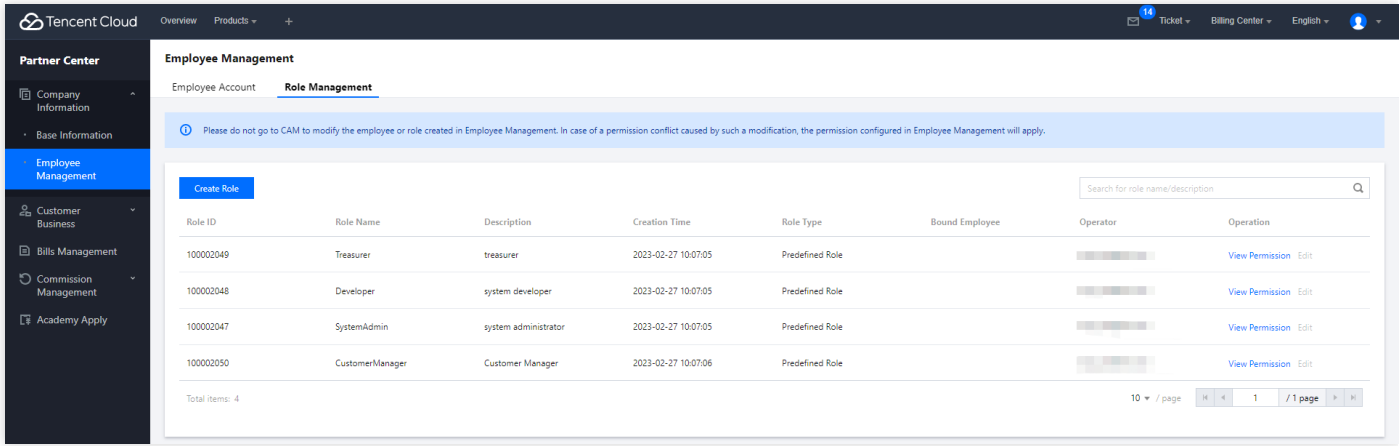
最近更新时间：2023-02-27 15:10:15

## 新增角色

经销商新增组织人员时，需要关联角色。经销商可以关联平台预设角色，也可以创建并关联自定义角色。

### 操作步骤

- 1. 登录[伙伴中心](#)。
- 2. 在左侧菜单中选择[公司信息 > 员工管理](#)。
- 3. 选择[角色管理](#)页签。
- 4. 单击[创建角色](#)。



- 5. 设置角色的基本信息。

6. 按照菜单级别选择需要关联的角色权限。

Create Role

Name \*

It cannot be modified once created successfully.

Description

0 / 1000

Permission Assignment \*

Select Permission

▶ ☐ Company Information

▶ ☐ Customer Business

▼ ☒ Commission Management

▼ ☒ Statement

☒ Statement View

☒ Statement Management

▶ ☐ Commission Details

▶ ☐ Agreement Management

▶ ☐ Academy Apply

Selected (2)

Menu	Permission	Operation
Statement-Com...	Statement View	✕
Statement-Com...	Statement Man...	✕

OK

Cancel

7. 单击**确认**。页面提示操作成功，可以在角色列表看到新增的角色。

## 角色相关操作

- 查询角色列表：可以按照特定查询条件查询角色列表。
- 查看权限：在角色列表中单击**操作**列的**查看权限**，可以查看角色权限的详情。
- 编辑权限：在角色列表中单击**操作**列的**编辑**，可以修改已创建的自定义角色。

版权所有：腾讯云计算（北京）有限责任公司

第249 共442页

# 新增员工

最近更新时间：2023-03-17 17:31:02

## 新增员工

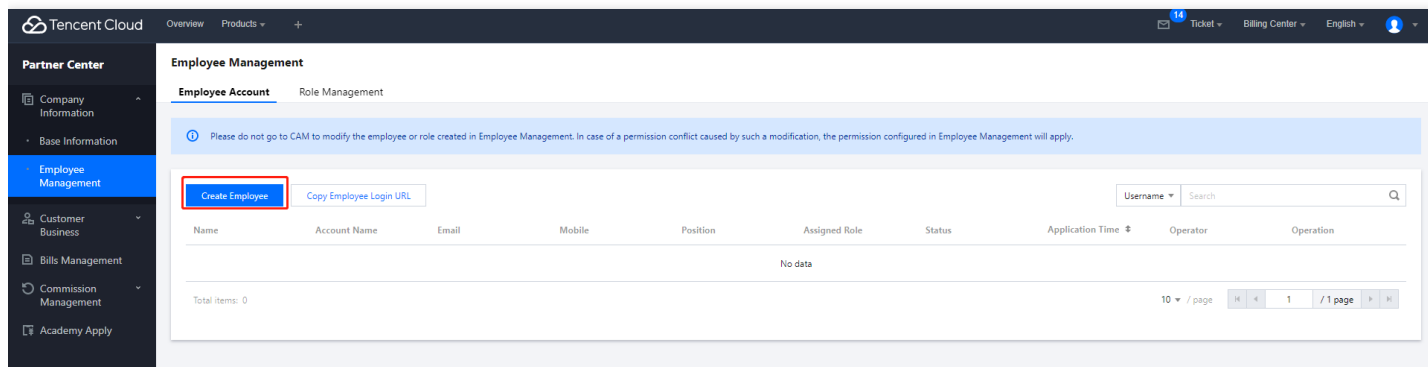
经销商可以创建员工，并关联角色。关联角色后，新创建的员工即拥有该角色的权限。  
创建员工成功后，经销商需要通过线下方式告知该员工账号名及密码。

### 操作步骤

1. [登入伙伴中心](#)。
2. 在左侧的菜单中选**公司信息 > 员工管理**。
3. 单击**创建员工**。

注意：

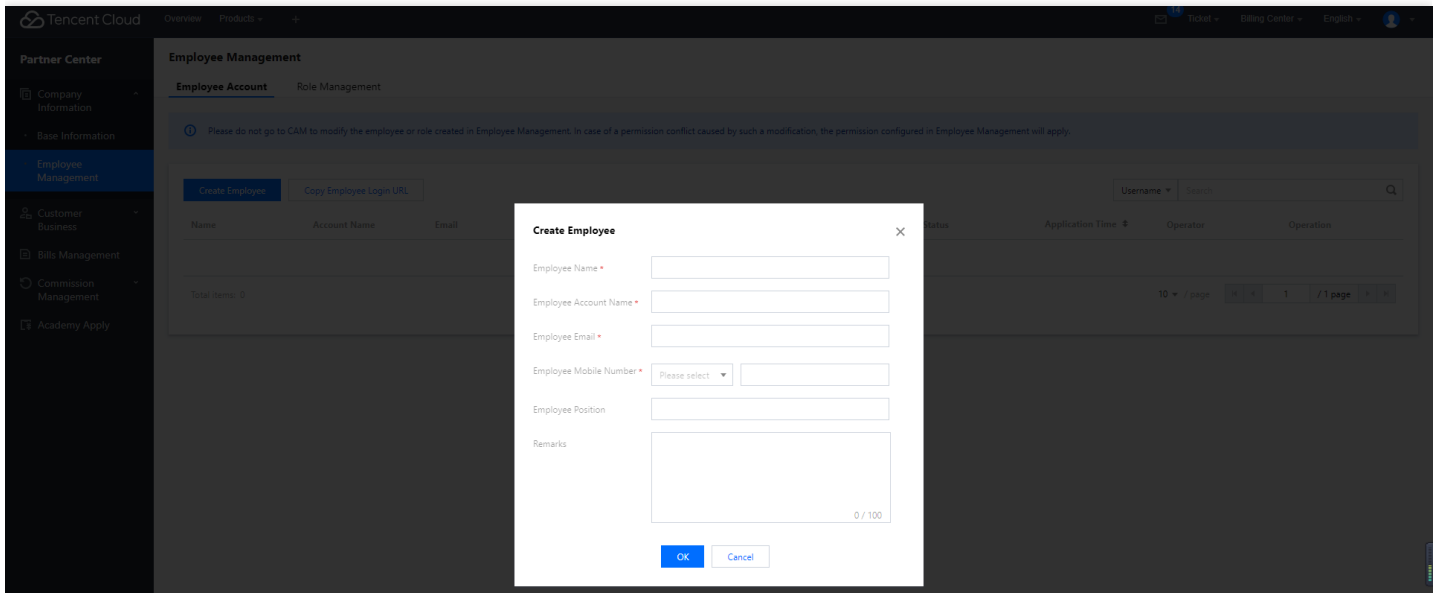
如员工已开通子账号，但尚未录入员工信息，需补充维护员工信息并关联角色后才可继续使用该子账号（员工账号名必须和子账号名一致），该员工子账号已授权的权限需解除绑定，以免和经销商平台分权管理不一致。



4. 填写员工信息，单击**提交**。

注意：

**员工账号名**必须唯一，且提交后无法修改，请谨慎填写。



- 系统提示，创建员工成功。
- 为新增的员工分配角色。勾选角色列表中的角色名称，单击**确认**。

注意：

对于新增的员工，必须为其分配角色，一个员工最多可以被分配3个角色。

- 创建员工和分配角色后，经销商通过线下方式告知员工登录信息。

登录信息	说明
员工登录地址	复制员工登录地址进行登录，可带出主账号ID
员工账号	提供员工账号名
员工初始密码	提供员工初始密码 如员工手机号码为 131XXXX4532 初始密码规则为手机号后四位与"@Tencent"组合，即初始密码为4532@Tencent

### 员工相关操作

- 查询员工列表：可以按照特定查询条件查询员工列表。
- 编辑员工：在员工列表中单击“操作”列的“编辑”，可以编辑员工的详情。

# 其他权限

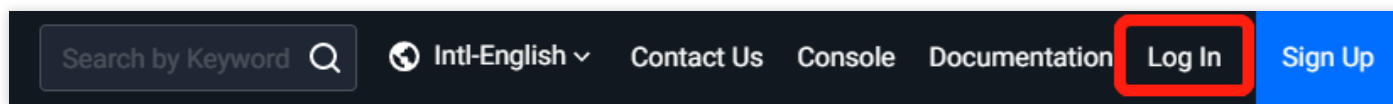
最近更新时间：2023-02-27 15:10:48

## 其他权限

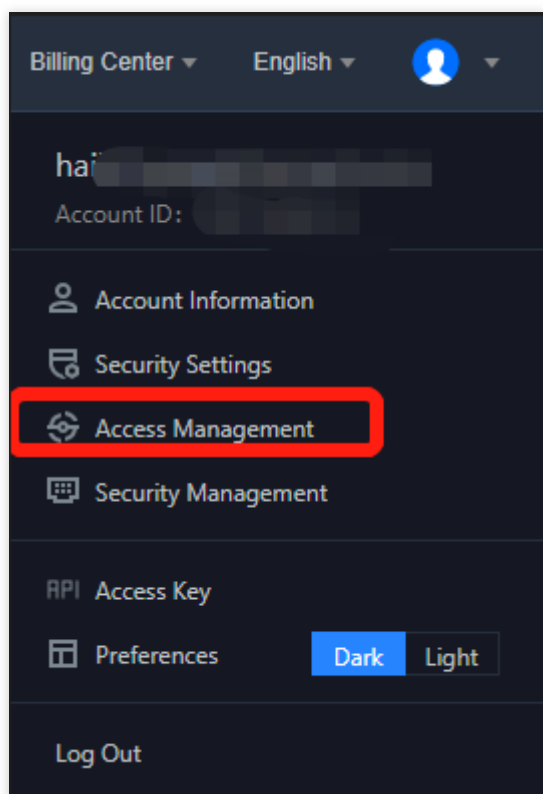
经销商员工管理仅维护经销商相关平台分权管理。如遇到其他产品涉及权限，请登录“访问管理”页面进行维护。

### 操作步骤

1. 进入[腾讯云官网](#)。
2. 单击**登录**，进入登录页面。

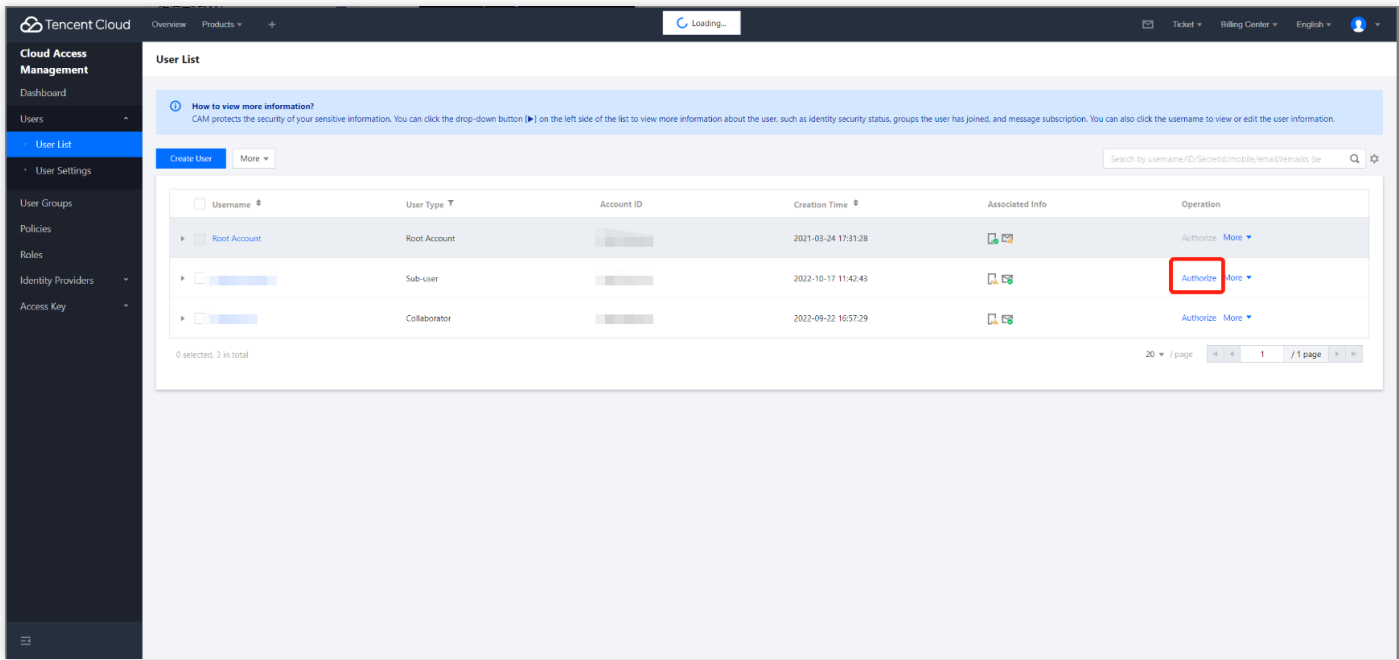


3. 输入主账号登录信息后，单击**登录**。
4. 登录后找到控制台，点击**访问管理**菜单入口。

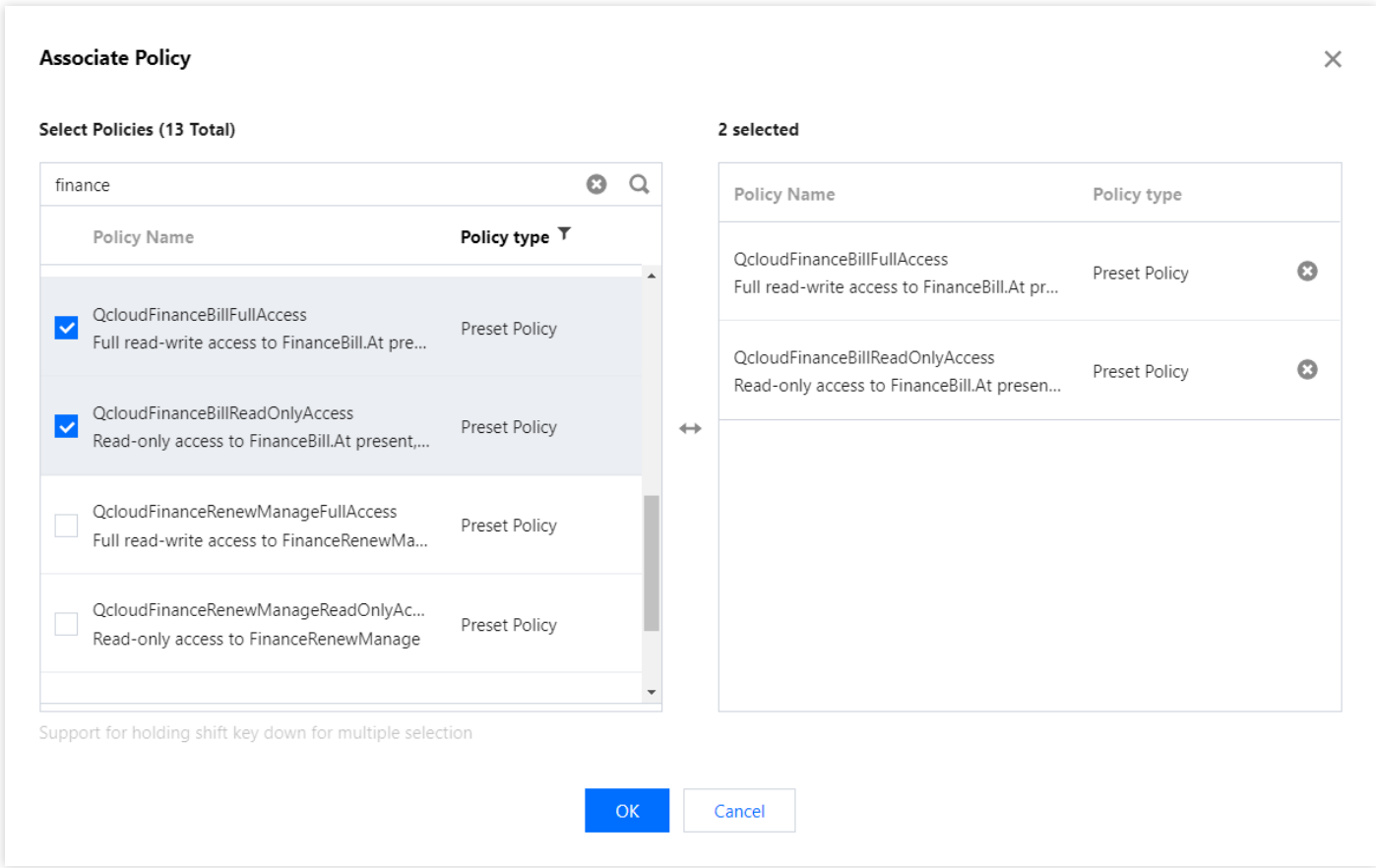


5. 在访问管理下，新增子账号用户权限。  
选择员工子账号，点击**授权**





选择非经销商平台的权限进行补充添加，点击提交



常见权限选择

权限说明

常见权限选择	权限说明
QCloudFinanceFullAccess	开通此权限后可访问经销商自身的账单管理和账户资产管理
QcloudCollPasswordManageAccess	允许自行管理其控制台登录密码
QcloudCollApiKeyManageAccess	允许自行管理其API密钥

注意：

- 访问管理仅允许添加非经销平台管理的权限，请勿直接新增和删除用户，否则将与经销商平台员工管理权限冲突。
- 如对经销商平台权限管理或访问管理产品有疑问，请[提交工单](#)联系我们。

# 子客业务

## 子客管理

### 查询子客

最近更新时间：2022-11-22 17:31:57

## 查询子客

合作伙伴可以查询其名下所有的子客，以及查看子客的基本信息、可用信用额度、信用扣减等。

第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。

第二步：左侧导航栏中选择【客户业务>客户管理】。

第三步：管理客户。

### 1、查询客户

伙伴可根据账号ID、账号名称、email等查询子客，此处email搜索需精准搜索，其余可模糊搜索。

The screenshot displays the 'Customer Management' page in the Tencent Cloud Partner Center. The page features a sidebar on the left with navigation options: 'Company Information', 'Customer Business', 'Bills Management', 'Commission Management', 'Contract Management', and 'Academy Apply'. The main content area is titled 'Customer Management' and includes a '+ Invite Customer' button. Below this, there are two tabs: 'My Customers' (selected) and 'Pending Customers'. The 'My Customers' tab shows a table of customer information. The table has columns for Account ID, Email, Mobile Number, Remarks, Name, Binding Time, Credit, Available Credit, and Operation. The table lists 10 customers, each with a unique Account ID, Email, and Mobile Number. The 'Operation' column for each row contains links for 'Allocate Credit' and 'More'. The table is paginated, showing 10 items per page and 9 pages in total. The bottom of the page shows 'Total items: 84' and '10 / page'.

Account ID	Email	Mobile Number	Remarks	Name	Binding Time	Credit	Available Credit	Operation
200000003533	200000003533@tencent.com				2022-11-08 10:52:39	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003536	200000003536@tencent.com				2022-11-07 17:13:05	\$11.00	\$11.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003536	200000003536@tencent.com				2022-11-02 18:50:39	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003539	200000003539@tencent.com				2022-10-28 18:58:45	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003534	200000003534@tencent.com				2022-10-28 11:12:00	\$0.60	\$0.60	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003541	200000003541@tencent.com				2022-10-20 17:02:39	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003516	200000003516@tencent.com				2022-10-20 14:59:59	\$3.00	\$3.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003533	200000003533@tencent.com				2022-10-06 14:13:16	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003537	200000003537@tencent.com				2022-09-30 19:43:49	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
200000003535	200000003535@tencent.com				2022-09-30 19:18:28	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>

### 2、导出客户

伙伴可导出全部子客。

Tencent Cloud

OverviewProducts+

99+TicketBilling CenterEnglish

Partner Center

Company Information

Customer Business

Overview

Customer Management

Customer Bills

Customer Management

+ Invite Customer

Account ID

Check rejection record

My Customers

Pending Customers

Account ID	Email	Mobile Number	Remarks	Name	Binding Time	Credit	Available Credit	Operation
2000	xin*****@163.com			有限公司	2022-11-08 10:52:39	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>

# 子客账户冻结和恢复

最近更新时间：2022-12-21 11:57:39

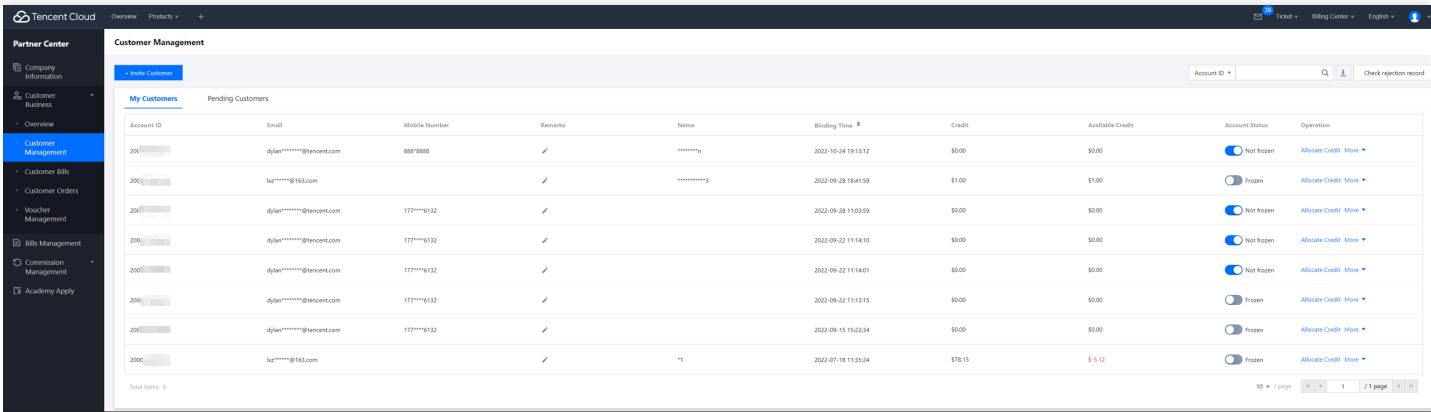
当经销商发现子客账户异常或子客拖欠还款时，合作伙伴可以冻结其名下所有的子客账户。

第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。

第二步：左侧导航栏中选择【客户管理】，选择【我的客户】页签，在客户列表冻结子客账户。

如冻结账户时，账户已欠费，则仅冻结账户，资源仍按欠费停服规则继续执行。

如冻结账户时，账户未欠费，则冻结账户和资源，资源按子客停服规则执行。



Account ID	Email	Mobile Number	Remarks	Name	Binding Time	Credit	Available Credit	Account Status	Operation
200*****	dylan*****@tencent.com	00878888	✓	*****2	2022-10-24 19:13:12	\$0.00	\$0.00	Not Frozen	Allocate Credit More
200*****	lu*****@163.com		✓	*****3	2022-09-28 18:41:59	\$1.00	\$1.00	Frozen	Allocate Credit More
200*****	dylan*****@tencent.com	177****6132	✓		2022-09-28 11:03:59	\$0.00	\$0.00	Not Frozen	Allocate Credit More
200*****	dylan*****@tencent.com	177****6132	✓		2022-09-22 11:14:10	\$0.00	\$0.00	Not Frozen	Allocate Credit More
200*****	dylan*****@tencent.com	177****6132	✓		2022-09-22 11:14:01	\$0.00	\$0.00	Not Frozen	Allocate Credit More
200*****	dylan*****@tencent.com	177****6132	✓		2022-09-22 11:13:15	\$0.00	\$0.00	Frozen	Allocate Credit More
200*****	dylan*****@tencent.com	177****6132	✓		2022-09-15 15:22:34	\$0.00	\$0.00	Frozen	Allocate Credit More
200*****	lu*****@163.com		✓	*1	2022-07-18 11:39:24	\$78.15	\$-5.12	Frozen	Allocate Credit More

第三步：子客账户冻结后账户状态变为已冻结，同时触发子客全部产品停服。

## 子客账户冻结

子客账户冻结后，子客新购、续费、升配、付费模式互转操作将受到限制。

已购买的预付费未到期可继续使用，已开通的后付费产品立即停服。

具体停服规则请参考[子客欠费停服规则](#)文档说明。

## 子客账户恢复

子客账户冻结关闭时，如账户仍欠费，需账户冲正后才能正常关闭冻结。

冻结关闭且账户不欠费后，子客停服将进行恢复。

说明：

- 子客账户冻结操作目前仍需开白使用，请联系销售经理可申请开通。
- 若该子客已开通计费特权则停服无法生效。

# 为子客分配信用

最近更新时间：2023-08-10 09:04:14

## 为子客分配信用

合作伙伴可以查询其名下所有的子客，以及查看子客的基本信息、可用信用额度等。

（注：经销商可分配给子客的信用额度无限制，请经销商自行管理。）

第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。

第二步：左侧导航栏中选择【客户业务>客户管理】，选择【我的客户】页签，在客户列表为子客分配信用。

The screenshot displays the 'Customer Management' interface in the Tencent Cloud Partner Center. The left sidebar contains navigation options like 'Company Information', 'Customer Business', 'Overview', 'Customer Management' (selected), 'Customer Bills', 'Customer Orders', 'Voucher Management', 'Bills Management', 'Commission Management', 'Contract Management', and 'Academy Apply'. The main area shows a table of customers under the 'My Customers' tab. The table has columns for Account ID, Email, Mobile Number, Remarks, Name, Binding Time, Credit, Available Credit, and Operation. The 'Allocate Credit' button in the Operation column is highlighted with a red box. The table lists several customers with their respective details and credit information.

Account ID	Email	Mobile Number	Remarks	Name	Binding Time	Credit	Available Credit	Operation
20...	x...@...com			大...公司	2022-11-08 10:52:39	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	q...@...com			伊...有限公司	2022-11-07 17:13:05	\$11.00	\$11.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	s...@tenc...	9876546		**1	2022-11-02 18:50:39	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	'9	com		神...限公司	2022-10-28 18:58:45	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	br...ent...			br...n2	2022-10-28 11:12:00	\$0.60	\$0.60	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	dj...nt...	86133			2022-10-20 17:02:39	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	d...nt...	177***6132			2022-10-20 14:59:59	\$3.00	\$3.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	...com			...;	2022-10-06 14:13:16	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	sv...@...e...	876*7686		***1	2022-09-30 19:43:49	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>
20...	sv...@...ce...	878*8611		***1	2022-09-30 19:18:28	\$1.00	\$1.00	<a href="#">Allocate Credit</a> <a href="#">More</a>

第四步：为客户调整信用。

### 1、分配信用

(1) 在客户列表中，选中一条客户记录，单击操作列的【设置信用】，进入分配信用页面。

(2) 设置【信用额度】，点击【确认】，系统提示分配成功信息。

Credit Allocation



Account name: d [REDACTED] nt.com  
Account ID: 8 [REDACTED] 5

**Available credit: \$178.00**

Total credit: \$178.00

Used credit: \$0.00

#### Notes:

1. The credit is the credit limit available to a customer. It is calculated as published at the Tencent Cloud official website and excludes deductions from vouchers.
2. Credit control is only a tool provided by Tencent Cloud for partners to control the approximate amount of credit available to customers. Due to the different billing modes and settlement cycles of Tencent Cloud services, there may be delays and differences in the monitoring of the fees incurred by customers.
3. We will send alarm notifications to you when a customer has used more than 75%, 90%, and 100% of their credit.
4. In the reseller mode, all fees incurred by customers are paid by the partner, so caution should be exercised.
5. A credit will immediately take effect once set.
6. You can contact your channel manager to add you to the allowlist of the customer service suspension rule to shorten the service suspension period. For details, see [Customer Service Suspension Rules](#).

\* Allocated amount: (USD)



Available credit: \$179.00

Confirm

Close

Allocation Record

说明：

- 1、信用额度，为客户消费信用限额，按腾讯云官网计算，不包含代金券已抵扣部分；
- 2、信用管控只是腾讯云为伙伴提供了一种控制子客大概消费额度的工具，因云服务计费模式、结算周期等特点，客户消费监控会存在延时和误差；
- 3、如果客户的已使用信用额度比例超过75%、90%、100%，我们将发送预警通知给您；
- 4、经销模式下，子客户消费最终由合作伙伴负责还款，请谨慎操作；
- 5、信用额度设置完成后，即时生效。

2、回收信用

如果分配子客的信用额度较高，您可输入负值，回收子客可用信用额度。最高【可回收子客信用额度】≤【子客可用信用额度】。

Credit Allocation



Account name: d' [redacted] t.com  
Account ID: { [redacted] 5

Available credit: \$178.00  
Total credit: \$178.00  
Used credit: \$0.00

Notes:



1. The credit is the credit limit available to a customer. It is calculated as published at the Tencent Cloud official website and excludes deductions from vouchers.
2. Credit control is only a tool provided by Tencent Cloud for partners to control the approximate amount of credit available to customers. Due to the different billing modes and settlement cycles of Tencent Cloud services, there may be delays and differences in the monitoring of the fees incurred by customers.
3. We will send alarm notifications to you when a customer has used more than 75%, 90%, and 100% of their credit.
4. In the reseller mode, all fees incurred by customers are paid by the partner, so caution should be exercised.
5. A credit will immediately take effect once set.
6. You can contact your channel manager to add you to the allowlist of the customer service suspension rule to shorten the service suspension period. For details, see [Customer Service Suspension Rules](#).

\* Allocated amount: (USD)

-1



Available credit: \$177.00

Confirm

Close

[Allocation Record](#)

说明：

- 1、当子客可用信用额度为0时，不会触发子客停服，也不会影响子客新购产品。账户资产（信用+代金券）对新购和停服的影响，请查看[账户资产对新购&停服影响](#)。
- 2、联系销售经理可申请开通子客欠费停服规则缩短停服期，具体规则请参考[子客欠费停服规则说明](#)。

3、分配记录

点击【信用分配页面-分配记录】，可查询经销商对子客全部的信用分配记录。

Tencent Cloud

OverviewProducts+

99+TicketBilling CenterEnglish

Partner Center

Company Information

Customer Business

Overview

Customer Management

Customer Bills

Customer Orders

Voucher Management

Bills Management

Commission Management

Contract Managemant

Academy Apply

Allocation Record

(200028333209)

Allocation Time	Current Allocated Credit	Total Allocated Credit	Operator
2022-11-08 15:41:24	\$1.00	\$1.00	

Total items: 1

1 / 1 page

# 代金券申请操作指引

最近更新时间：2023-10-19 18:05:29

## 代金券申请操作指引

本文档提供的表格详细列举了经销商申请代金券的各种场景，以及在每种场景下申请代金券的平台和方法，若您在使用过程中有其他疑问或需要进一步的指导，请随时与您的渠道经理取得联系以获取更多的帮助。

### 经销代金券分使用场景操作指引

代金券使用场景	如何操作	代金券类型	申请者	申请平台	成本承担方	代金券抵扣逻辑	示例
经销商 <b>赔偿</b>	渠道经理在腾讯内部磐石平台为经销商申请即可	1st Type：经销商代金券	渠道经理	腾讯内部磐石平台	腾讯云	<b>折扣价</b> 抵扣经销商账单	适用于需要通过代金券赔偿经销商的场景
子客 <b>测试、体验</b> 用途	<b>第一步：</b> 经销商在经销平台申请第二类厂商代金券（需腾讯侧审批）	2nd Type：厂商代金券	经销商	经销平台入口：[合作伙伴中心]->[代金券管理]->[厂商代金券申请]	腾讯云	<b>折扣价</b> 抵扣经销商账单（抵扣申请时绑定的子客uin产生的账单）	假设：子客要购买刊例价100美元的产品，经销商与腾讯之间的折扣是75折（25% off） <b>第一步：</b> 经销商在经销平台申请第二类厂商代金券，因第二类代金券 <b>折扣价抵扣</b> 经销商账单，经销商申请75美金第二类代金券即可cover子客测试成本
	<b>第二步：</b> 经销商在经销平台向子客发放第三类客户代金券（无需腾讯侧审批） <b>注：如须腾讯云承担全部/部分子客测试成本，两类代金券都需申请；但以上两步没有确定的先后顺序</b>	3rd Type：客户代金券	经销商	经销平台入口：[合作伙伴中心]->[代金券管理]->[客户代金券发放]	经销商	<b>刊例价</b> 抵扣子客账单	<b>第二步：</b> 经销商在经销平台向子客发放第三类客户代金券，因客户代金券以 <b>刊例价抵扣</b> 子客账单，经销商需发放给子客100美金客户代金券即可cover子客测试成本
经销商因活动/促销等其他用途给子客发代金券	经销平台向子客发放第三类客户代金券（无需腾讯侧审批）	3rd Type：客户代金券	经销商	经销平台入口：[合作伙伴中心]->[代金券管理]->[客户代金券发放]	经销商	<b>刊例价</b> 抵扣子客账单	经销商需要向子客发放代金券的其他场景（除子客测试）

本次代金券改造主要变化点：

- 取消子客代金券池
- 新增第三类客户代金券，伙伴自主下发，无需经过腾讯侧审批
- 针对子客测试需求，伙伴仍可申请第二类厂商代金券报销全部/部分子客测试成本

# 为客户分配代金券

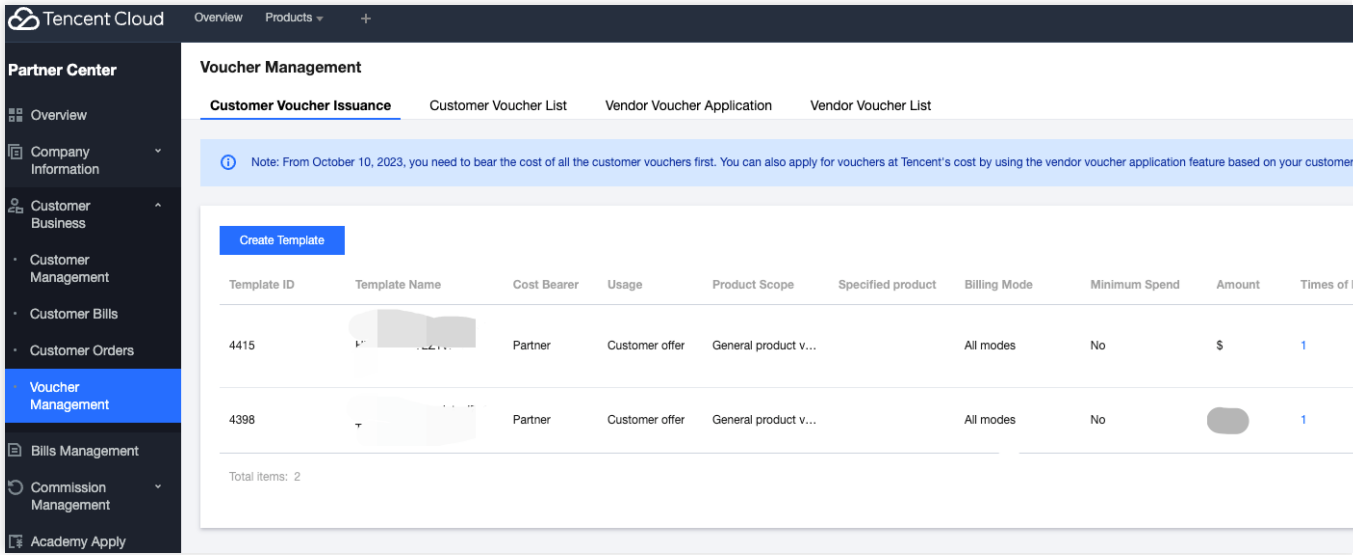
最近更新时间：2024-06-14 15:16:39

## 代金券发放

说明：

● 23年10月10日起，所有的客户代金券费用均由伙伴自行承担成本，针对子客产品测试场景发放的客户代金券成本费用，可根据子客实际消耗情况，在厂商代金券申请入口进行申请核销。

- 第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。
- 第二步：点击[客户业务](#) > [代金券管理](#)菜单进入代金券发放页面。



第三步：点击[创建代金券模板](#)，填写代金券规则。

## Create Template

Template Name \*

Cost Bearer \*

☒ Partner

Usage \*

☒ Product trial ☐ Customer offer

Product Scope \*

☒ Specific Product Blacklist Voucher ☐ Specified product voucher ☐ General pr

Specified product \*

☐ One-Click Selection for the blacklist products corresponding to Manufacturer Vouche

Billing Mode \*

☒ All modes ☐ Prepaid ☐ Postpaid

Minimum Spend \*

☒ No

Voucher Type \*

☒ Balance deduction

Amount \*

USD

Validity Period \*

From the issuance date

Please selec

Month(s)

Description \*

0 / 1000

OK

Cancel

## 说明：

通用产品代金券：适用于可对客户任意产品的消耗费用进行抵扣。

指定产品代金券：适用于具体的单个或多个产品的产品测试场景申请，只对指定范围内的产品消耗费用进行抵扣。

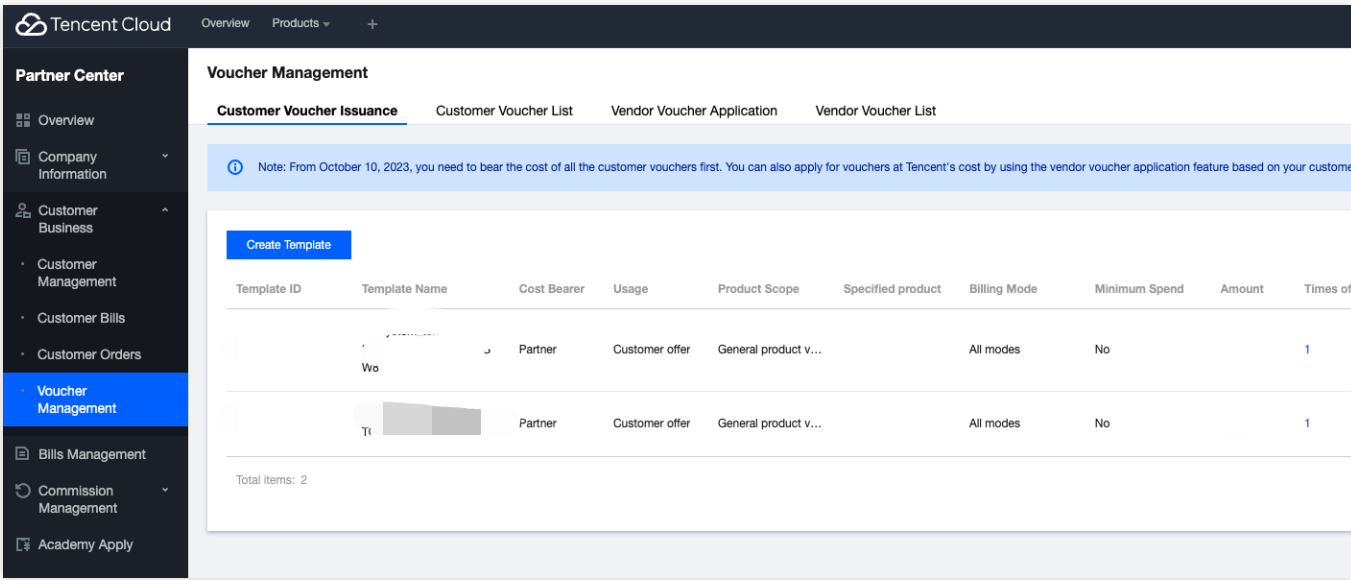
一键选中“厂商代金券 - 通用产品代金券”对应的黑名单产品：自动选中一级经销商申请[申请厂商代金券](#)时，对应的黑名单产品列表，以代金券发放时为准。

**第四步：**确认填写内容后点击**确认**保存代金券模板。

**说明：**

代金券模板保存成功后，如未发放给实际客户，仍可以进行编辑，发放给客户后则模板无法继续编辑，可重新创建新的模板。

**第五步：**代金券模板创建完毕后，可以查看已创建的代金券模板，也支持按条件查询代金券模板。



**第六步：**点击**发放**，可将代金券发放给具体的某一客户。

**说明：**

伙伴承担费用的客户代金券无需腾讯审批，伙伴确认发放后，子客即可收到代金券进行下单使用。

Voucher Issuance

Template Name

t

Validity Period

1 month from the issuance date

Product Scope

Specific Product Blacklist Voucher / All modes

Usage

Product trial

Cost Bearer

Partner

Customer Account ID \*

Select the customer account ID

Customer Name \*

Amount \*

USD

Issuance Remarks \*

Up to 1,000 characters

0 / 1000

OK

Cancel

## 代金券清单查询

点击客户业务>代金券管理 菜单进入客户代金券清单页面。客户代金券确认发放给客户后，可在此页面查询代金券状态和使用情况，支持全量查询或输入具体条件查询代金券。

### 说明：

客户代金券发放后，点击 客户代金券清单 即可查询到此代金券记录。

客户代金券发放后，可以通过代金券余额、代金券状态查看客户使用情况。

客户代金券发放后，如子客未使用完该代金券，允许经销商撤回代金券。

Partner Center

Overview

Company Information

Customer Business

Customer Management

Customer Bills

Customer Orders

Voucher Management

Bills Management

Commission Management

Voucher Management

Customer Voucher Issuance

Customer Voucher List

Vendor Voucher Application

Vendor Voucher List

Template Name	Voucher ID	Cost Bearer	Customer Account ID	Customer Email	Amount	Balance	Issuance Time
...		Partner		k*****e@outlook.com	\$459	\$459.00	2023-10-10 17:
		Partner		k*****e@outlook.com	\$498	\$496.86	2023-10-10 17:

Total items: 2



# 申请厂商代金券

最近更新时间：2024-06-14 15:18:04

## 申请厂商代金券

**说明：**

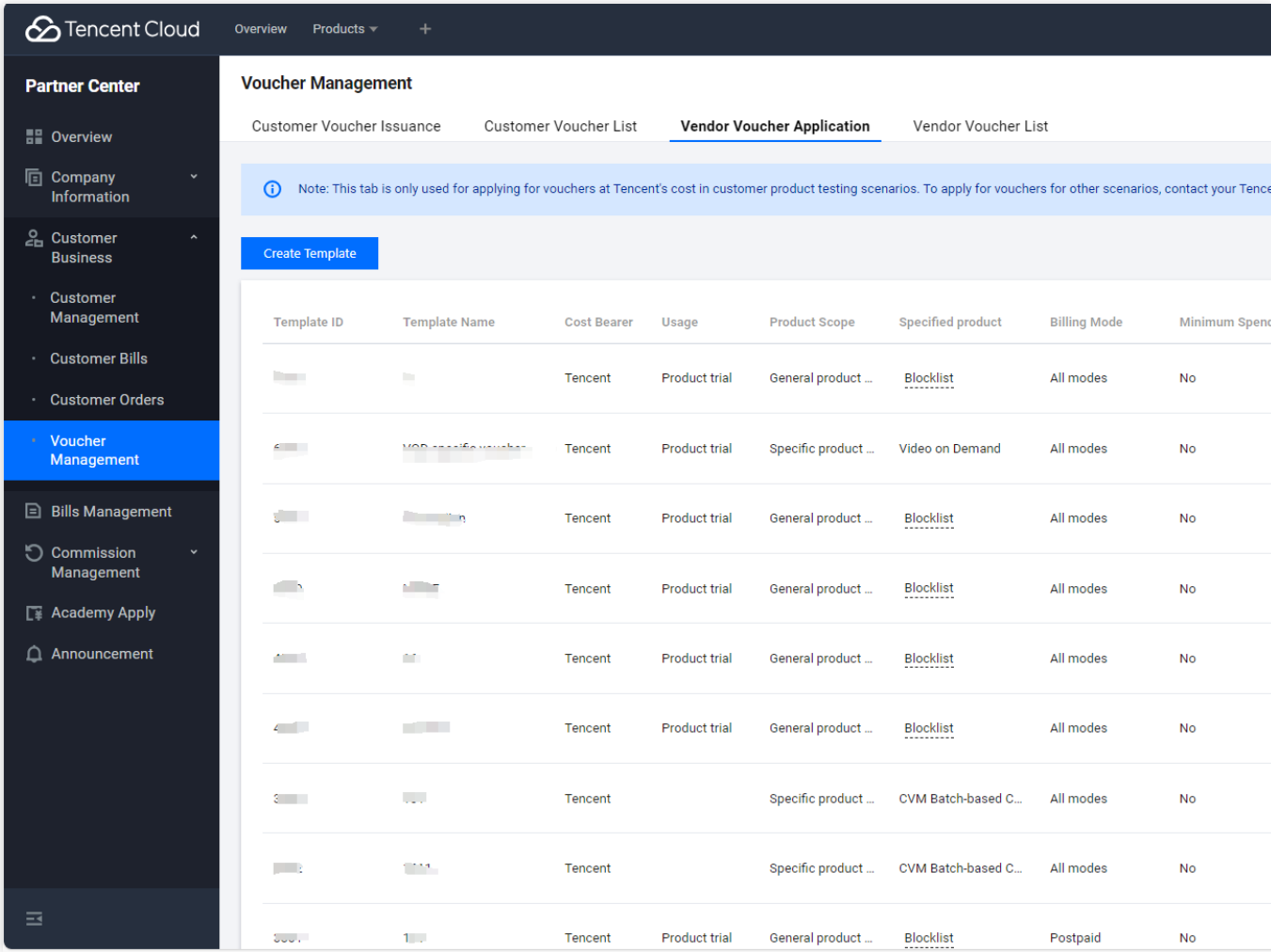
厂商代金券申请入口针对客户产品测试场景申请腾讯承担成本的代金券，其他场景的代金券申请请与腾讯云商务联系。

厂商代金券申请后需经过腾讯侧审核，审核通过后代金券会发放给到伙伴，对客户侧不可见。

厂商代金券审批通过发放后，仅适用于对指定客户满足代金券条件的伙伴代付产品费用抵扣。

第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。

第二步：点击[客户业务](#) > [厂商代金券申请](#)菜单进入厂商代金券申请页面。



第三步：点击[创建代金券模板](#)，填写厂商代金券申请规则。

### Create Template

Template Name \*

Cost Bearer \*

☒ Tencent

Usage \*

☒ Product trial

Product Scope \*

☒ Specific product voucher ☐ General product voucher

Product Scope \*

Billing Mode \*

☒ All modes ☐ Prepaid ☐ Postpaid

Minimum Spend \*

☒ No

Voucher Type \*

☒ Balance deduction

Amount \*

USD

Validity Period \*

Starting from the date of approval

Please select

Month(s)

Description \*

0 / 1000

OK

Cancel

#### 说明：

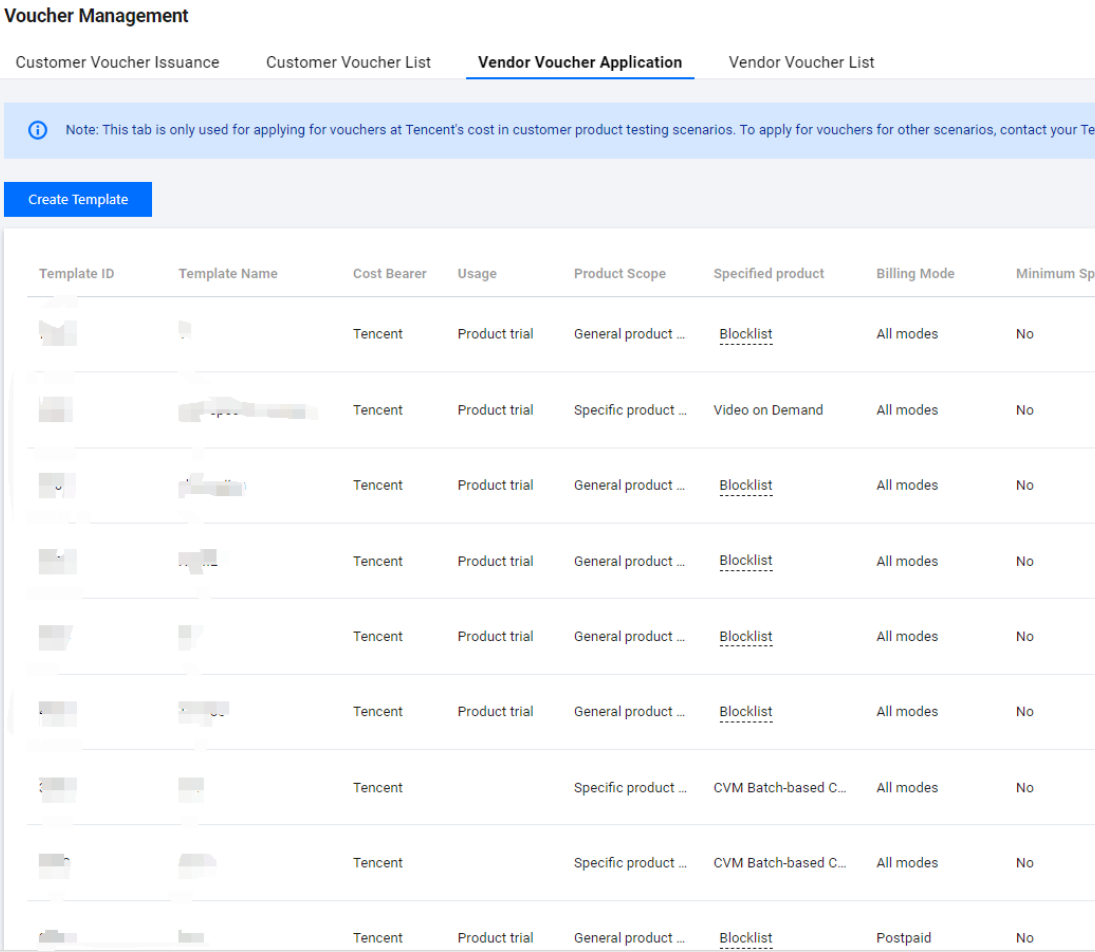
通用产品代金券：该类优惠券存在无法使用的产品清单，清单外的产品都可以用券。（鼠标悬停在“黑名单”文字时可展示不适用的产品清单，以代金券审批通过时为准）。

指定产品代金券：适用于具体的单个或多个产品，只有适用产品列表里的产品可以使用。

第四步：确认填写内容后点击**确认**保存代金券模板。

厂商代金券申请模板保存成功后，如未发起厂商代金券申请，仍可以进行编辑，发起申请后则模板无法继续编辑，可重新创建新的模板。

第五步：厂商代金券申请模版创建完毕后，可以查看已创建的厂商代金券申请模版，也支持按条件查询已创建厂商代金券模板。



说明：

申请厂商代金券，需经过腾讯侧审批，约1-3个工作日。

厂商代金券审批通过后，经销商将收到厂商代金券，即可对此客户满足代金券条件的经销商代付费用进行抵扣。

### Apply for Vendor Voucher

Template Name

T

Validity Period

Valid for 3 month from the date of application submission

Product Scope

General product voucher (Blocklist) / All modes

Usage

Product trial

Cost Bearer

Tencent

Customer Account ID \*

Select the customer account ID

Customer Name \*

Amount \*

Please enter an integer amount

USD

Estimated Revenue Converted for Tencent \*

Please enter an integer amount

USD

Estimated Time of Revenue Conversion \*

Select date

Remarks \*

Up to 1,000 characters

0 / 1000

OK

Cancel

## 厂商代金券清单查询

点击客户业务 > 代金券管理 菜单进入厂商代金券清单页面。厂商代金券发放给伙伴后，可在此页面查询厂商代金券状态和使用情况，支持全量查询或输入具体条件查询厂商代金券。

### 说明：

厂商代金券申请后，点击 厂商代金券清单 即可查询到此厂商代金券记录。

厂商代金券申请后，进入审批流程，此时可查看审批状态确认审批进展。

厂商代金券审批中，可以取消审批流程。

厂商代金券审批完成后，厂商代金券发放到伙伴的伙伴代金券池中，可以通过厂商代金券余额、代金券状态查看使用情况。

Tencent Cloud

OverviewProducts+

Partner Center

Overview

Company Information

Customer Business

Customer Management

Customer Bills

Customer Orders

Voucher Management

Bills Management

Commission Management

Academy Apply

Voucher Management

Customer Voucher IssuanceCustomer Voucher ListVendor Voucher ApplicationVendor Voucher List

Template Name	Voucher ID	Customer Account ID	Customer Email	Estimated Revenue	Estimated Time	Amount	Balance
	HNKGJT1ETE21VFLZE	200026L	*****e@ok.com	\$1000	2023-10-27	\$500	\$458.27
	/TQXIORNBQ7BYTB4Y	200026	*****e@ok.com	\$1000	2023-08-31	\$500	\$497.84
t	VMUYF34QUK1XQBG5	20002	*****e@ok.com	\$2000	2023-06-30	\$2000	\$1,810.36
t	XCAUIIZ60P32WA6K43	20002	*****e@ok.com	\$3000	2023-01-31	\$2000	\$1,990.06
esting2	SEYJHMMWR52H7US9	20002	***2@.im	\$500	2023-02-01	\$100	\$100.00
esting2	MOUBJW6AZ939EVR	20002	***2@.com	\$500	2023-03-01	\$100	\$99.55
esting2	0017029_1647299294	20002	***v@.com	\$100	2022-03-31	\$100	\$100.00
esting2	0017029_1647249935	20002	***v@.com	\$100	2022-03-31	\$100	\$100.00
esting	0017029_1646043950	20002	***d@.l.com	\$100	2022-02-26	\$100	\$0.00
00	0017029_1647077500	20002	***d@.il.com	\$10000	2022-03-11	\$5000	\$0.00

Total quantity: 13 Total cost: \$16500

# 管理子客关联关系

最近更新时间：2022-11-22 18:01:18

## 管理子客关联关系

说明：

子客解绑：暂不支持线上解绑，如您的子客有解绑需求，请联系销售进行线下解绑处理。

### 1、邀请子客

可发送邀请链接给子客，成为经销商的子客。未注册或已注册腾讯云账号的客户，均可邀请绑定成经销商子客。

（注：若已注册用户绑定前有未回款帐单，绑定前的未回款帐单只能通过绑定前的身份回款流程进行回款，如：绑定前为腾讯云客户，未回款帐单的回款流程只能通过腾讯云客户的回款方式进行回款。）

Account ID	Name	Mobile Number	Email	Application Time	Status	Operation
20****	-	+	q*****4@163.com	2022-10-13 15:00:14	Under review	<a href="#">Review</a>
20****	-	+	r*****u@outlook.com	2022-09-20 18:26:12	Under review	<a href="#">Review</a>
20****	-	+1 32****5297	l*****t@tencent.com	2022-01-18 10:35:48	Unmatched customer	<a href="#">Review</a>

### 2、审核子客

子客提交绑定申请后，需经销商经销审核，确认是否可绑定。

**Customer Management**

+ Invite Customer

Account ID

**My Customers** **Pending Customers** 3

Account ID	Name	Mobile Number	Email	Application Time	Status	Operation
20[REDACTED]	-	+	q*****4@163.com	2022-10-13 15:00:14	Under review	<a href="#">Review</a>
20[REDACTED]	-	+	r*****u@outlook.com	2022-09-20 18:26:12	Under review	<a href="#">Review</a>
20[REDACTED]	-	+1 32****5297	i*****t@tencent.com	2022-01-18 10:35:48	Unmatched customer	<a href="#">Review</a>

Total items: 3

10 / page 1 / 1 page

### 3、驳回记录

子客提交绑定申请后，经销商驳回，可查看所有驳回记录。

**Rejected Record**

2021-11

Account ID

Rejected Time	Account ID	Rejected Phrase	Reason for rejected	Operator
2021-09-27 20:41:42	200021479462			200018967974

Total items: 1

10 / page 1 / 1 page

# 子客账单管理

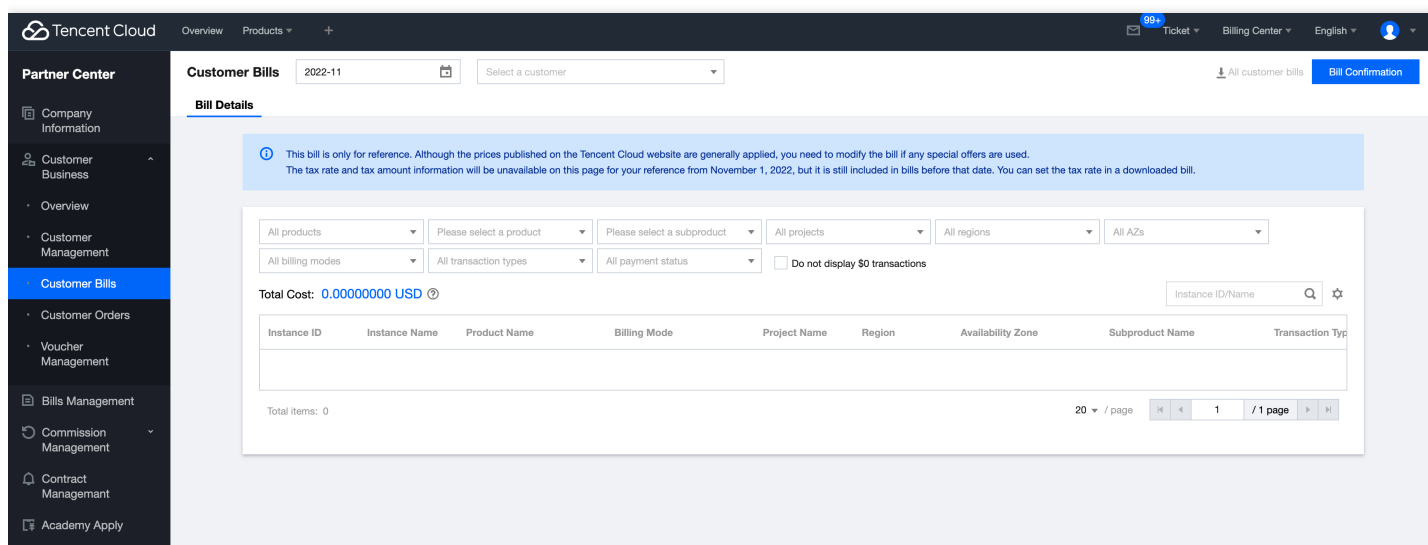
最近更新时间：2022-11-22 18:18:39

## 子客账单管理

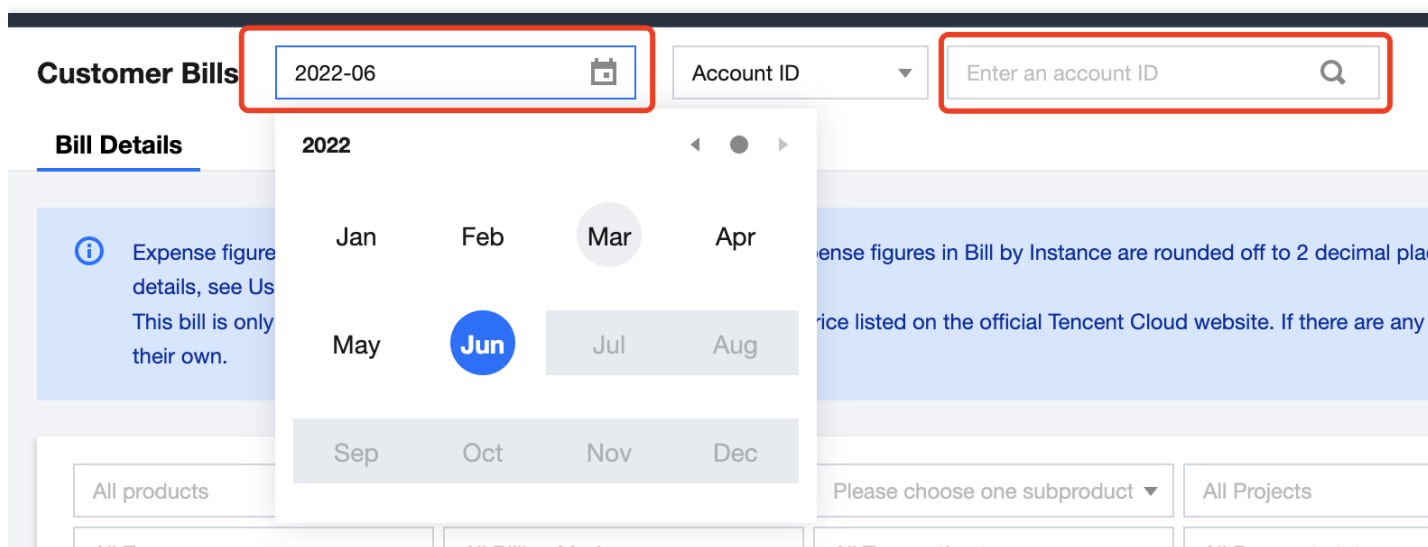
### 1. 子客账单查询

第一步：使用合作伙伴账号登录[腾讯云](#)，进入[伙伴中心](#)。

第二步：点击左侧菜单【客户业务>客户账单】进入子客账单页面。



第三步：选择账单月份及子客UIN/子客名称展示该月份指定子客的信用。





Tencent Cloud

OverviewProducts+87TicketBilling CenterEnglish

Partner Center

OverviewCompany InfoCustomer ManagementBills ManagementVoucher ManagementContract managementCustomer Bills ManagementNEWOrder Management

Customer Bills

2022-06Account ID200022170073Bill Confirmation

Bill Details

Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more details, see User Guide of Current Bills. This bill is only provided for reference. By default, resellers sell at the price listed on the official Tencent Cloud website. If there are any discounts or other requirements, the resellers must modify the bill on their own.

All productsPlease choose one productPlease choose one subproductAll ProjectsAll RegionsAll ZonesAll Billing ModesAll Transaction typesAll Payment statusDo not display \$0 transactions

Total Cost (Including Tax): 6.00000000 USDInstance ID/Instance Name

Instance ID	Instance Name	Product Name	Billing Mode	Project Name	Region	Availability Zone	Subproduct Name	Transaction Type	Transa
ins-ki0pzb8i		Cloud Virtual Machine(CVM)	Pay-As-You-Go ...	default	Guangzhou	Guangzhou Zon...	CVM Standard S5	Hourly settlement	202206
ins-fcjgth4a		Cloud Virtual Machine(CVM)	Pay-As-You-Go ...	default	Guangzhou	Guangzhou Zon...	CVM Standard S5	Hourly settlement	202206
ins-ki0pzb8i		Cloud Virtual Machine(CVM)	Pay-As-You-Go ...	default	Guangzhou	Guangzhou Zon...	CVM Standard S5	Hourly settlement	202206

2. 子客账单下载

经销商可在账单界面列表右上方点击下载按钮对该子客的制定月份账单进行全量下载。

注意：

- 由于当月账单实时变化，暂时不提供下载功能。
- 历史月账单下载时会下载该月全量、全字段数据（界面筛选及定制字段不对下载有影响）。

版权所有：腾讯云计算（北京）有限责任公司

第277 共442页

Tencent Cloud Overview Products + 87 Ticket Billing Center English

**Partner Center**

- Overview
- Company Info
- Customer Management
- Bills Management
- Voucher Management
- Contract management
- Customer Bills Management** NEW
- Order Management

**Customer Bills** 2022-06 Account ID 200022170073 Bill Confirmation

**Bill Details**

Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more details, see User Guide of Current Bills.  
This bill is only provided for reference. By default, resellers sell at the price listed on the official Tencent Cloud website. If there are any discounts or other requirements, the resellers must modify the bill on their own.

All products Please choose one product Please choose one subproduct All Projects All Regions  
All Zones All Billing Modes All Transaction types All Payment status ☐ Do not display \$0 transactions

Total Cost (Including Tax): 6.00000000 USD

The current month's final bill will be generated on the 3 day of the upcoming month.

Instance ID	Instance Name	Product Name	Billing Mode	Project Name	Region	Availability Zone	Subproduct Name	Transaction Type	Transa
ins-ki0pzp8i		Cloud Virtual Machine(CVM)	Pay-As-You-Go ...	default	Guangzhou	Guangzhou Zon...	CVM Standard S5	Hourly settlement	202206
ins-fcjqth4a		Cloud Virtual Machine(CVM)	Pay-As-You-Go ...	default	Guangzhou	Guangzhou Zon...	CVM Standard S5	Hourly settlement	202206
ins-ki0pzp8i		Cloud Virtual Machine(CVM)	Pay-As-You-Go ...	default	Guangzhou	Guangzhou Zon...	CVM Standard S5	Hourly settlement	202206

### 3. 子客账单回款

经销商对子客的历史账单进行回款操作，点击子客账单管理界面右上角“Bill Confirmation”进入回款界面。

Tencent Cloud Overview Products + 87 Ticket Billing Center English

**Partner Center**

- Overview
- Company Info
- Customer Management
- Bills Management
- Voucher Management
- Contract management
- Customer Bills Management** NEW
- Order Management

**Customer Bills** 2022-06 Account ID 200022170073 Bill Confirmation

**Bill Details**

Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more details, see User Guide of Current Bills.  
This bill is only provided for reference. By default, resellers sell at the price listed on the official Tencent Cloud website. If there are any discounts or other requirements, the resellers must modify the bill on their own.

All products Please choose one product Please choose one subproduct All Projects All Regions  
All Zones All Billing Modes All Transaction types All Payment status ☐ Do not display \$0 transactions

Total Cost (Including Tax): 6.00000000 USD

Instance ID	Instance Name	Product Name	Billing Mode	Project Name	Region	Availability Zone	Subproduct Name	Transaction Type	Transa
ins-ki0pzp8i		Cloud Virtual Machine(CVM)	Pay-As-You-Go ...	default	Guangzhou	Guangzhou Zon...	CVM Standard S5	Hourly settlement	202206

通过月份及子客uin对子客月账单进行查询。

Tencent Cloud

预览135516  
5ea53ed145

OverviewProducts+

7TicketBilling CenterEnglish

Partner Center

Overview

Company Info

Customer Management

Bills Management

Voucher Management

Customer Bills Management

Bill Confirmation

Bill Confirmation

After the payment is collected, the credits will be returned to your customer.

2022-05to2022-07800000310739Query

Account ID	Account Name	Bill month	Total Amount	Status	Operation
800000310739		2022-05	0.00 USD	Pending confirmation	Confirm Bill

可以点击列表最右侧的【回款】按钮确认子客该月是否回款，确认后该笔账单的回款将变更为“已回款”并显示回款金额。

# 子客账单字段说明

最近更新时间：2023-09-11 17:03:15

## 账单字段说明

字段	字段说明
Instance ID	实例ID，可以在各产品控制台查看
Instance Name	资源别名，由用户为资源自助设置，未设置则为空
Product Name	云产品大类，产品四层的第1层，如云服务器CVM、云数据库MySQL
Payer Account ID	支付者的账号 ID，账号 ID 是用户在腾讯云的唯一账号标识
Owner Account ID	资源归属者账号ID，此处是子客的ID
Operator Account ID	操作者账号ID，下单购买或开通产品的用户，此处是子客的ID
Reseller Account ID	管理者账号ID，为资源归属者的直接管理经销商ID。
Billing Mode	资源的计费模式，区分为包年包月和按量计费
Instance Type	购买的产品服务对应的实例类型，包括资源包、RI、SP、竞价实例。常规实例类型默认展示为"-"
Project Name	资源所属项目，由用户为资源自助分配，未分配则为默认项目
Region	资源所属地域，例如华南地区（广州）
Availability Zone	资源所属可用区，例如广州三区
Subproduct Name	云产品子类，产品四层的第2层，如云服务器CVM-标准型S1
Transaction Type	资源的购买、开通、续费、退费等交易行为，具体枚举值可参见页面下方《关键字段枚举值说明》
Transaction ID	交易唯一标识
Transaction Time	资源扣费时间
Usage Start Time	资源开始使用时间
Usage End Time	资源结束使用时间
Component Type	组件类型的名称，产品四层的第3层，如CPU、内存、带宽、系统盘等

字段	字段说明
Component Name	组件的名称，产品四层的第4层，如内存-标准型S2、高性能云硬盘-存储空间等
Component List Price	组件的官网原始单价
Component Price Measurement Unit	组件刊例价对应的价格单位
Component Usage	组件的用量
Component Usage Unit	组件用量对应的单位
Usage Duration	资源使用的时长
Duration Unit	资源使用时长的单位
Original Cost	资源的原始总价，等于刊例价 * 用量 * 时长
RI Deduction (Duration)	预留实例抵扣的使用时长，时长单位与被抵扣的时长单位保持一致
RI Deduction (Cost)	本产品或服务使用预留实例抵扣的组件原价金额
Customer Discount Rate	客户折扣率，当前默认为1
Total Amount Before Voucher	卷前总价，本资源未使用代金券前的总金额，等于（原始总价-预留实例抵扣金额）* 客户折扣率
Customer Voucher Deduction	客户代金券支出总额
Total Cost	资源的折后总价，等于券前总价-客户代金券支出
Currency	组件结算使用的货币种类
Payment Status	支付状态
Reseller Discount Rate	伙伴折扣率【注：同计费中心账单字段，下载文件中不包含该字段】
Total Amount After Discount (Excluding Tax)	优惠后总价（不含税）【注：同计费中心账单字段，下载文件中不包含该字段】
Reseller Voucher Deduction	伙伴代金券支出【注：下载文件中不包含该字段】

字段	字段说明
Amount Before Tax	扣完代金券税前金额【注：同计费中心账单字段，下载文件中不包含该字段】
Tax Rate	税率【注：同计费中心账单字段，下载文件中不包含该字段】
Tax Amount	税额【注：同计费中心账单字段，下载文件中不包含该字段】
Total Cost （Including Tax）	资源的折后含税总价，等于组件原价 * 折扣率 * （1+税率），等于组件单价 * 用量 * 时长 * （1+税率）【注：同计费中心账单字段，下载文件中不包含该字段】

字段名称	字段说明
Transaction Type	枚举值如下：Purchase Renewal Modify Refund Deduction Hourly settlement Daily settlement Monthly settlement Offline project deduction Offline deduction adjust-CR adjust-DR One-off RI Fee Spot Hourly RI fee New monthly subscription Monthly subscription renewal Monthly subscription specification adjustment Monthly subscription specification adjustment Monthly subscription refund

# 财务管理

## 折扣管理

最近更新时间：2022-07-08 17:00:59

### 折扣管理

此折扣为腾讯云转售合作伙伴的折扣，即合作伙伴的折扣价。

#### 1、合作伙伴折扣申请

与销售经理线下商定您的折扣，销售经理会提供您完整的产品报价单，包含折扣、优惠等信息。

#### 2、合作伙伴折扣查看

暂不支持线上查看，请联系您的销售经理。

#### 3、合作伙伴折扣调整

请联系您的销售经理，进行商谈和调整。

# 账户信息

最近更新时间：2022-07-11 18:55:47

## 账户管理

### 账户介绍

经销商账户是信用账户，信用额度由您的渠道经理进行管理和调整，经销商可以直接使用，用于给名下的子客消费云服务的代付。如果经销商有自消费行为，也会占用此信用额度。

### 账户充值

经销商可以进行充值操作，当前支持信用卡或银行转账方式。

### 操作步骤

#### 1. 银行转账方式

(1) 使用经销商账号登录腾讯云；

(2) 进入菜单，Billing Center -> Payment Management -> Payment -> [Bank Transfer](#).

(3) 查询和开通专属银行账号

查看判断您的账户是否已经开通了专属银行账号功能，如果已经开通，则可直接获取收款户名、收款账号、收款银行和SWIFT CODE等专属银行收款账户信息。

Credit Card

**Bank Transfer**

Note: If your account has outstanding fees, the system will automatically make the payment for you once receiving your bank transfer.

If you are unable to pay online, you can apply for payment via bank transfer.

1

Transfer money to your Tencent Cloud beneficiary account

Tencent Cloud provides you with a beneficiary account. Once Tencent Cloud received the funds, the system will automatically make the payment for your Tencent Cloud account. The developer and collaborator will see the same beneficiary account.

Transfer method

Online banking/Mobile banking/Wire transfer/Cheque/Over-the-counter cash deposit

Beneficiary name

ACEVILLE PTE.LTD.

Beneficiary Account Number

Beneficiary bank

HSBC, Singapore

SWIFT CODE

HSBCSGSG

2

Bank transfer result feedback

It generally takes one business day to complete the bank transfer, which is subject to the bank system. We will send the result to you via SMS, email or internal message. You can also check the bank transfer status at the [Bank Transfer Query](#).

(4) 使用专属账号进行线下对公打款

根据您的专属银行收款账户信息，您可发起线下对公打款，系统会自动检测，请您打款前务必填写正确。



银行转账时间通常需要3-5个工作日，具体到账时间依赖于银行系统。

#### (5) 打款信息和进度查询

查询打款信息和进度，请前往腾讯云官网费用中心 > 资金管理 > [银企直连](#)。

##### Bank Transfer Query

1. You can pay by Credit Card or Bank Transfer to add your credit balance.
2. After the bank transfer is completed, you can go to the Bank Transfer Query page to check the process status.
3. Bank transfer may incur bank charges. All bank charges will be borne by customers. If you have any questions, please submit a ticket.

Bank Account Name	Bank Account	Accounting Date <sup>+</sup>	Transfer Amount (USD)	Status <sup>▼</sup>	Operation
			0.01	Success	-
Total items: 1			Records per page: 20 <span>1 / 1 page</span>		

(6) 专属银行账号功能目前只支持北美主体和新加坡主体的经销商。如您是欧洲主体的经销商，请按照如下汇款进行打款，打款后联系您的渠道经理，由渠道经理代为充值。

Beneficiary name: TENCENT CLOUD EUROPE B.V.

Beneficiary account: NL49HSBC2031728156 (USD account)

Beneficiary bank: HSBC BANK PLC, Amsterdam z.o. The Netherlands

Address: De Entree 236, 1101 EE Amsterdam

SWIFT Code: HSBCNL2A

Remarks: Cloud service fee + developer account (unique ID)

收款人名称：腾讯云欧洲B.V.

收款人账户：NL49HSBC2031728156（美元账户）

收款银行：阿姆斯特丹汇丰银行有限公司荷兰

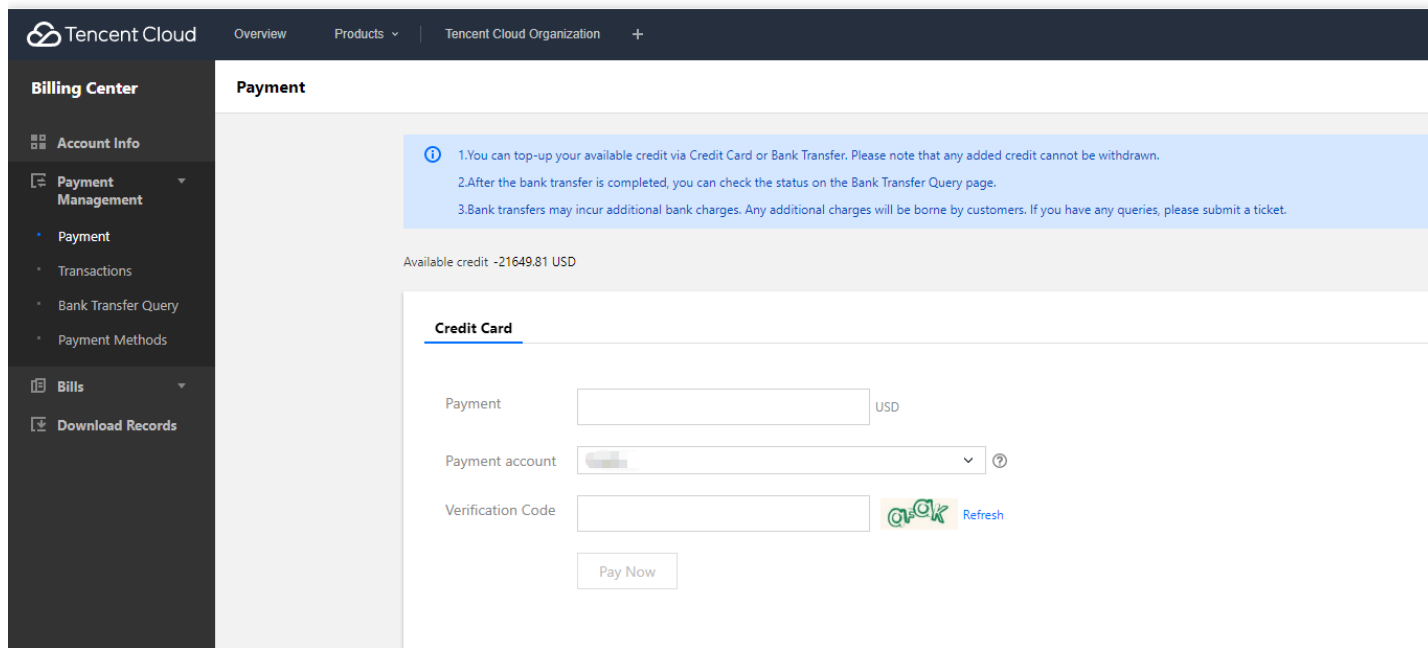
地址：De Entree 236, 1101 EE 阿姆斯特丹

SWIFT 代码：HSBCNL2A

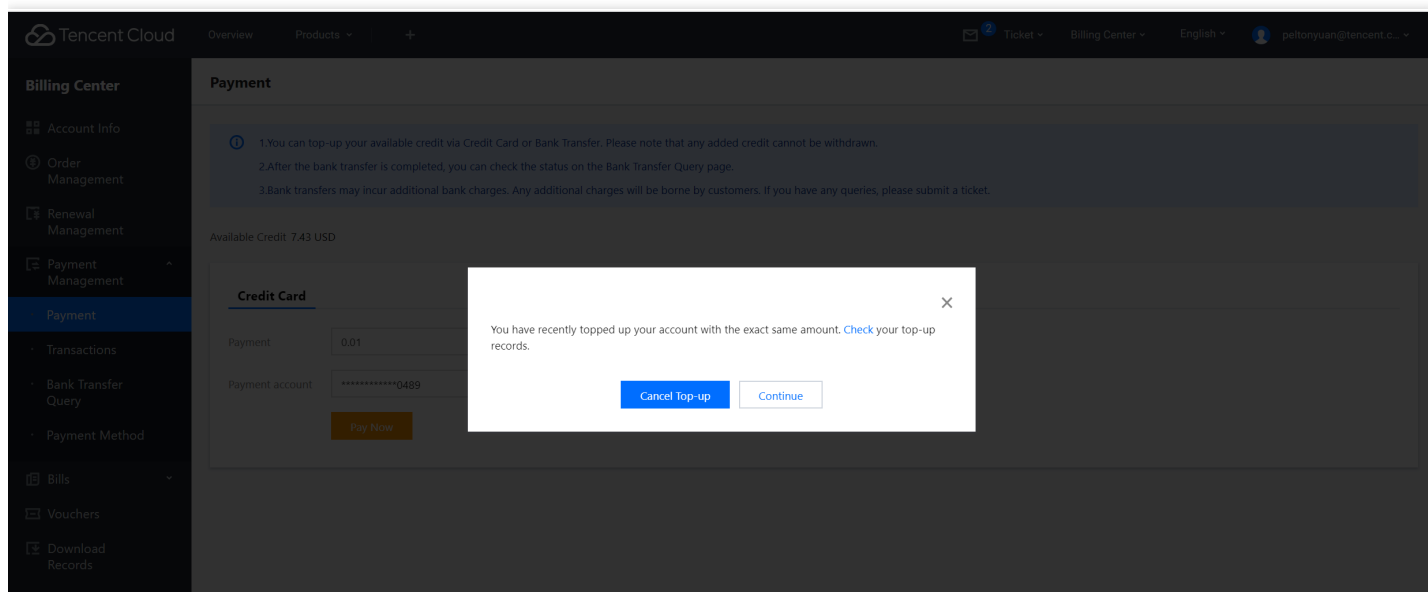
备注：云服务费 + 开发者账户（唯一 ID）

#### 2.信用卡充值方式

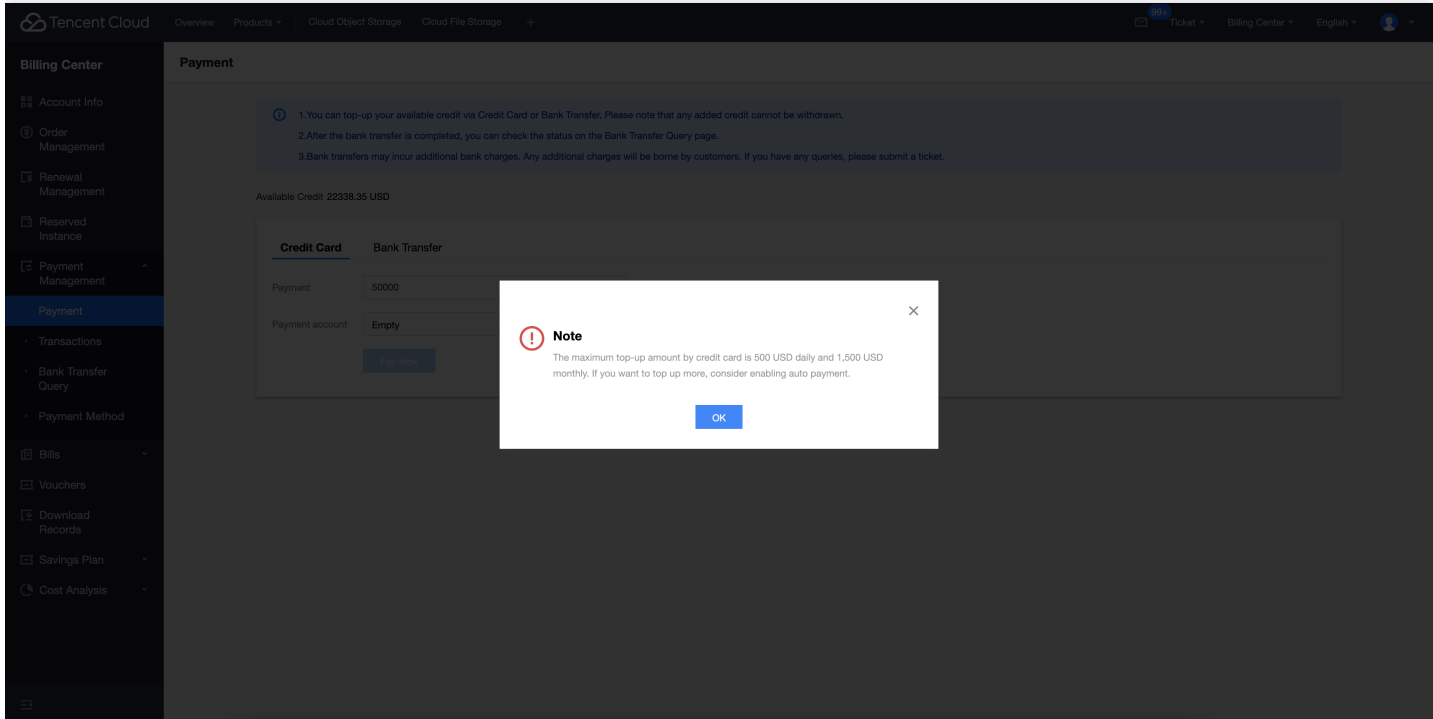
(1) 登录经销商账号登录腾讯云，进入Billing Center -> Payment Management -> Payment。输入充值金额和付款帐户，然后点击立即付款。



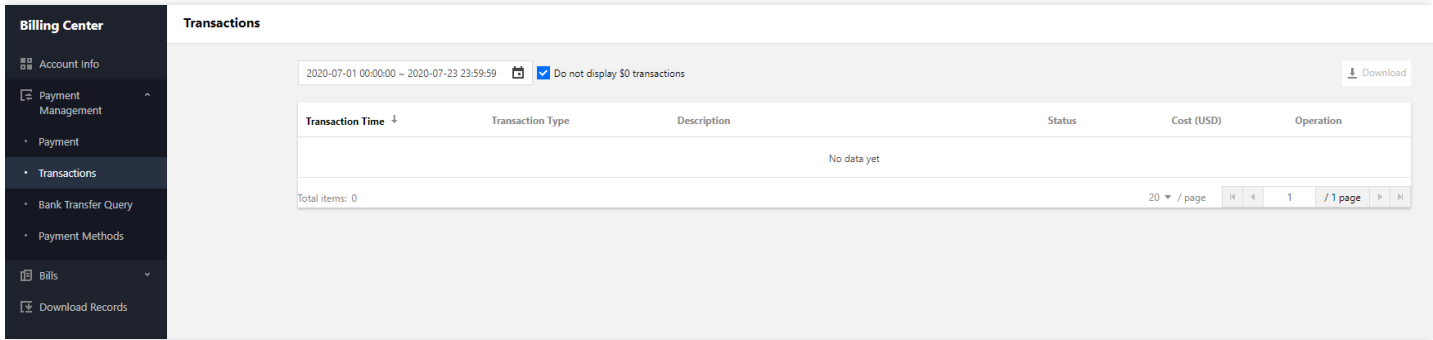
(2) 为避免重复付款，如果您在一分钟内两次充值相同的金额，则会弹出一个确认窗口，要求您进行检查。



(3) 信用卡的最高充值金额为每天500美元，每月1, 500美元。如果您的支出很高，我们的自动付款机制可以帮助您满足您的需求。



(4) 付款后，您可以转到[交易](#)记录以查看付款详细信息。



# 订单管理

最近更新时间：2022-11-22 18:38:17

## 订单管理

”订单管理“是名下的子客购买或开通云服务之后产生的订单。如果经销商有自消费行为，也会产生自付订单。

### 操作步骤

#### 1. 查看子客订单：

- (1) 使用经销商账号登录腾讯云；
- (2) 进入菜单：客户业务>订单管理；
- (3) 子客订单包含：包年包月订单、按量付费订单；
- (4) 子客包年包月订单：经销商可以查看详情，针对“已下单待支付”订单，经销商可以发起代付操作或取消订单；
- (5) 子客按量付费订单：经销商可以查看订单详情。

Prepaid Order

Postpaid Order


This page only shows orders you pay on behalf of others after July 1, 2022. To view your own orders, go to [Order Management](#).

2022-07-04 ~ 2022-07-04

Reseller customer ID/Order ID/Instance ID

Reseller c...	Customer...	Order No.	Product	Subproduct	Type ▾	Creation Date(UTC... ⚙	Status ▾	Order A...	Operation
200022170...	zroozhang	202207040...	cloud bloc...	Premium c...	Purchase	2022-07-04 15:01:33	Finished	0.00000 000	<a href="#">Details</a>
200022170...	zroozhang	202207040...	cloud bloc...	Premium c...	Purchase	2022-07-04 11:22:37 2022-07-19 11:22:37 (Expiry)	Pending payment	0.59500 000	<a href="#">Pay on behalf</a> <a href="#">Cancel</a> <a href="#">Details</a>

Order Details

 **Finished** Amount Paid: 0.59500000 USD

Order No.	20220625974000018562431	Order Type	Purchase
Order Creator	200018967974	Creation Date(UTC+ 8)	2022-06-25 17:05:03
Order Payer	200018967974	Payment Date(UTC+ 8)	2022-06-25 17:05:09

Order Information

Sub-order No.	Product	Specification	Unit Price	Quantity	Payment Mode	Order Amount
20220625974000018562...	cloud block storage Instance ID: <a href="#">disk-qp6lveek</a>	Disk Usage: Data Disk Disk Size: 10 GB Disk Type: Premium Cloud Disk Disk Name: Unnamed Disk Backup Quota: 0 Availability Zone: ap-guangzhou-3	0.70000000 USD/month	x1	By month: 1 month	0.59500000 ⓘ 0.70000000
<div><div>• Tax = (Total Amount - Voucher Deduction) x Tax Rate</div><div>0.00000000 USD 0.59500000 USD 0.00000000 USD 0 %</div></div> <div>Amount Paid: Order(0.59500000 USD)+Tax(0.00000000 USD) ⓘ</div>						

2. 查看经销商自付订单

- (1) 使用经销商账号登录腾讯云；
- (2) 进入菜单：Billing Center -> Order Management；
- (3) 自付订单包含：包年包月订单、按量付费订单；
- (4) 包年包月订单：经销商可以查看详情，针对"已下单待支付"订单，经销商可以发起自付操作或取消订单；

(5) 按量付费订单：经销商可以查看订单详情。

## Order Management

[Prepaid Order](#)
[Postpaid Order](#)

① For orders purchased with a promo voucher, the voucher value will not be refunded if you request a refund.

[Consolidated Payment](#)
[Cancel](#)

2022-04-04 ~ 2022-07-04



<input type="checkbox"/> Order No.	Product	Subproduct	Type ▾	Creation Date(UT... ⚙	Status ▾	Order Amo...	Operation
<input type="checkbox"/> 20220625974000018581621	Message ...	ckafka-profession	Return	2022-06-25 18:38:17	Finished	-340.26678400	<a href="#">Details</a>
<input type="checkbox"/> 20220625974000018551381	Message ...	ckafka-profession	Purchase	2022-06-25 18:24:07	Finished	352.00000000	<a href="#">Details</a>
<input type="checkbox"/> 20220625974000018562431	cloud blo...	Premium cloud bloc...	Purchase	2022-06-25 17:05:03	Finished	0.59500000	<a href="#">Details</a>
<input type="checkbox"/> 20220625974000018562201	cloud blo...	Premium cloud bloc...	Purchase	2022-06-25 16:58:25	Finished	0.59500000	<a href="#">Details</a>

Total items: 4

20 / page

1 / 1 page

## Order Management

[Prepaid Order](#)
[Postpaid Order](#)

2022-06-26 ~ 2022-06-30



Order No.	Product	Subproduct	Type ▾	Creation Date(UTC... ⚙	Status ▾	Operation
20220627115483	Cloud Virtual Machine(CVM) cloud block storage	CVM Standard S5 Premium cloud block storage	Purchase	2022-06-27 15:38:26	Processing succeeded	<a href="#">Details</a>

Total items: 1

10 / page

1 / 1 page

# 账单管理

## 经销商账单

最近更新时间：2022-07-20 10:02:58

## 账单管理

### 查看账单

经销商账单是名下的子客消费云服务产生的账单，经销商可基于该账单还款或申请发票。如果经销商有自消费行为，也会产生自付账单。

注意：

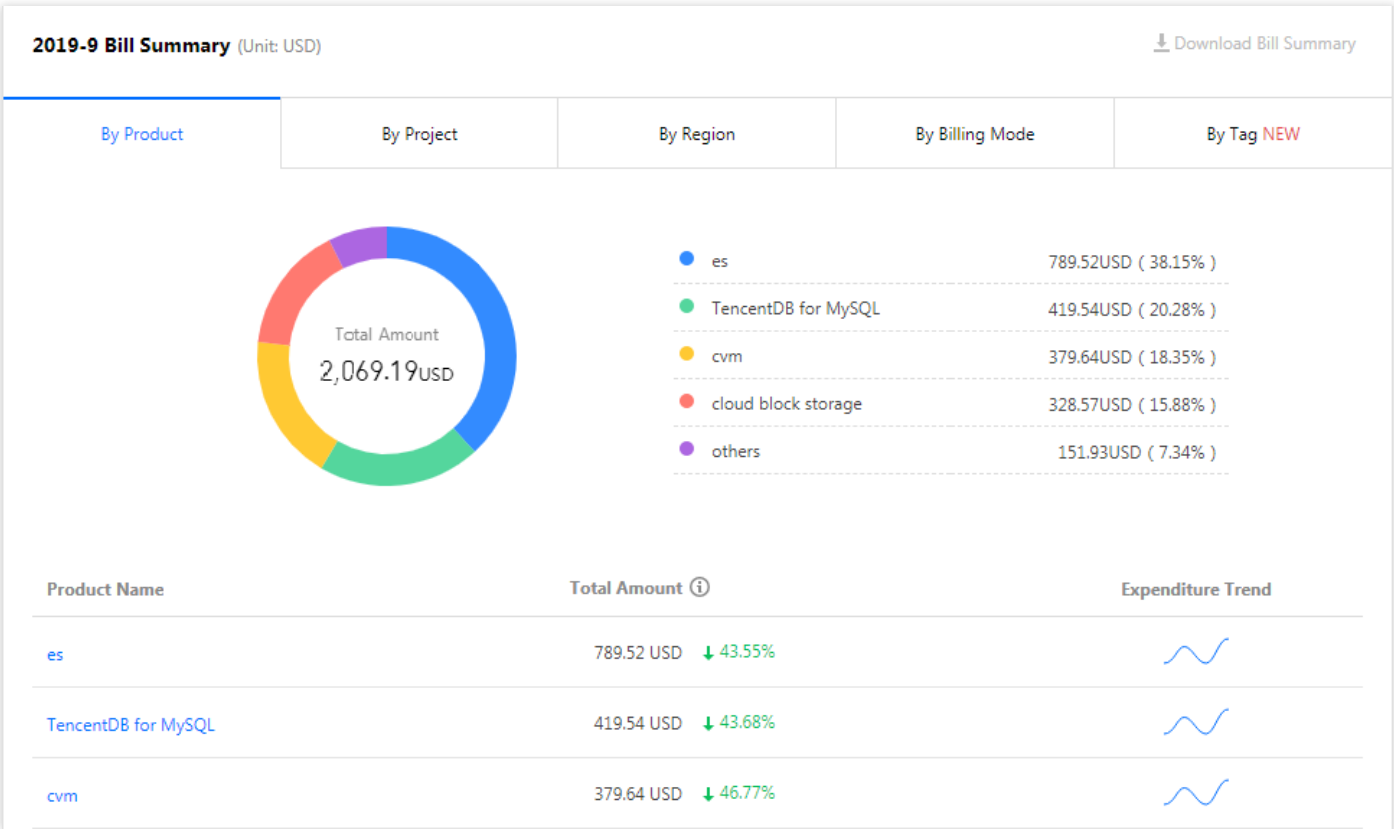
- 腾讯云国际的所有结算日期和时间均以北京时间（UTC+08：00）为准。
- 账单在每个月的第2天或第3天生成。实际日期以账单中心账单管理页面显示的通知为准。任何先前显示的账单信息仅供参考。

### 操作步骤

- 1、使用经销商账号登录腾讯云；
- 2、进入菜单：Billing Center -> Bills-> Overview
- 3、按产品分类汇总

- 您可以查看产品的每月成本及其百分比、上个月的成本差异以及过去六个月的项目/产品成本趋势。

- 单击产品名称，进入账单明细页面，查看相应资源的成本。

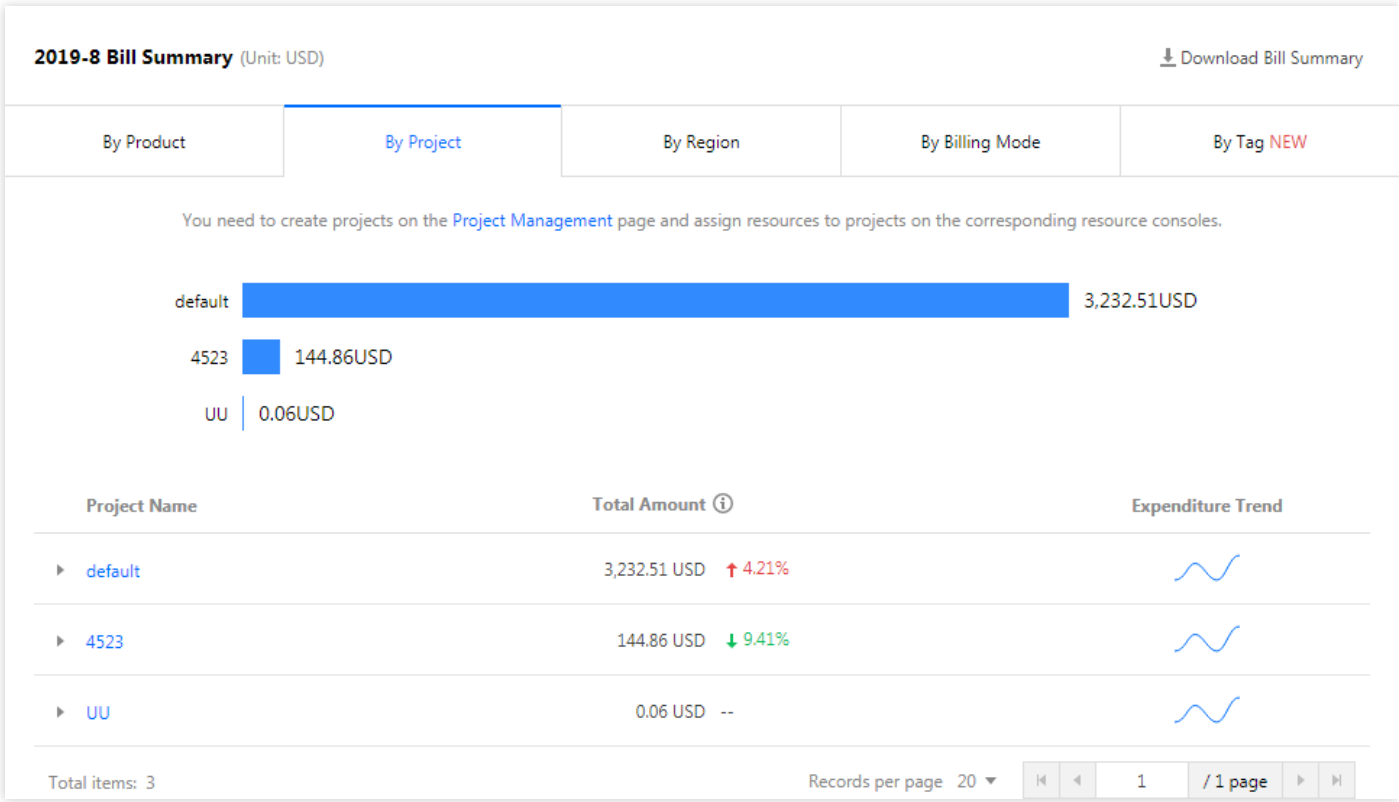


4、按项目分类汇总。

- 您可以查看产品的每月成本及其百分比、上个月的成本差异以及过去六个月的项目/产品成本趋势。



- 单击项目名称左侧的箭头以查看产品详细信息。单击项目/产品名称，进入账单明细页面，查看相应资源的成本。

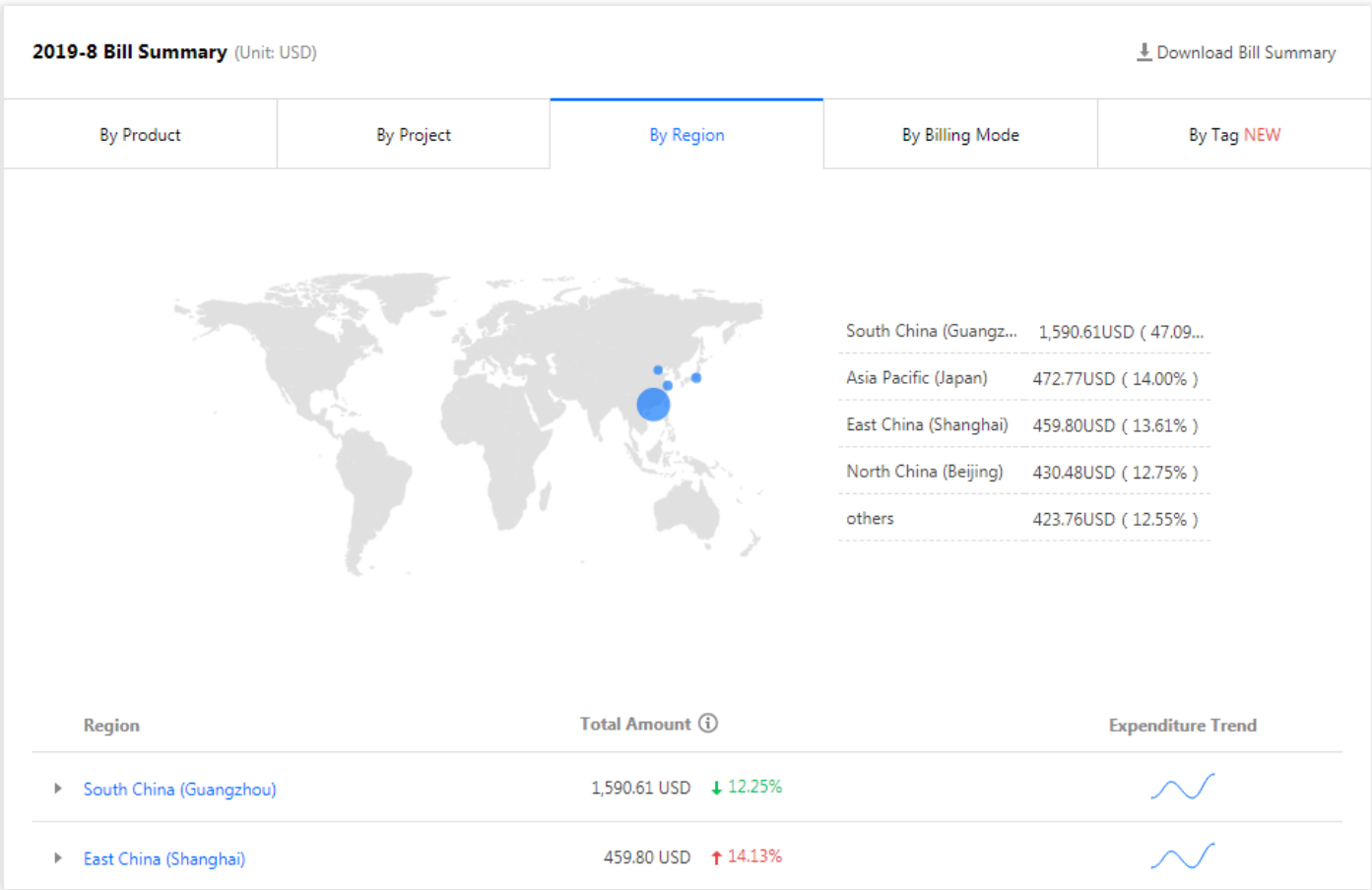


5、按地区汇总

该账单按地区细分。

- 您可以查看产品的每月成本及其百分比、上个月的成本差异以及过去六个月的区域/产品成本趋势。

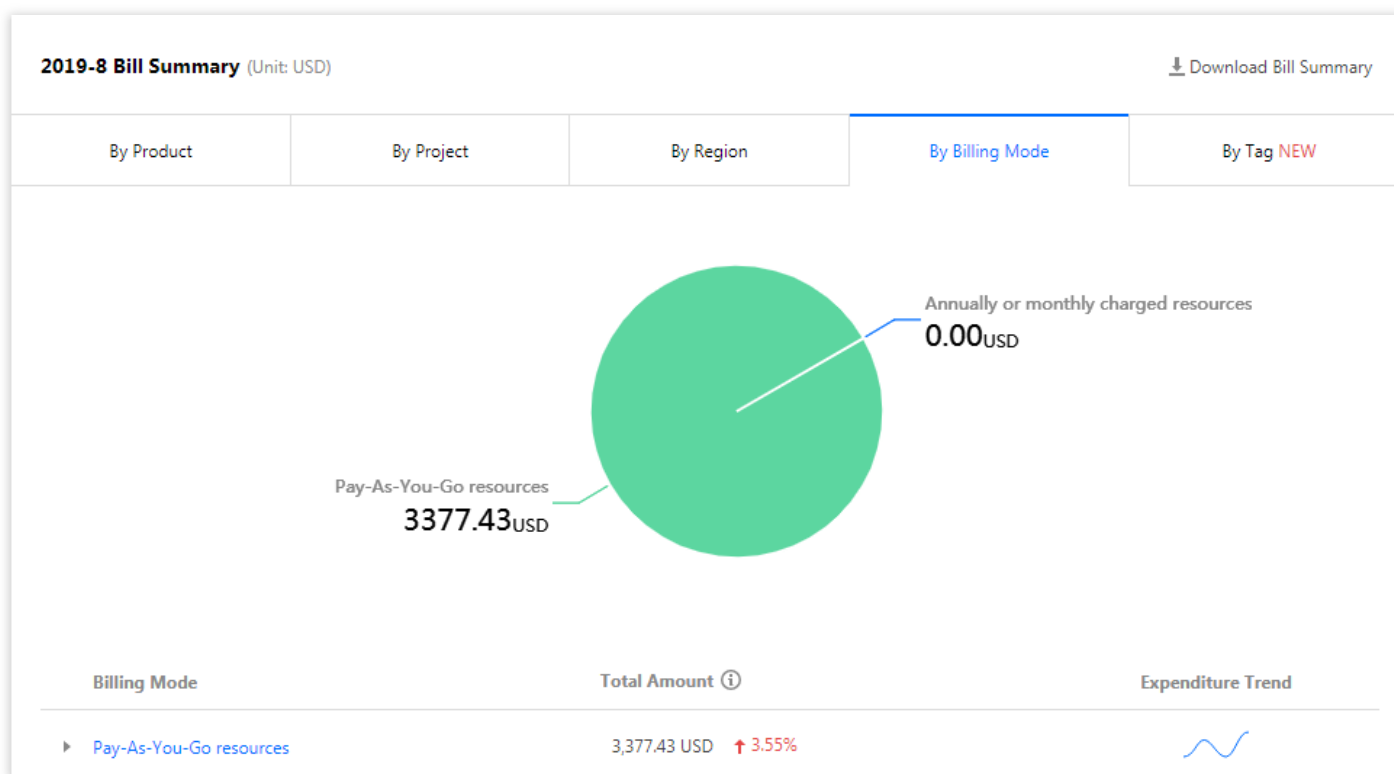
- 单击区域左侧的箭头可查看产品详细信息。单击地域/产品名称，进入账单明细页面，查看相应资源的成本。



6、按计费模式汇总

账单按计费模式细分。

- 您可以查看产品的每月成本及其百分比、上个月的成本差异以及过去六个月的计费模式/产品成本趋势。
- 单击计费模式左侧的箭头以查看产品详细信息。单击计费方式/产品名称，进入账单明细页面，查看相应资源的成本。



## 账单下载

经销商可以下载自账单 3.0（2021 年 7 月发布）以来的账单数据。具体而言，您可以：

1. 下载账单包、PDF 账单（L0）、账单摘要（L1）、按实例划分的账单（L2）和账单详情（L3）
2. 下载多个月的账单数据
3. 下载汇总账单数据（每小时/每日计费产品的数据可在下载前按月汇总，以减少账单条目数量）

## 操作步骤

- 1、使用经销商账号登录腾讯云；
- 2、进入菜单：Billing Center -> Bills-> Bill Download
- 3、PDF 账单（L0）

使用案例：L0账单为PDF格式，可用于付款请求或存档。您可以一次下载多个月的L0账单。

L0: PDF Bills

L1: Bill Summary

L2: Bill by Instance

L3: Bill Details

L0 bills are in PDF format and can be used for payment requesting or archiving.

Period

2021-12

to

2021-12

Account No

3465611991@qq.com (200000095802)

☐ Include sub-accounts

Download

#### 4、账单摘要（L1）

使用案例：L1 账单按产品、项目、区域、标签等提供账单数据，允许您按不同指标查看账单信息。您可以在一个文件中下载多个月的账单摘要，并可以指定是否聚合不同账户的数据。例如，您可以按产品下载过去 6 个月内某个账户的账单摘要。

L0: PDF Bills

L1: Bill Summary

L2: Bill by Instance

L3: Bill Details

L1 bills offer bill data by product, project, region, tag, etc., allowing to view bill information by different metrics.

Period

2021-12

to

2021-12

Account No

3465611991@qq.com (200000095802)

☐ Include sub-accounts

Download

#### 5、按实例计费（L2）

使用案例：L2 账单按实例（资源）ID 提供账单数据。您可以将多个月的L2账单下载到一个文件中，并可以指定是否聚合不同账户的数据。

L0: PDF Bills

L1: Bill Summary

L2: Bill by Instance

L3: Bill Details

L2 bills offer bill data by resource ID (instance).

Period

2021-12

to

2021-12

Account No

3465611991@qq.com (200000095802)

☐ Include sub-accounts

Download

#### 6、账单明细（L3）

使用案例：L3 账单在组件级别提供账单数据。您可以一次下载多个月的L3账单，并可以指定是否按月聚合数据。

L0: PDF Bills

L1: Bill Summary

L2: Bill by Instance


**L3: Bill Details**

i

L3 bills offer bill data at the finest granularity. For example, if a product is billed hourly, a bill entry will be generated per hour for each component.


Period

2021-12



to

2021-12



You can download bill details of up to 6 months at a time.

Account No

3465611991@qq.com (200000095802)


☐ Include sub-accounts

Aggregate

☒ Show details

☐ By month

[About Aggregation](#)



Download

# 账单字段说明

最近更新时间：2022-12-26 11:50:16

## 账单字段说明

字段	描述
Payer Account ID	支付者账号，是经销商账号
Owner Account ID	资源归属者账号，是子客账号
Operator Account ID	操作者账号，可以是子客账号、子客对应的cam子用户、子客的协作者
ProductName	产品名称
BillingMode	计费模式 Monthly subscription 包年包月 Pay-As-You-Go resources 按量计费 Standard RI 预留实例
ProjectName	项目名称
Region	资源所属区域
Availability Zone	资源所属可用区
InstanceId	实例ID
InstanceName	实例名称
SubproductName	子产品名
TransactionType	结算类型
TransactionID	交易流水ID
TransactionTime	结算时间
Usage Start Time	资源开始使用时间
Usage End Time	资源结束使用时间
ComponentType	组件
ComponentName	组件名称
Component List Price	组件刊例价

字段	描述
Component Contracted Price	组件合同签约价 $\text{Component Contracted Price} = \text{Component List Price} * \text{DiscountRate}$
Component Price Measurement Unit	价格单位
Component Usage	组件用量
Component Usage Unit	组件用量单位
Usage Duration	资源使用时长
Duration Unit	时长单位
Reserved Instances	预留实例
OriginalCost	原始总价 $\text{Original Cost} = \text{Component List Price} * \text{Component Usage} * \text{Usage Duration}$
DiscountRate	伙伴折扣
Currency	币种
Total Amount After Discount (Excluding Tax)	折后税前总费用 $\text{Total Amount After Discount (Excluding Tax)} = \text{OriginalCost} * \text{DiscountRate}$
Voucher Deduction	代金券扣减金额
Amount Before Tax	扣完代金券税前金额 $\text{Amount Before Tax} = \text{Total Amount After Discount (Excluding Tax)} - \text{Voucher Deduction}$
TaxRate	税率 合作伙伴所在国家税率
TaxAmount	税额 $\text{TaxAmount} = \text{Amount Before Tax} * \text{TaxRate}$
Total Cost (Including Tax)	含税总额 $\text{Total Cost (Including Tax)} = \text{Amount Before Tax} + \text{TaxAmount}$

# 账单存至COS存储桶

最近更新时间：2022-07-08 17:25:09

请查看此[文档](#)。



# COS存储桶API获取账单

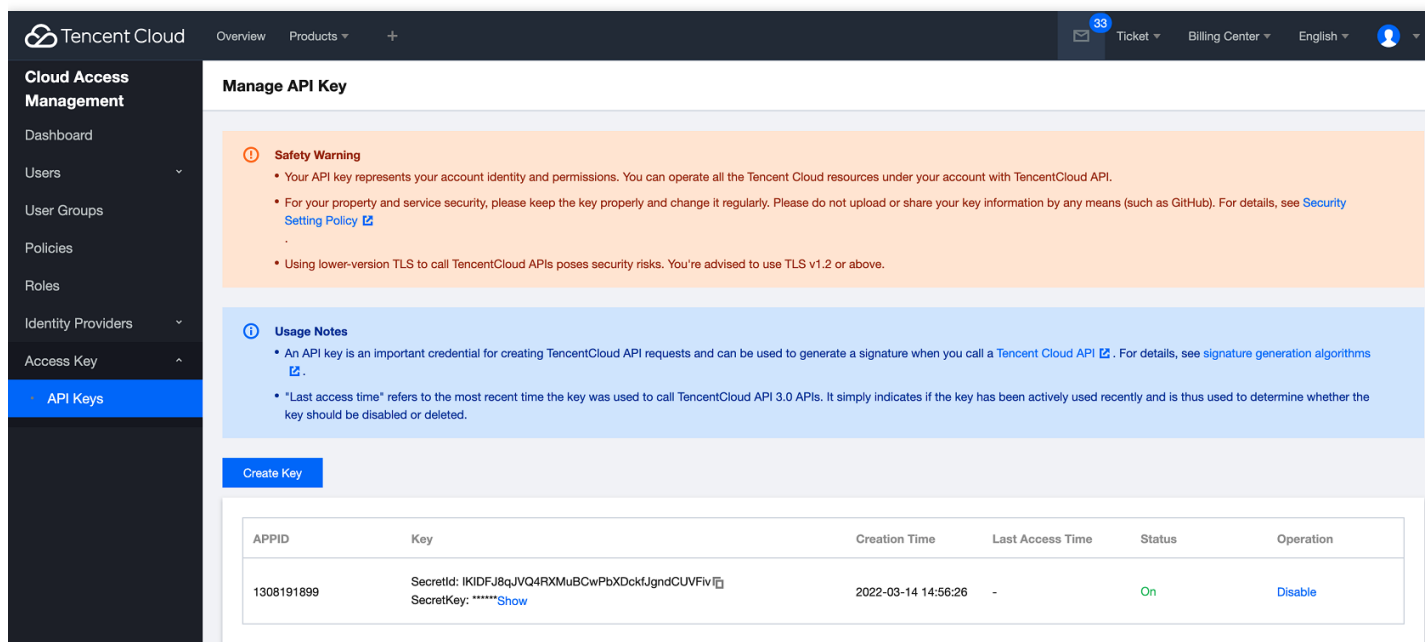
最近更新时间：2022-07-11 14:22:53

## COS存储桶API获取账单

第一步：完成存储桶的创建、存储桶的授权，详情请查看[账单存至COS存储桶](#)。

第二步：申请API访问腾讯云的key。

1. 登录 [这里](#)。
2. 点击**Create Key**创建一个新的Key，需填写手机验证码。



**Manage API Key**

**Safety Warning**

- Your API key represents your account identity and permissions. You can operate all the Tencent Cloud resources under your account with TencentCloud API.
- For your property and service security, please keep the key properly and change it regularly. Please do not upload or share your key information by any means (such as GitHub). For details, see [Security Setting Policy](#).
- Using lower-version TLS to call TencentCloud APIs poses security risks. You're advised to use TLS v1.2 or above.

**Usage Notes**

- An API key is an important credential for creating TencentCloud API requests and can be used to generate a signature when you call a [Tencent Cloud API](#). For details, see [signature generation algorithms](#).
- "Last access time" refers to the most recent time the key was used to call TencentCloud API 3.0 APIs. It simply indicates if the key has been actively used recently and is thus used to determine whether the key should be disabled or deleted.

**Create Key**

APPID	Key	Creation Time	Last Access Time	Status	Operation
1308191899	SecretId: IKIDFJ8qJVQ4RXMuBCwPbXDckfJgndCUVfiv SecretKey: ***** <a href="#">Show</a>	2022-03-14 14:56:26	-	On	<a href="#">Disable</a>

第三步：API获取账单压缩包名称

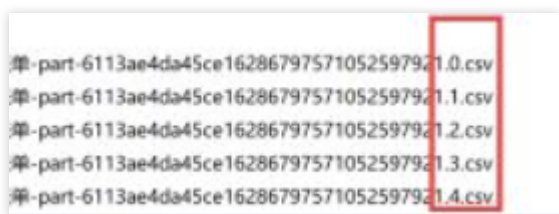
注意：  
以下两步参考示例代码

### 1. API文档

2. 使用上述列出文件列表的api，支持前缀、路径过滤

3. 根据列表中的文件及约定好的命名规则提取需要下载的文件列表（文件命名请参考示例）

存储桶文件类型	文件命名	文件格式	上传时间	备注
日明细账单（包含伙伴自用账单+代替子客支付的账单）	200020475883-20210810-bill_details.zip	ZIP	2021-08-11 15:45:00	Day+1上午3点（每月1日出账日为20点），新增的账单明细会存储到 COS 存储 Bucket 中。解压后包含1个CSV文件，如果明细量级超过excel最大行数，会拆成多个CSV文件，如下图。
月明细账单（包含伙伴自用账单+代替子客支付的账单）	200018967974-202201-by_used_time-bill_details.zip	ZIP	2021-08-11 15:45:00	每月2号，更新一份完整的上月账单明细。解压后包含1个CSV文件，如果明细量级超过excel最大行数，会拆成多个CSV文件，如下图。



#### 第四步：API下载压缩包

##### 1. API文档

2. 使用上述下载api下载文件到本地，传入参数（要下载的文件名、本地路径）

3. 自行编写解压读取csv代码

说明：

- 1、存储桶账单字段说明，请参考[账单详情](#)。
- 2、建议每月3日调用接口，获取上月月明细账单。不是最终的本月账单费用，仅供参考。
- 3、明细账单费用最多支持8位小数，资源ID账单展示的费用为四舍五入后保留2位小数的费用，实际从账户扣费时按2位小数进行扣费（即扣到分）。
- 4、如果需要区分自用账单、子客账单，可通过UIN过滤区分。

# 结算管理

## 发票管理

最近更新時間：2022-07-11 19:08:55

### 发票管理

经销商可以按账单向腾讯云索取发票。

### 操作步骤

- 1、使用经销商账号登录腾讯云，进入Billing Center -> Bills -> Invoicing
- 2、验证您的身份：经销商需要在提交第一个发票请求之前[完成身份验证](#)。
- 3、填写信息：转到账单中心>账单>发票，然后在“发票设置”区域中填写发票信息。

注意：

如果注册您账户的实体位于欧洲（VAT）或新加坡（GST），则您还需要在控制台中输入该实体的税号。请务必输入正确的税号，否则可能无法提交纳税申报表。

**Invoice Settings**

Invoice Title \*

Email \*

**GST Number \***

Note: the GST number will be displayed on your invoice. An incorrect GST number will affect your tax declaration.

Auto Invoicing ☒ After you enable this, the system will invoice the bills of the last month on the 6th day of the current month and send the invoice to your email address in 3 to 5 days.

[Save](#)

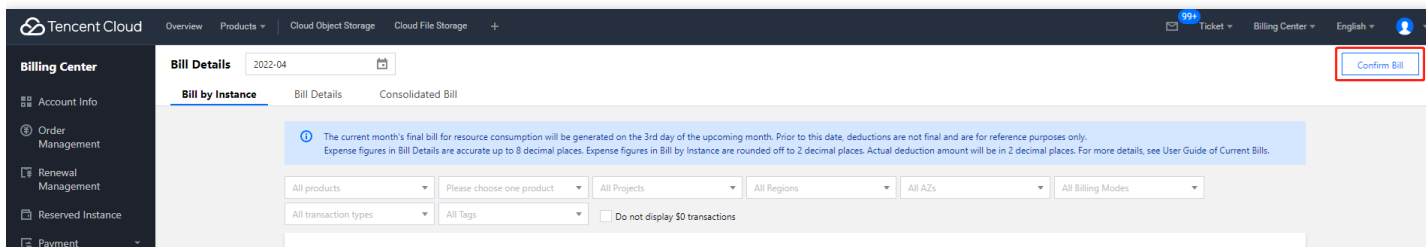
**Invoice History** You can request for invoicing or download bills of the last 6 months.

Billing Period	Application Time	Invoice Status	Invoiced Amount (USD)	Operation
2022-03	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2022-02	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2022-01	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-12	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-11	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-10	-	Not invoiced	-	<a href="#">Apply for Invoice</a>

- 4、查看您的月度账单：账单在每个月第 2 天或第 3 天生成。请务必及时[检查您的账单](#)。

注意：

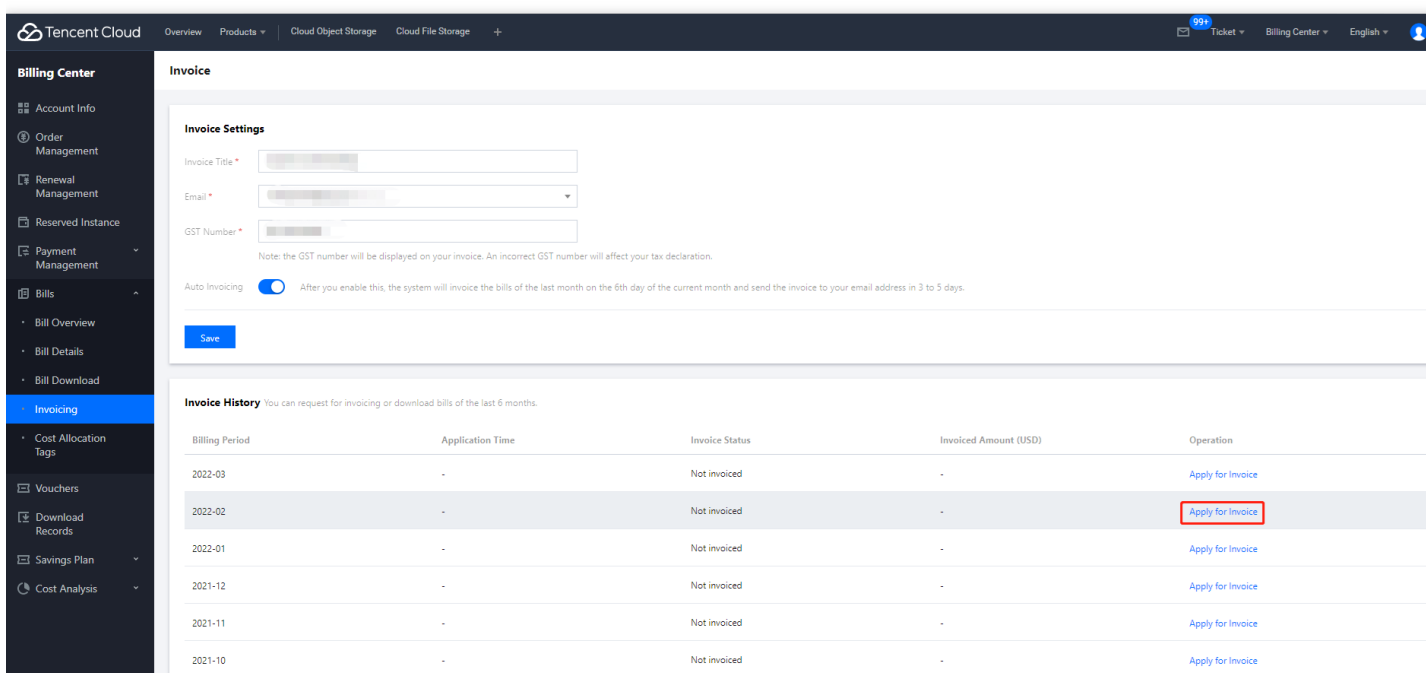
如果找不到用于确认帐单信息的按钮，请继续执行下一步。



## 5、申请发票：找到您要申请发票的月份，然后点击申请发票。

注意：

您只能申请过去六个月的发票。提交请求后，发票将在 2-3 小时内发送到您的电子邮件收件箱。



## 6、查看/下载发票：检查收件箱以下载发票。您也可以在控制台中下载它。

### 自动开具发票

默认情况下，“自动开票”复选框处于未选中状态。如果您选择它，在每个月的第6天，系统将自动为您上个月的交易开具发票（PDF），并在1-3个工作日内将副本发送到您的收件箱。

Tencent Cloud

OverviewProductsCloud Object StorageCloud File Storage

99+TicketBilling CenterEnglish

Billing Center

Account Info
Order Management
Renewal Management
Reserved Instance
Payment Management
Bills
Bill Overview
Bill Details
Bill Download
Invoicing
Cost Allocation Tags
Vouchers
Download Records
Savings Plan
Cost Analysis

Invoice

Invoice Settings

Invoice Title \*

Email \*

GST Number \*

Note: the GST number will be displayed on your invoice. An incorrect GST number will affect your tax declaration.

Auto Invoicing

After you enable this, the system will invoice the bills of the last month on the 6th day of the current month and send the invoice to your email address in 3 to 5 days.

Save

Invoice History

You can request for invoicing or download bills of the last 6 months.

Billing Period	Application Time	Invoice Status	Invoiced Amount (USD)	Operation
2022-03	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2022-02	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2022-01	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-12	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-11	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-10	-	Not invoiced	-	<a href="#">Apply for Invoice</a>

## 申请过去几个月的发票

转到“帐单中心”，然后选择“帐单>帐单开票”。找到您要申请发票的月份，然后点击申请发票。您只能申请过去六个月的发票。提交请求后，发票将在 2-3 小时内发送到您指定的电子邮件地址。如果您在收件箱中找不到发票，也可以从控制台的发票页面下载。

Tencent Cloud

OverviewProductsCloud Object StorageCloud File Storage

99+TicketBilling CenterEnglish

Billing Center

Account Info
Order Management
Renewal Management
Reserved Instance
Payment Management
Bills
Bill Overview
Bill Details
Bill Download
Invoicing
Cost Allocation Tags
Vouchers
Download Records
Savings Plan
Cost Analysis

Invoice

Invoice Settings

Invoice Title \*

Email \*

GST Number \*

Note: the GST number will be displayed on your invoice. An incorrect GST number will affect your tax declaration.

Auto Invoicing

After you enable this, the system will invoice the bills of the last month on the 6th day of the current month and send the invoice to your email address in 3 to 5 days.

Save

Invoice History

You can request for invoicing or download bills of the last 6 months.

Billing Period	Application Time	Invoice Status	Invoiced Amount (USD)	Operation
2022-03	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2022-02	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2022-01	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-12	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-11	-	Not invoiced	-	<a href="#">Apply for Invoice</a>
2021-10	-	Not invoiced	-	<a href="#">Apply for Invoice</a>

# 返佣管理

## 对账单管理

最近更新时间：2022-09-23 11:38:02

## 对账单管理

### 对账单说明

经销商返佣对账单是符合腾讯返佣激励政策规则条件下产生的返佣对账结果，经销商可基于该对账单进行下载，核对和确认。

注意：

- 对账单下载的结果与对账单明细数据结果一致。
- 账单欠费意味着客户尚未完成付款，我们会在付款完成后发起返佣对账单付款。
- 合同尚未归档意味着合同流程尚未完成，我们会在合同完成后发起返佣对账单付款。
- 如果您对返佣对账单有任何疑问，请发送邮件到intl\_cloudpartner@tencent.com邮箱咨询。

### 操作步骤

- 使用经销商账号登录腾讯云
- 进入菜单：**Partner Center -> Rebate Management -> Statement**
- 对账单相关操作：

Commission Month	Statement Amount	Adjustment Amount	Reason for Adjustment	Actual Commission Amount	Creation Time	Confirmation Status	Confirmation Time	Operation
2022-09					2022-07-12 08:07:00	To be confirmed		<a href="#">Details</a> <a href="#">Download</a> <a href="#">Confirm</a>

Total items: 1

- 查看明细：点击后跳转到返佣明细进行查看。

- 对账单下载：下载对应月份的对账单excel。
- 对账单确认：对账单核对后完成对账确认，必须在对账单产生15天内完成对账确认或拒绝，如未按时完成会默认账单确认。

Tencent Cloud

OverviewProducts

Partner Center

Overview

Company Info

Customer Management

Customer Bids

Download Resource

Commission Management

Statement

Commission Details

Commission Management / Statement

Note

1. The data on the statement download page is consistent with that on the statement details page.

2. An overdue bill indicates that the customer hasn't paid the bill. We will issue a commission statement after the bill is paid.

3. An unconfirmed account indicates the confirm process hasn't been completed. We will issue a commission statement after the confirm process is completed.

4. If you have any questions about commission statements, contact us at the email address: bill\_statement@tencent.com.

Commission Month	Statement Amount	Adjustment Amount	Reason for Adjustment	Actual Commission Amount	Creation Time	Confirmation Status	Confirmation Time	Operation
2020-01	3164.00	0.00		3164.00	2020-07-12 06:07:00	To be confirmed		DetailsDownloadConfirm

Please click "Confirm" if the statement is correct. If you need to adjust the statement, click "Reject" and contact us via email as soon as possible. You must confirm or reject the statement in 15 days after it is issued; otherwise, it will be confirmed by default.

ConfirmReject

Total Rows: 1

10 / page121 / 1 page

# 返佣明细

最近更新时间：2022-09-21 16:03:57

## 返佣明细

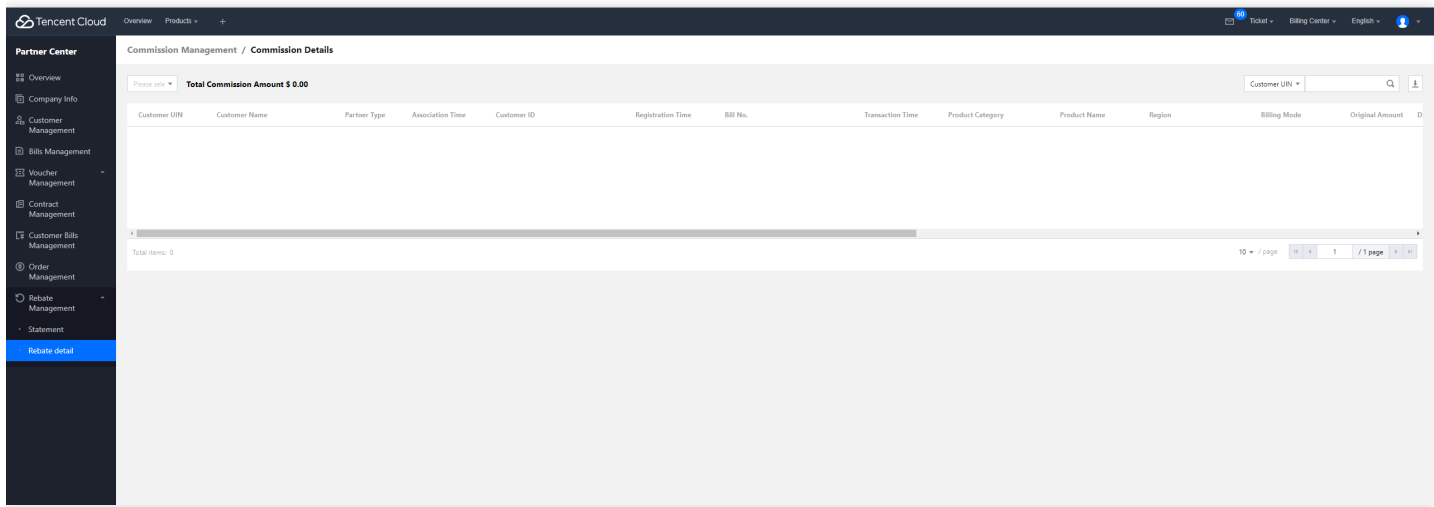
### 返佣明细说明

经销商返佣对明细是符合腾讯返佣激励政策规则条件下产生的返佣对账明细结果，明细数据与账单对应，经销商可基于该明细数据进行详细核对。

### 操作步骤

- 1、使用经销商账号登录腾讯云
- 2、进入菜单：**Partner Center -> Rebate Management-> Rebate Detail**
- 3、返佣明细相关操作：

- 查看明细：按照月份查看返佣明细，此明细与对账单下载总数一致，仅数据颗粒度不同。
- 明细下载：下载对应月份明细的查询结果数据。





# 协议管理

## 业务相关

### 腾讯云国际合作伙伴条款

最近更新时间：2024-02-20 14:49:20

Welcome your participation in Tencent Cloud Partner Program!

#### PLEASE READ THESE TERMS CAREFULLY

YOUR PARTICIPATION IN THE TENCENT CLOUD PARTNER PROGRAM AND YOUR ACCESS AND USE OF THE TENCENT CLOUD PARTNER CONSOLE IS SUBJECT TO THESE TERMS AND CONDITIONS (THESE “**TERMS**”). DO NOT PARTICIPATE IN TENCENT CLOUD PARTNER PROGRAM OR ACCESS TENCENT CLOUD PARTNER CONSOLE IF YOU DO NOT AGREE TO THESE TERMS IN FULL.

BY CLICKING “AGREE” BUTTON BELOW, YOU REPRESENT AND WARRANT THAT YOU HAVE READ AND UNDERSTOOD THESE TERMS AND YOU ARE DULY AUTHORISED TO ACT ON BEHALF OF THE ENTITY APPLYING TO PARTICIPATE IN THE TENCENT CLOUD PARTNER PROGRAM AND TO ENTER INTO THESE TERMS AND LEGALLY BIND SUCH ENTITY (“**PARTNER**”) TO THESE TERMS. IF YOU ARE NOT AUTHORISED TO BIND THE PARTNER OR DO NOT AGREE TO THESE TERMS IN FULL, DO NOT CLICK THE “AGREE” BUTTON BELOW AND DO NOT ACCESS THE PARTNER PORTAL.

#### WHO WE ARE AND WHAT THESE TERMS DO

DEPENDING ON WHERE PARTNER IS DOMICILED, “WE”, “US’ OR “TENCENT” IN THESE TERMS MEANS THE FOLLOWING TENCENT ENTITY:

DOMICILE	TENCENT ENTITY
If Partner is domiciled in European Economic Area, UK and Switzerland	<b>Tencent Cloud Europe B.V.</b> , a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands
If Partner is domiciled in North America	<b>Tencent Cloud LLC</b> , a Delaware corporation registered company located at Claremont2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America
If Partner is domiciled in South Korea	<b>Tencent Korea Yuhan Hoesa</b> , 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

DOMICILE	TENCENT ENTITY
If Partner is domiciled in rest of the world except the People's Republic of China	<b>Aceville Pte Ltd</b> , a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622

THESE TERMS GOVERN YOUR ACCESS AND USE OF TENCENT CLOUD PARTNER CONSOLE AND YOUR PARTICIPATION IN THE TENCENT CLOUD PARTNER PROGRAM. YOU ACKNOWLEDGE AND AGREE THAT TENCENT MAY AMEND THESE TERMS AT ANY TIME BY POSTING THE UPDATED TERMS ON THE PARTNER CONSOLE AND WILL BE EFFECTIVE IMMEDIATELY UPON POSTING.

## ADDITIONAL TERMS AND POLICIES

We offer a diverse range of benefits and training through the Partner Program, and depending on the Partner Type in which you participate in, there may be additional terms and policies that are applicable to your use of such benefits and training, and Partner Type activities ("Additional Terms"). You agree to comply with these Terms and all additional terms that are applicable to your Partner Benefits, Partner Type and training through your participation in the Partner Program and all relevant Additional Terms are incorporated by reference into these Terms.

Additional Terms may include additional agreements and policies that apply to your participation in Partner Program, depending on your Partner Type as follows:

- Tencent Cloud Referral Agreement
- Tencent Cloud Reseller Agreement
- Tencent Cloud Sales Agent Agreement
- Tencent Cloud International Partner Academy Terms of Service
- Tencent Cloud Voucher Terms and Conditions
- Tencent Cloud Partner Data Processing Agreement

## 1.DEFINITIONS

(a) "**Applicable Data Protection Laws**" means, in respect of a Party, any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument relating to the protection of Personal Data, in each case as amended, consolidated, re-enacted or replaced from time to time, including but not limited to, as applicable, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the UK Data Protection Act 2018 ("**UK DPA**"), the UK General Data Protection Regulation as defined by the UK DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, and the Privacy and Electronic Communications Regulations 2003, the California Consumer Privacy Act ("**CCPA**").

(b) "**Console Documentation**" means the information relating to the user guides, pricing, operation, support, functions of Tencent Services, Partner Program and the Partner Console that are made available via the Partner Console.

(c) "**Customer**" means a customer of Partner who purchases Tencent Services through Partner or referred to Tencent

by Partner, as part of the Partner Program where Partner is one of the Partner Type under the Partner Program.

(d) **“European Economic Area”** means the member countries of the European Union specified in the official website of the [European Union](#).

(e) **“Intellectual Property Rights”** means all intellectual property rights including, without limitation, rights with respect to trademarks, copyrights, patents, trade secrets, know-how, databases, registered designs, moral rights and trade dress, whether registered, registrable or unregistered, under all applicable laws worldwide.

(f) **“North America”** means Canada and the United States of America.

(g) **“Partner Account”** means the Partner’s own login account for accessing the Partner Console to administer and manage partner activities in connection with the Partner Program.

(h) **“Partner Benefits”** means the benefits made available to Partner specified in the Partner Program Policies or otherwise provided to Partner, based on the relevant Program Type and Partner Tier.

(i) **“Partner Console”** means the area designated as Console in the Tencent Cloud portal at <http://www.tencentcloud.com>. The Partner Console will provide Partner with Console Documentation, updates, and online tools to administer and manage Partner’s activities relating to the Partner Program.

(j) **“Partner Program”** means the partner program described in these Terms and any applicable Additional Terms, including the Partner Benefits and rights and obligations of Partner that are conferred based on the relevant Partner Type and Partner Tier Program.

(k) **“Partner Program Policies”** means the documentation and terms describing in greater details the Partner Program, Partner Benefits, Partner Tier Program, Partner Tier, Partner Type and other policies relating to and governing Partner’s participation in the Partner Program, which are set out under these Terms, provided to Partner separately and/or made available to Partner through the Partner Console.

(l) **“Partner Tier Program”** means the various partner tier qualifying requirements applicable to Partner based on certain performance results including minimum Tencent Cloud yearly revenue achieved by Partner. Depending on the Partner Tier achieved, Partner will be entitled to different Partner Benefits based on the Partner Tier achieved.

(m) **“Partner Tier”** means the Partner’s level in the Partner Tier Program relevant to the Partner Type applicable to the Partner.

(n) **“Partner Type”** means (a) reseller partner; (b) sales agent partner; (c) referral partner; or (d) any other partner type designated and added by Tencent.

(o) **“Personal Data”** and **“Processed”** shall have the meaning as set out in the Applicable Data Protection Laws, and where such term is not defined in Applicable Data Protection Laws such term shall be defined by reference to the materially analogous term in the Applicable Data Protection Laws, and in respect of Data Subjects located in the state of California, “Data Subject” shall have the meaning given to the term “Consumer” in the CCPA and “Personal Data” shall have the meaning given to the term “Personal Information” in the CCPA.

(p) **“Tencent Cloud Partner Data Processing Agreement”** means any additional data processing agreement between Tencent and Partner if required by Tencent for the relevant Partner Program.

(q) **“Tencent Services”** means software, content, digital materials and other items and services as made available by Tencent to Partner under the terms of this Agreement, including, without limitation, those software, content, digital

materials, items or services made available to Partner to conduct Partner Type related activities through the Tencent Cloud international portal at intl.cloud.tencent.com.

## 2.REQUIREMENTS FOR PARTICIPATION IN TENCENT CLOUD PARTNER PROGRAM

(a)**Enrollment.** Partner shall enroll in a Program Type in order to participate in the Partner Program. Certain participation requirements will apply to Partner and they will be designated by Tencent through the Partner Program Policies which Partner must meet before Partner will be accepted to participate in the Partner Program, and is subject to Tencent at its sole discretion. Partner must disclose and provide all relevant information to Tencent in order to process the Partner enrollment to participate in the Partner Program, and Partner warrants that it has the full legal authority and power to provide such information to Tencent to process Partner's enrollment to the Partner Program under these Terms.

(b)**Program Benefits.** The Partner Program Policies will specify certain benefits entitlements available to a Partner, based on the applicable Program Type, Program Tier in the Program Tier Program.

(c)**Program Type and Fees.** Depending on the Program Type, Partner shall enter into the relevant agreements applicable to the Program Type. All applicable fees payable by Partner under each Partner Type are described in the relevant Additional Terms relevant to the Partner Type.

(d)**Account Managers.** Each party will designate and notify the other party of such designation in writing a single point of contact within its organization to manage the relationship between the parties as established by these Terms ("**Account Manager**"). The Account Managers will meet as necessary to discuss the business relationship and manage the activities contemplated by these Terms. Disputes that cannot be resolved by the Account Managers will be escalated to more senior executives for resolution.

## 3.PARTNER CONSOLE ACCESS AND USE

(a)**Partner Console.** Depending on the Partner Type, Tencent will grant a limited, revocable, non-exclusive, license to Partner to access and use Partner Console to administer various Partner Type related activities and other related functions relevant to the Partner Type. However, Tencent may suspend or terminate Partner's access to the Partner Console if Partner is in breach of these Terms or to comply with any applicable law or court orders.

(b)**Partner Console Admin.** Partner shall designated trusted individual within the Partner's organization to have primary access to use the Partner Console ("**Partner Console Admin**"). Partner is at all times responsible for all actions carried out though the Partner Console by Partner Console Admin or anyone to whom Partner Console Admin provided access to Partner Console, and/or any unauthorized use of Partner Console due to an employee and/or agent of Partner. Partner is solely responsible to ensure that only the Partner Console Admin should have secured access to the Partner Console and Partner shall not share any login passwords to any other person or entity or permit any other person or entity to access or use the Partner Console.

(c)**Marketing.** From time to time, Partner may receive marketing communications relating to Tencent Services through the Partner Console. Partner acknowledges and agrees that it has obtained all necessary rights and consents from Partner's customers to send and receive the Tencent Services marketing information that may be made available through the Partner Console.

(d)**Data Collection.** The Partner Console may collect various data from Partner's use of the Partner Console in order to improve the Partner Console and marketability of Tencent Services. The collection and use of such information relating to Partner's use of the Partner Console is subject to the Tencent Cloud Privacy Policy.

#### 4.PARTNER OBLIGATIONS AND RESTRICTIONS

(a)**Business Conduct.** Partner will use its best efforts to market and promote Tencent Services in the Territory and to conduct its business in such manner as will reflect favorably on Tencent and the Tencent Services, and Partner will not engage in any deceptive, misleading, illegal or unethical business practice.

(b)**Partner Professionalism.** Partner shall ensure that its employees who are engaged in Partner Type activities under these Terms will act in a professional manner and shall be generally knowledgeable about Tencent Services before engaging any potential customers.

(c)**Partner Marketing.** Partner will use commercially reasonable efforts to either independently or work together with Tencent to identify, pursue and/or carry out promotional opportunities designed to enhance the Partner activities contemplated by these Terms. These efforts may include: (i) the promotion of Partner Type activities in relation to Tencent Services; (ii) website promotion; (iii) trade show collaboration; (iv) EDMs and newsletter highlights; (v) participation in public relations activities; (vi) use of each other's trademarks on specific targeted creative advertising executions; and (vii) press releases. Each party shall be responsible for complying with all applicable personal data and privacy laws when carrying out marketing activities.

(d)**Non-exclusivity.** Partner acknowledges and agrees that this is a non-exclusive arrangement and neither party is prevented from pursuing other opportunities, including competitive opportunities during or after the Term, provided always that in do so the party shall not breach any of these Terms in undertaking such opportunities.

(e)**No false marketing or misrepresentations.** Partner shall not make any false marketing statements relating to or misrepresents the capabilities or functionalities of any Tencent Services, and all marketing and representations relating to Tencent Services by Partner must adhere in substance to the marketing information that are supplied by Tencent.

(f)**Compliance with applicable laws.** Partner shall comply with all applicable laws and regulations when performing Partner activities contemplated under these Terms.

(g)**Support.** Partner and Tencent will provide support services to customers in accordance with the relevant agreement applicable to the Partner Type.

(h)**Market Intelligence.** Partner will use commercially reasonable efforts to keep Tencent informed of market developments concerning the Tencent Services in the territories where Partner operate.

(i)**Training**

- Partner will ensure that all of their respective sales representatives, technical support personnel, and agents will receive appropriate and adequate training relating to the Tencent Services. Partner will inform and educate its sales representatives, technical support personnel, and agents about the nature of the business relationship between the parties and Tencent Services.

- Tencent, at its discretion, may provide Partner's sales and technical support personnel training, which may include: (1) demonstrations of the Tencent Services; (2) summaries of market and competitive positioning; (3) materials regarding key features, benefits, and value of Tencent Services to customers; (4) marketing materials; (5) common technical and support issues; and (6) any other information that may be beneficial for the provision of sales and technical support. Such training may be provided at additional fees and expenses, in which case such additional fees and expenses will be subject to separate agreement between Tencent and Partner.

(j)**Consents and Permits.** Partner is solely responsible (at its sole expense) for obtaining all licenses, consents, and approvals that are necessary to its performance of these Terms (including those that are required for the resale of Tencent Services in the Territory).

(k)**Demonstration Versions or Accounts.** Tencent, at its sole discretion, may provide Partner with demonstration versions or accounts of the Tencent Services for Partner to use in its marketing and promotion of the Tencent Services. Partner's use of such demonstration versions may be subject to additional terms and restrictions.

## 5.INTELLECTUAL PROPERTY

(a)**Intellectual Property.** All Intellectual Property Rights in Partner Console, Tencent Services, related documentation and any derivative work thereof are and will remain exclusively with Tencent. Except as expressly licensed to Partner to access and use Partner Console under these Terms, nothing in these Terms grants Partner any license, rights or interest in or to any of Tencent's Intellectual Property Rights.

(b)**Proprietary Rights Notices.** Partner may not remove or alter any trademark, trade name, copyright, patent, patent pending, or other proprietary notices, legends, symbols, or labels appearing on or with the Tencent Services, Partner Console or related documentation provided by Tencent.

(c)**Tencent Trademarks.** Tencent hereby grants to Partner a non-exclusive, non-transferable, and non-sublicensable license in the Territory to use Tencent's trademarks, trade names, service marks, and logos of Tencent ("**Tencent Trademarks**"), during the Term and solely in connection with Partner's marketing and promotional activities of the Tencent Services in accordance with the terms of these Terms. Partner will ensure that its use of any Tencent Trademark complies with Tencent's then-current trademark use guidelines as may be changed by Tencent from time to time. Any use of Tencent's Trademarks by Partner will first be submitted to Tencent for approval. Partner will not alter or remove any Tencent Trademarks provided with or embedded in the Tencent Services or Partner Console. Other than otherwise expressly provided herein, nothing contained in these Terms will grant or will be deemed to grant to Partner any right, title, or interest in or to Tencent's Trademarks. All uses of Tencent's Trademarks and related goodwill will inure solely to Tencent. Partner may not register or attempt to register, directly or indirectly, within the Territory or elsewhere, any trademarks, service marks, or URLs that utilize, or that are confusingly similar to, a Tencent Trademark.

(d)**Partner Trademarks.** Partner hereby grants to Tencent a non-exclusive, non-transferable, and non-sublicensable license in the Territory to use Tencent's trademarks, trade names, service marks, and logos of Partner ("**Partner Trademarks**") that are provided by Partner and/or uploaded by Partner to the Partner Console, during the Term and solely in connection with Tencent's marketing and promotion of the Tencent Services involving Partner's participation



as a reseller of Tencent Services in accordance with the terms of these Terms. Tencent will ensure that its use of any Partner Trademark complies with Partner's then-current trademark use guidelines as may be changed by Partner from time to time. Other than otherwise expressly provided herein, nothing contained in these Terms will grant or will be deemed to grant to Tencent any right, title, or interest in or to Partner's Trademarks. All uses of Partner's Trademarks and related goodwill will inure solely to Partner. Tencent may not register or attempt to register, directly or indirectly, within the Territory or elsewhere, any trademarks, service marks, or URLs that utilize, or that are confusingly similar to, a Partner Trademark. For the avoidance of doubt, Tencent may identify Partner as a partner/reseller/referral (as applicable) of the Tencent Services on its website and marketing and promotional materials.

## 6.TERM AND TERMINATION

(a)**Term.** These Terms commence upon the Effective Date and shall remain in effect until termination in accordance with this Section 6.

(b)**Termination for Convenience.** Either party may terminate these Terms without cause upon 60 days prior written notice to the other party. If Tencent considers, at its sole discretion, the participation of the Partner in the Partner Program will adversely damage the reputation of Tencent and/or Tencent Services, Tencent may terminate these Terms upon 30 days prior written notice to Partner. However, if Tencent reasonably believes Partner is in violation of section 12(f) Export Restrictions and/or 12(g) Sanctions Compliance, Tencent may terminate these Terms or the Partner's participation in any part of the Partner Program immediately upon giving notice to Partner.

(c)**Suspension by Tencent.** Tencent may immediately suspend Partner's access to Partner Console if Partner breaches any of these Terms.

(d)**Termination for Cause.** Either party may terminate these Terms if the other party commits a material breach of these Terms and fails to cure that material breach within 30 days following its receipt of notice regarding that material breach from the non-breaching party.

(e)**Effects of Termination.** Upon termination of these Terms, unless provided otherwise under an agreement in Additional Terms:

- (i) All licenses granted to Partner under these Terms will terminate automatically and Partner's access to Partner Console will terminate with immediate effect;
- (ii) Partner will promptly return, or at Tencent's direction, destroy all Tencent-provided materials relating to the Partner Program except where such materials are required to enable Partner to continue support for its Customers, as applicable, under the relevant agreement in the Additional Terms;
- (iii) Partner will forthwith cease using Tencent Trademarks and discontinue to represent that it is an authorized Partner of Tencent Cloud Services; and
- (iv) Partner will pay Tencent all amounts, if any, which remain outstanding and unpaid under an agreement in the Additional Terms prior to the effect date of termination.

(f)**Survival.** Sections 1, 5(a), 5(b), 6(e), 6(f), 7, 8, 9, 10, 11 and 12. The termination or expiration of these Terms will not relieve Partner of: (i) the obligation to pay any fees that are due to Tencent under these Terms; or (ii) Partner's obligation to indemnify Tencent as specified in these Terms.

## 7.WARRANTIES; DISCLAIMER

(a)**Warranties.** Each party represents and warrants to the other party that: (i) these Terms have been duly and validly executed and delivered and constitutes a valid and binding agreement enforceable against such party in accordance with its terms; (ii) no authorization or approval from any third party is required in connection with such party's execution, delivery, or performance of these Terms; (iii) the performance of the parties' obligations under these Terms will not violate the applicable laws of any jurisdiction; and (iv) there are no pre-existing obligations or commitments under any other agreements that would conflict with or be inconsistent with or that would hinder such party's performance of its obligations under these Terms.

(b)**Disclaimer.** EXCEPT FOR THE WARRANTIES SET FORTH IN SECTION 7(a), TENCENT DISCLAIMS ALL WARRANTIES WITH REGARD TO THE TENCENT SERVICES. ALL TENCENT SERVICES AND PARTNER CONSOLE ARE PROVIDED "AS IS". TENCENT MAKES NO ADDITIONAL REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS, IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), OR STATUTORY, AS TO ANY MATTER WHATSOEVER. TENCENT EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, ACCURACY, INFRINGEMENT AND TITLE. TENCENT DOES NOT WARRANT AGAINST INTERFERENCE WITH THE ENJOYMENT OF THE TENCENT SERVICES / PARTNER CONSOLE OR AGAINST INFRINGEMENT. TENCENT DOES NOT WARRANT THAT THE TENCENT SERVICES / PARTNER CONSOLE ARE ERROR-FREE OR THAT OPERATION OF THE TENCENT SERVICES / PARTNER CONSOLE WILL BE SECURE OR UNINTERRUPTED. PARTNER WILL NOT HAVE THE RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTIES ON BEHALF OF TENCENT TO ANY OTHER THIRD PARTY. USE OF ANY INFORMATION OR DATA OBTAINED THROUGH THE TENCENT SERVICES / PARTNER CONSOLE IS AT PARTNER'S AND CUSTOMER'S SOLE RISK. THE PARTIES AGREE THAT TENCENT WILL BEAR NO RESPONSIBILITY FOR THE ACCURACY OR QUALITY OF INFORMATION OR DATA OBTAINED THROUGH THE TENCENT SERVICES AND/OR PARTNER CONSOLE.

## 8.INDEMNIFICATION

(a)**Indemnification by Partner.** Partner hereby indemnifies, defends, and holds harmless of Tencent and its affiliates and their respective employees, directors, agents, and representatives ("**Tencent Indemnified Parties**") from and against any and all third party claims, demands, suits, actions, judgments, damages, costs, losses, expenses (including attorneys' fees) and other liabilities (each, a "Claim") arising out of or relating to (i) any actual or alleged breach of any of the representations, warranties, or covenants made by Partner under these Terms; (ii) any actual or alleged breach of any Terms or unauthorized use of the Partner Console; (iii) any claims of unfair or deceptive business practices by Partner; (iv) any infringement of Tencent's Intellectual Property Rights; (v) any violation of or non-compliance with any applicable law; or (vi) Partner's negligence or willful misconduct.

(b)**Indemnification Procedures.** Tencent will promptly give Partner written notice of the Claim and will grant to Partner control over the defense and settlement of the Claim. Upon reasonable request by Partner, Tencent will provide assistance in connection with the defense and settlement of the Claim. However, Tencent's failure to comply with one or more of the obligations in the preceding sentence will not relieve Partner of its obligations under this



Section 8 except and solely to the extent that such failure materially prejudices Partner's defense of the Claim. Partner may not settle any Claim without Tencent's prior written consent.

## 9.DATA PRIVACY

(a) Partner acknowledges and agrees that to the extent any Personal Data is Processed in connection with its participation in the Partner Program, such Processing is undertaken in accordance with, and Partner shall comply with the Tencent Cloud Partner Data Processing Agreement.

(b) To the extent Partner provides any Personal Data in connection with the Partner Program, Partner represents, warrants and undertakes that: (i) it has a lawful basis for Processing such Personal Data; (ii) it has complied with and shall comply with Applicable Data Protection Laws in connection with the collection, Processing, and transfer of such Personal Data; and (iii) it has obtained all necessary consents and provided all disclosures required to ensure the lawful transfer and Processing of such Personal Data by Tencent or relevant third parties.

## 10.CONFIDENTIAL INFORMATION

(a)**Definition.** "Confidential Information" means any proprietary information of a party to these Terms disclosed by one party to the other that is in written, graphic, machine readable, or other tangible form and is marked "Confidential" or "Proprietary" or in some other manner to indicate its confidential nature. The Tencent Cloud Partner Program offers, benefits, policies, rules, operational, management, financial, non-public roadmaps and related information will be the Confidential Information of Tencent. Confidential Information also includes oral disclosures provided that such information is designated as confidential at the time of disclosure and reduced to a written summary by the disclosing party within 30 days after its oral disclosure, which is marked in a manner to indicate its confidential nature and delivered to the receiving party.

(b)**Exceptions.** Confidential Information will not include any information that: (i) was publicly known and made generally available prior to the time of disclosure by the disclosing party; (ii) becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party; (iii) is already in the possession of the receiving party at the time of disclosure; or (iv) is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality.

(c)**Non-Use and Non-Disclosure.** During the Term and thereafter, each party will: (i) treat as confidential all Confidential Information of the other party; (ii) not disclose such Confidential Information to any third party, except on a "need to know" basis to third parties that have signed a non-disclosure agreement containing provisions substantially as protective as the terms of this Section provided that the disclosing party has obtained the written consent to such disclosure from the other party; and (iii) will not use such Confidential Information except in connection with performing its obligations or exercising its rights under these Terms. Each party is permitted to disclose the other party's Confidential Information if required by law so long as the other party is given prompt written notice of such requirement prior to disclosure and assistance in obtaining an order protecting such information from public disclosure.

(d)**Confidentiality.** Neither party may disclose the existence or terms of these Terms to any third party without the consent of the other party, except that each party may disclose the terms of these Terms: (i) in connection with the requirements of a public offering or securities filing; (ii) in confidence, to accountants, banks, and financing sources

and their advisors; (iii) in confidence, in connection with the enforcement of these Terms or rights under these Terms; or (iv) in confidence, in connection with a merger or acquisition or proposed merger or acquisition, or the like.

(e)**Return of Materials.** Upon the termination or expiration of these Terms, or upon earlier request, each party will deliver to the other all Confidential Information that it may have in its possession or control. Notwithstanding the foregoing, neither party will be required to return materials that it must retain in order to receive the benefits of these Terms or properly perform in accordance with these Terms.

## 11.LIMITATION OF LIABILITY

(a)**Disclaimer of Damages.** EXCEPT WITH REGARD TO PARTNER'S INFRINGEMENT OF TENCENT'S INTELLECTUAL PROPERTY RIGHTS OR PARTNER'S BREACH OF APPLICABLE DATA PROTECTION LAWS, EITHER PARTY WILL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO THE OTHER PARTY FOR CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE TRANSACTION CONTEMPLATED UNDER THESE TERMS, INCLUDING LOST PROFITS AND LOSS OF BUSINESS, EVEN IF THE OTHER PARTY IS APPRISED OF THE LIKELIHOOD OF SUCH DAMAGES OCCURRING.

(b)**Cap on Liability.** UNDER NO CIRCUMSTANCES WILL TENCENT'S TOTAL LIABILITY OF ALL KINDS ARISING OUT OF OR RELATED TO THESE TERMS (INCLUDING WARRANTY CLAIMS), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT, OR OTHERWISE, EXCEED FIVE HUNDRED US DOLLARS (USD500).

(c)**Risk Mitigation.** EACH PARTY SHALL TAKE ALL REASONABLE STEPS TO MITIGATE ANY LOSS AND DAMAGE IT INCURS IN RELATION TO ANY CLAIM OR ACTION, BREACH OF STATUTORY DUTY, UNDER AN INDEMNITY OR OTHERWISE, WHICH IT BRINGS AGAINST THE OTHER PARTY.

## 12.GENERAL

(a)**Independent Contractors.** The relationship of the parties established by these Terms is that of independent contractors, and nothing contained in these Terms should be construed to give either party the power to (i) act as an agent or (ii) direct or control the day-to-day activities of the other. Financial and other obligations associated with each party's business are the sole responsibility of that party.

(b)**Non-Assignability and Binding Effect.** Neither party will assign its rights and obligations under these Terms without the written consent of the other party, except: (i) that either party may assign these Terms to a successor to its business (including a successor by way of merger, acquisition, sale of all or substantially all of its assets, or operation of law); and (ii) Tencent may freely assign these Terms to its affiliates. Subject to the foregoing, these Terms will be binding upon and inure to the benefit of the parties and their successors and assigns.

(c)**Non-solicitation.** During the Term and for a period of one year thereafter, Partner may not, directly or indirectly, employ or solicit the employment or services of a Tencent employee or independent contractor without the prior written consent of Tencent.

(d)**Notices.** Except for provisions that expressly allow for email notice, any notice required or permitted to be given under these Terms will be effective if it is in writing and sent by certified or registered mail, or insured courier, return

receipt requested, to the appropriate party at the address as the party may specify. For any notice sent to Tencent, copies of the notice will also need to be sent to Tengyun Building, Tower A, No. 397 Tianlin Road, Xuhui District, Shanghai, 200233, China (Attn: International Business Legal Center) and by email to IBLCLegalnotice@tencent.com.

(e)**Force Majeure.** Nonperformance of either party will be excused to the extent that performance is rendered impossible by strike, fire, flood, governmental acts, orders or restrictions, or any other reason where failure to perform is beyond the control and not caused by the negligence of the non-performing party.

(f)**Export Restrictions.** Partner acknowledges that certain equipment, encryption products, software, and Confidential Information provided under these Terms may be subject to export laws and regulations of the United States, the European Union, the People's Republic of China and other countries (cumulatively, "Export Laws"). Partner agrees that it will not use, distribute, export, re-export, transfer, or transmit such equipment, encryption products, software, or Confidential Information (even if incorporated into other items) in violation of applicable Export Laws.

(g)**Sanctions Compliance.** None of the Partner, any of its subsidiaries or, to the knowledge of the Partner, any director, officer, or employee of the Partner or any of its subsidiaries is a person (i.e., an individual or entity) who is located or resident in or organized under the laws of a country or region that is, or whose government currently is, the target of comprehensive sanctions imposed by any sanctions authority of the United States, Canada, the United Kingdom, or the European Union, which are currently Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine (each a "Sanctioned Jurisdiction"). Without limiting the foregoing, none of the Partner, any of its subsidiaries or, to the knowledge of the Partner, any director, officer, or employee of the Partner or any of its subsidiaries is (i) the target of sanctions imposed by any sanctions authority of the United States, Canada, the United Kingdom, or the European Union, including, without limitation, the sanctions maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), including, without limitation, OFAC's Specially Designated Nationals and Blocked Persons List (any such person targeted by these sanctions a "Sanctioned Person") or (ii) directly or indirectly owned or controlled by (x) any Sanctioned Person, (y) any person located or resident in or organized under the laws of a Sanctioned Jurisdiction, or (z) the government of Venezuela, as that term is defined in Executive Order 13884 of August 5, 2019.

(h)**Governing Law and Resolution of Disputes.** These Terms shall be governed by and interpreted in accordance with the laws as follows:

- If Partner is located in Europe Economic Area, UK and Switzerland, these Terms are governed by and interpreted in accordance with English laws. Any claims for equitable relief may be brought in any court of competent jurisdiction even if the parties have chosen an exclusive venue below. Any dispute or difference between the parties arising out of or in connection with this Agreement, its interpretation or subject-matter, shall be referred to and finally resolved by arbitration under the London Court of International Arbitration (LCIA) Rules, which rules are deemed to be incorporated by reference into this clause. The seat of arbitration shall be London, the United Kingdom. The language to be used in the arbitral proceedings shall be English;

- If Partner is located in North America, these Terms are governed by and interpreted in accordance with the laws of the state of California, USA. Any claims for equitable relief may be brought in any court of competent jurisdiction and for all claims arising out of or relating to this Agreement or the Services. Any dispute or difference between the parties arising out of or in connection with this Agreement will be settled by binding arbitration in Santa Clara County, California under the auspices of the American Arbitration Association (the “Association”) and under the rules of the Association in force at the commencement of such arbitration proceedings. Judgment upon the award rendered by the arbitrators may be entered in any court of competent jurisdiction; and
- If Partner is located in the rest of the world except People’s Republic of China, these Terms are governed by and interpreted in accordance with the laws of Singapore. Except for the right of either party to apply to any court of competent jurisdiction for a temporary restraining order, a preliminary injunction, or other equitable relief to preserve the status quo or prevent irreparable harm, any dispute as to the interpretation, enforcement, breach, or termination of these Terms will be settled by binding arbitration under the Rules of Singapore International Arbitration Center (“SIAC Rules”) by three arbitrators appointed in accordance with the SIAC Rules. The place of arbitration shall be Singapore. The language of proceedings shall be English. Judgment upon the award rendered by the arbitrators may be entered in any court of competent jurisdiction. The prevailing party will be entitled to receive from the other party its reasonable attorneys’ fees and costs incurred in connection with any arbitration or litigation instituted in connection with these Terms.

(i)**Remedies Cumulative.** The remedies provided to the parties under these Terms are cumulative and will not exclude any other remedies to which a party may be lawfully entitled.

(j)**Waiver and Severability.** The waiver by either party of any breach of these Terms does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation under these Terms will not be a waiver of such party’s right to demand strict compliance in the future, nor will the same be construed as a novation of these Terms. If any part of these Terms is unenforceable, the remaining portions of these Terms will remain in full force and effect.

(k)**Entire Agreement.** These Terms and any applicable Additional Terms, policies and rules constitute the entire agreement between you and Tencent with respect to your participation in the Tencent Cloud Partner Program, and supersedes all previous oral and written agreements regarding these matters.

(l)**Modification of these Terms.** Tencent may amend these Terms, including the Additional Terms, from time to time by posting updated versions to the Partner Console. Updated versions will be effective no earlier than the date of posting. Tencent will use reasonable efforts to notify you of the changes, but you are responsible for periodically checking these Terms and the Additional Terms for any modifications. Your continued participation in the Partner Program constitutes your acceptance of any amended Terms. Amended Terms are not applicable retroactively.

(m)**No Third Party Rights.** No one other than a party to these Terms, their successors and permitted assignees, will have any right to enforce any of its terms.

# 腾讯云代金券条款

最近更新时间：2024-03-04 09:55:48

Last updated: 2024-02-06

## PLEASE READ THESE TERMS CAREFULLY

BY USING TENCENT CLOUD VOUCHER (“**TENCENT CLOUD VOUCHER**”) PROVIDED BY THE TENCENT CONTRACTING ENTITY THAT ENTERED INTO A TENCENT CLOUD RESELLER AGREEMENT (“**TENCENT**”) WITH PARTNER (“YOU”), YOU AGREE TO THESE TENCENT CLOUD VOUCHER TERMS AND CONDITIONS (THESE “**TERMS**”). BY YOUR ACCEPTANCE OF THESE TERMS, A LEGALLY BINDING CONTRACT AND AGREEMENT IS ENTERED INTO BETWEEN YOU AND TENCENT GOVERNING YOUR USE OF TENCENT CLOUD VOUCHER. TENCENT MAY UPDATE OR REVISE THESE TERMS FROM TIME TO TIME. YOU AGREE THAT YOU WILL REVIEW THESE TERMS PERIODICALLY AND YOUR USE OF TENCENT CLOUD VOUCHER WILL CONSTITUTE YOUR ACCEPTANCE OF THESE TERMS AS UPDATED OR REVISED. IF YOU USE TENCENT CLOUD VOUCHER ON BEHALF OF A ENTITY, THEN (1) “YOU” SHALL INCLUDE YOU AND THE ENTITY, (2) YOU REPRESENT AND WARRANT THAT YOU ARE AUTHORIZED TO BIND THE ENTITY TO THESE TERMS, AND THAT YOU AGREE TO THESE TERMS ON THE ENTITY’S BEHALF, AND (3) YOUR ENTITY IS RESPONSIBLE FOR YOUR USE OF TENCENT CLOUD VOUCHER. IF YOU DO NOT AGREE TO THESE TERMS OR THE UPDATED OR REVISED TERMS, YOU ARE NOT PERMITTED TO, AND SHOULD NOT, USE TENCENT CLOUD VOUCHER.

Please print or save a copy of these Terms for future reference.

## 1. DEFINITIONS

**1.1** Unless otherwise defined in these Terms, all capitalized terms shall have the same meaning as defined in the Tencent Cloud Reseller Agreement.

## 2. TENCENT CONTRACTING ENTITY

**2.1** Depending on the territory where Partner is located, Tencent means the following:

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands, if Partner is located in European Economic Area, UK and Switzerland;

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America;

**Tencent Korea Yuhan Hoesa**, a South Korean registered company located at 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, Korea; or

**Aceville Tencent Cloud International Pte Ltd**, a Singapore registered company located at 10 Anson Road, #21-07, International Plaza,, Singapore 079903., if Partner is located in the rest of the world except People's Republic of China.

### 3. PURPOSE OF TENCENT CLOUD VOUCHER

**3.1** In order to help our Tencent Cloud Partners promote Tencent Cloud Products, Tencent may periodically issue online vouchers via the Console to Tencent Cloud Partners for distribution to Partner's customers' accounts in the Console. Tencent Cloud Voucher is non-redeemable for cash and cannot be exchanged for cash in part or full and is only entitled for purchase of Tencent Services by Partner's customers during its validity period.

### 4. ISSUANCE OF TENCENT CLOUD VOUCHER

**4.1** The issuance, distribution and use of the Tencent Cloud Voucher will be provisioned through the Console only.

**4.2** The total quota amount of Tencent Cent Cloud Vouchers issued to Partner and remaining available amount of Tencent Cloud Vouchers available for distribution by Partner will be shown in the Tencent Cloud Voucher information menu in the Console. If a Partner distributes Tencent Cloud Voucher to its customer, the Tencent Cloud Voucher amount distributed will be deducted from the Partner's Tencent Cloud Voucher balance and added to the Partner's customer's Tencent Voucher balance in the Console. All distribution and use of the Tencent Cloud Voucher will be made via the Console only.

**4.3** Partner may apply to Tencent for issuance of Tencent Cloud Voucher, all application requests will be reviewed by Tencent and are subject to approval by Tencent in its sole discretion. Tencent may impose applicable conditions on the issuance and/or distribution of Tencent Cloud Voucher, which shall be communicated to you separately via your BD contact.

### 5. DISTRIBUTION AND USE OF TENCENT CLOUD VOUCHER

**5.1** Partner may check the Tencent Cloud Voucher balance, distribute Tencent Cloud Voucher to its customers and check on usage of Tencent Cloud voucher by its customers via the Voucher system features and tools in the Console. The distribution of Tencent Cloud Voucher to Partner's customer may be subject to prior approval by Tencent. Where

such Tencent approval is required, it will be processed by the sales and operation team and the approval status will be shown in the Console.

**5.2** Tencent Cloud Voucher can only be used to apply to the purchase of Tencent Services by Partner's customer. Partner cannot use Tencent Cloud Voucher to purchase Tencent Services.

**5.3** The Tencent Cloud Voucher amount available for distribution by Partner to its customer will be shown in the Partner's balance for Tencent Cloud Voucher in the Console.

**5.4** The Tencent Cloud Voucher amount available for purchase of Tencent Services will be shown in the Partner's customer balance for Tencent Cloud Voucher.

**5.5** If the value of the purchased Tencent Services exceeds the amount stated in the Tencent Cloud Voucher, the remaining Fees (after deduction of the Tencent Cloud Voucher amount) shall be paid by the Partner's customer.

## 6. PARTNER OBLIGATIONS

**6.1** By using Tencent Cloud Voucher, you agree to the following:

- (a) you have the legal capacity and authority and you are not prohibited by law from accessing or using Tencent Cloud Voucher;
- (b) you shall not resell or make available for sale or auction any Tencent Cloud Voucher issued to you;
- (c) you shall not use Tencent Cloud Voucher for any illegal purposes;
- (d) you shall not take any acts which are out of the ordinary course (including, without limitation, damaging, or attacking the servers) that may affect the use of Tencent Cloud Voucher;
- (e) you shall not attack or attempt to attack the servers, routers, switches and other devices provisioning Tencent Cloud Voucher in any manner;
- (f) you shall not use any technical defects or bugs in the systems provisioning Tencent Cloud Voucher to benefit yourself and/or others in any manner or engage in any other misconduct;
- (g) you shall not take any acts that may interfere with the use of Tencent Cloud Voucher in an ordinary manner; and
- (h) you shall not upload or introduce any viruses, Trojan horses, malicious code, worms, logic bombs or other material which is malicious or technologically harmful into our systems facilitating Tencent Cloud Voucher.

## 7. TERM AND TERMINATION

**7.1** Term. These Terms will become effective upon your agreement to these Terms and will continue in effect unless earlier terminated in accordance with the provisions of these Terms.

**7.2** Termination by Tencent. Tencent may terminate these Terms and Tencent Cloud Voucher issued to Partner and/or distributed by Partner to its customer at any time in its sole discretion for any or no reason upon five (5) days' written notice provided to you.



**7.3 Expiry of Tencent Cloud Voucher.** Tencent may set an expiry date for use of Tencent Cloud Voucher upon issuance. Unless renewed in accordance with these Terms, any unused Tencent Cloud Voucher after the expiry will be void and deducted from the Partner's and the Partner's customer's Tencent Cloud Voucher balance (as applicable).

**7.4 Renewal of Tencent Cloud Voucher.** Before expiry of Tencent Cloud Voucher, you may apply to renew Tencent Cloud Voucher in the Partner Console. All renewal requests are subject to approval by Tencent in its sole discretion. You will be notified if the renewal request is approved. If you do not receive any approval notification within 10 business days, your renewal request is deemed to be denied.

## 8. DISCLAIMER OF WARRANTIES

**8.1** TO THE EXTENT PERMITTED BY APPLICABLE LAWS, TENCENT CLOUD VOUCHER IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS AND NEITHER TENCENT NOR ANY OF TENCENT'S AFFILIATE COMPANIES, NOR ITS LICENSORS, MAKE ANY REPRESENTATION OR WARRANTY IN RELATION TO TENCENT CLOUD VOUCHER PROVISIONED BY TENCENT, INCLUDING ANY REPRESENTATION OR WARRANTY THAT DISTRIBUTION AND/OR USE OF TENCENT CLOUD VOUCHER WILL BE UNINTERRUPTED, SECURE, ERROR-FREE OR FREE FROM VIRUSES OR FROM LATENT/HIDDEN DEFECTS. TENCENT, ON BEHALF OF ITS AFFILIATE COMPANIES AND LICENSORS, HEREBY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY AND NON-INFRINGEMENT.

## 9. LIMITATION OF LIABILITY

**9.1 Cap on Liability.** TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAW, THE TOTAL AGGREGATE LIABILITY OF TENCENT AND TENCENT'S AFFILIATES FOR ALL CLAIMS IN CONNECTION WITH THESE TERMS OR TENCENT CLOUD VOUCHER, ARISING OUT OF ANY CIRCUMSTANCES WHETHER FROM BREACH OF CONTRACT, NEGLIGENCE, HIDDEN/LATENT DEFECTS OR ANY OTHER CAUSE, WILL BE LIMITED TO USD10.

**9.2 Disclaimer of Damages.** NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THESE TERMS, EXCEPT FOR LIABILITIES THAT CANNOT BE WAIVED, LIMITED OR EXCLUDED DUE TO APPLICABLE LAW, IN NO EVENT WILL TENCENT (OR ANY OF TENCENT'S AFFILIATES) BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR LOSSES, INCLUDING, WITHOUT LIMITATION ANY LOSS OF DATA, LOSS OF USE, LOSS OR INTERRUPTION OF BUSINESS, REVENUES, PROFITS, ANTICIPATED SAVINGS, GOODWILL, CONTENT OR DATA, ANY THIRD PARTY'S CLAIMS OR ANY OTHER DAMAGE OF ANY KIND ARISING OUT OF THESE TERMS OR BINARY AI, WHETHER ALLEGED AS A BREACH OF CONTRACT OR TORTIOUS CONDUCT, NON-CONTRACTUAL FAULT OR



NEGLIGENCE, HIDDEN OR LATENT DEFECTS, EVEN IF TENCENT HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**9.3** NOTHING IN THESE TERMS SHALL OPERATE OR HAVE EFFECT SO AS TO LIMIT OR EXCLUDE THE LIABILITY OF A PARTY FOR DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE OR FOR FRAUD INCLUDING FRAUDULENT MISREPRESENTATION OR FOR ANY LIABILITY THAT MAY NOT BE LAWFULLY EXCLUDED UNDER APPLICABLE LAW.

## 10. INDEMNIFICATION

You agree to defend, indemnify and hold harmless Tencent, its directors, employees, agents, partners, affiliates and subsidiaries, from and against any claims, damages, costs, liabilities and expenses (including, but not limited to, reasonable attorneys' fees) arising out of or related to your violations of these Terms, including without limitation, any unauthorized and/or misuse of Tencent Cloud Voucher.

## 11. GOVERNING LAWS AND DISPUTE RESOLUTION

**11.1** These Terms shall be governed by and interpreted in accordance with the laws as follows:

If Partner is located in Europe Economic Area, UK and Switzerland, these Terms are governed by and interpreted in accordance with English laws. Any claims for equitable relief may be brought any court of competent jurisdiction even if the parties have chosen an exclusive venue below. The parties submit to the jurisdiction of the English courts in relation to any dispute or difference between the parties arising out of or in connection with these Terms, its interpretation or subject-matter, but Tencent is also entitled to apply to any court worldwide for injunctive or other remedies in order to protect or enforce its intellectual property rights and/or confidential information;

If Partner is located in North America, these Terms are governed by and interpreted in accordance with the laws of the state of California, USA. Any claims for equitable relief may be brought any court of competent jurisdiction and for all claims arising out of or relating to these Terms. The parties submit to the exclusive jurisdiction of the state and federal courts located in Los Angeles County, California in relation to any dispute or difference between the parties arising out of or in connection with these Terms, its interpretation or subject-matter, but Tencent is also entitled to apply to any court worldwide for injunctive or other remedies in order to protect or enforce its intellectual property rights and/or confidential information; and

If Partner is located in the rest of the world except People's Republic of China, these Terms are governed by and interpreted in accordance with the laws of Singapore. Except for the right of either party to apply to any court of competent jurisdiction for a temporary restraining order, a preliminary injunction, or other equitable relief to preserve the status quo or prevent irreparable harm, any dispute as to the interpretation, enforcement, breach, or termination of these Terms will be settled by binding arbitration under the Rules of Singapore International Arbitration Center ("SIAC Rules") by three arbitrators appointed in accordance with the SIAC Rules. The place of arbitration shall be Singapore.

The language of proceedings shall be English. Judgment upon the award rendered by the arbitrators may be entered in any court of competent jurisdiction. The prevailing party will be entitled to receive from the other party its reasonable attorneys' fees and costs incurred in connection with any arbitration or litigation instituted in connection with these Terms.

## 12. CONFIDENTIAL INFORMATION

**12.1** Neither party (the "Recipient") will disclose the other party's (the "Discloser") Confidential Information except to those of the Recipient's affiliates, employees, and contractors who need to know the Confidential Information for the purposes of exercising Recipient's rights and performing Recipient's obligations under these Terms, and who have agreed in writing to confidentiality obligations that are at least as protective as these Terms. The Recipient will, and will take appropriate measures to ensure that its affiliates, employees, and contractors do: (a) take at least reasonable care to protect the confidentiality of the Discloser's Confidential Information; and (b) not use the Discloser's Confidential Information for any purpose other than to exercise the Recipient's rights and perform the Recipient's obligations under these Terms. However, the Recipient may also disclose Confidential Information to the extent required by applicable laws, regulations, or government orders; provided that the Recipient uses commercially reasonable efforts, if legally permitted, to: (i) promptly notify the Discloser of those disclosure requirements before disclosing the Discloser's Confidential Information; and (ii) provide to Discloser any information reasonably requested to assist Discloser in seeking a protective order or other confidential treatment for that Confidential Information. "Confidential Information" means information that one party (or an affiliate) discloses to the other party under these Terms, and that is marked as confidential or should reasonably be considered confidential based on the nature of the information and the circumstances of its disclosure. Confidential Information does not include information that: (a) is independently developed by the Recipient without use of the Confidential Information of the Discloser; (b) is, at the time of disclosure by the Discloser, already known to the Recipient without confidentiality obligations; (c) is rightfully given to the Recipient by a third party without confidentiality obligations; or (d) becomes publicly known through no fault of the Recipient. This Section will survive for a term of three (3) years following termination or expiration of these Terms for whatever reason.

## 13. WAIVER AND SEVERABILITY

**13.1** The waiver by either party of any breach of these Terms does not waive any other breach. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under these Terms. If any part of these Terms is unenforceable, the remaining portions of these Terms will remain in full force and effect.

## 14. FORCE MAJEURE

**14.1** If the performance of these Terms is delayed or either party breaches these Terms due to an event of force majeure, including but not limited to natural disasters, acts of government, promulgation or change of policies, promulgation or change of laws and regulations, strikes and unrest, neither party will be liable for the breach, provided that the affected party will notify the other party as soon as practicable. If an event of force majeure prevents the performance of these Terms for more than 30 calendar days, either party may terminate these Terms, without assuming any liability, by giving 15 days' advance written notice to the other party.

## 15. ENTIRE AGREEMENT

**15.1** These Terms are the final and complete expression of all agreements between you and Tencent regarding their subject matter and supersede all prior oral and written agreements regarding these matters.

## 16. MODIFICATION OF THESE TERMS

**16.1** Tencent may amend these Terms from time to time by posting updated versions to the Tencent Cloud Partner Console. Updated versions will be effective no earlier than the date of posting. Tencent will use reasonable efforts to notify you of the changes, but you are responsible for periodically checking these Terms for any modifications. Your continued use of the Tencent Cloud Voucher constitutes your acceptance of any amended Terms. Amended Terms are not applicable retroactively.

# Tencent Cloud International Data Processing Agreement (with Resellers)

最近更新时间：2024-03-04 16:49:15

## Tencent Cloud International Data Processing Agreement (with Resellers)

If you have (a) registered as a Partner under the Tencent Cloud Partner Program Terms and Conditions and (b) entered into a reseller arrangement (whether or not involving integration services) with us under a Reseller Agreement, this Data Processing Agreement (“**DPA**”) applies to any processing of Personal Data in connection with such Reseller Agreement. In the event of any conflict between this DPA, the Reseller Agreement, or the Additional Terms, this DPA shall prevail to the extent of the inconsistency. References to “Partner” and “Tencent” in this DPA have the same meaning as set out in the Reseller Agreement.

**Now it is hereby agreed** as follows:

## 1. Definitions

**1.1** Capitalised terms shall have the meaning given to them in the Reseller Agreement, unless otherwise defined below:

“**Personal Data**”, “**Special Categories of Data/Sensitive Data**”, “**Process/Processing**”, “**Controller**”, “**Processor**”, and “**Data Subject**” shall have the same meaning as in the relevant Applicable Data Protection Laws. “**Additional Terms**” means, collectively, the then-current additional terms posted online at <https://www.tencentcloud.com/partner>, including the Privacy Policy and the Data Processing and Security Agreement. The Additional Terms do not include the online Terms of Service.

“**Applicable Data Protection Law**” shall mean:

- a. the General Data Protection Regulation 2016/679 (the “**GDPR**”);
- b. the Privacy and Electronic Communications Directive 2002/58/EC;
- c. the UK Data Protection Act 2018 (“**DPA**”), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (“**UK GDPR**”), and the Privacy and Electronic Communications Regulations 2003;
- d. the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq. as amended by the California Privacy Rights Act of 2020, Cal. Civil Code § 1798.100 et seq. (collectively, “**CCPA**”), the Virginia Consumer Data Protection Act (“**VCDPA**”), the Colorado Privacy Act (“**CPA**”), Connecticut Data Privacy Act (“**CDPA**”), Utah Consumer Privacy Act (“**UCPA**”), Iowa Consumer Data Protection Act (“**ICDPA**”), Indiana Consumer Data Protection Act (“**INCDPA**”), Montana Consumer Data Privacy Act (“**MCDPA**”), Tennessee Information Protection Act (“**TIPA**”), Texas Data Privacy and Security Act (“**TDPSA**”), Oregon Consumer Privacy Act (“**OCPA**”), Florida Digital Bill of Rights (“**FDBR**”) (collectively, “**Applicable US Data Protection Law**”);
- e. any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or

the use of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

“**Data Discloser**” means the Party who transfers Personal Data to the other Party.

“**Data Receiver**” means the Party who receives Personal Data from the Data Discloser for Processing in accordance with the terms of this Agreement.

“**Lawful Export Measure**” means a method allowing for the lawful transfer of Personal Data from a data exporter to a data importer, as may be stipulated by Applicable Data Protection Law or a Regulator from time to time, which may include (depending upon the Applicable Data Protection Laws) model transfer terms prescribed by Applicable Data Protection Laws; or prior registration, licensing or permission from a Regulator.

“**Party**” means a party to this DPA.

“**Partner Console**” means the area designated as console in the Tencent Cloud portal at <http://www.tencentcloud.com>.

“**Personal Data Breach**” means any improper, unauthorised or unlawful access to, use of, or disclosure of, or any other compromise which affects the availability, integrity or confidentiality of Personal Data.

“**Reseller Agreement**” means the reseller agreement in place between Tencent and the Partner. “**Member State**” means the member states of the European Union from time to time.

“**Regulator**” means the data protection supervisory authority which has jurisdiction over a Party's Processing of Personal Data.

“**Relevant Data Export**” means:

- a. a transfer of Personal Data:
  - i. from a Party which is subject to Applicable Data Protection Law in respect of that Personal Data;
  - ii. to another Party that is in a Third Country or a territory which otherwise (but for the operation of this DPA) does not offer an adequate level of protection as required by Applicable Data Protection Law; and
  - iii. which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law;
- and
- b. the onward transfer of Personal Data pursuant to (a) to a Third Country or a territory which otherwise (but for the operation of this DPA) does not offer an adequate level of protection as required by Applicable Data Protection Law and which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law.

“**Security Standards**” shall mean the technical and organisational security measures set out in Schedule C.

“**Standard Contractual Clauses**” means:

- a. in the case of transfers of Personal Data relating to Data Subjects in the European Economic Area (“**EEA**”), the standard contractual clauses for the transfer of Personal Data to data processors established in third countries set out in the Commission Decision of 4 June 2021 (C(2021) 3972), as amended and restated from time to time;
  - b. in relation to transfers of Personal Data from the UK, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner; and
- in each case, as amended, updated or replaced from time to time, as attached to and incorporated into this DPA to cover Personal Data transfers to Controllers or Processors, as applicable, established in Third Countries which do not

ensure an adequate level of data protection.

“**Third Country**” means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time; and (iii) in relation to Personal Data transfers from any other jurisdiction, any country other than those approved as providing adequate protection for Personal Data by the relevant competent authority of such country from time to time.

**1.2** References to a statutory provision include any subordinate legislation made from time to time under that provision.

**1.3** References to this DPA include the Schedules.

**1.4** Headings shall be ignored in construing this DPA.

**1.5** If a word or phrase is defined, its other grammatical forms have a corresponding meaning.

**1.6** The words “include”, “includes” and “including”, and any succeeding words shall be construed without limitation to the generality of any preceding words or concepts.

**1.7** If there is any inconsistency between the Clauses and Schedules to this DPA the Clauses shall take precedence.

## SCOPE OF THIS AGREEMENT

### 2. General

**2.1** This DPA governs the transfer of Personal Data between Tencent and Partner. This DPA is divided into the following sections:

- a. Module A (Transfers between Controllers) sets forth the terms governing any transfer (including a Relevant Data Export) between the Parties, each acting as an independent Data Controller;
- b. Module B (Transfers from a Data Controller to a Data Processor) sets forth the terms governing any transfer (including a Relevant Data Export) from Partner (acting as a Data Controller) to Tencent (acting as a Data Processor); and
- c. Module C (Transfers from a Data Processor to a Data Controller) sets forth the terms governing any transfer (including a Relevant Data Export) from Partner (acting as a Data Processor) to Tencent (acting as a Data Controller).

## MODULE A – TRANSFERS BETWEEN DATA CONTROLLERS

### 3. APPLICATION OF THIS MODULE A

**3.1** The Parties agree that this Module A applies in each case and only where Personal Data is transferred from Data Discloser to Data Receiver, in circumstances where each Party is acting as an independent Data Controller.

**3.2** The details of the transfers covered by this Module A are specified in Schedule B which forms an integral part of this Module A.

**3.3** In the case of a Relevant Data Export to a Third Country, clause 7 shall govern the terms of the transfer and clauses 4, 5 and 6 shall not apply.

### 4. OBLIGATIONS OF BOTH PARTIES

**4.1** Each Party shall:

- a. Process Personal Data fairly and lawfully;
- b. ensure that Personal Data is accurate and up to date, and inform the other without undue delay if it becomes aware that any of the Personal Data is inaccurate or out of date;
- c. provide reasonable assistance as necessary to the other to enable them to comply with subject access requests and to respond to any other queries or complaints from Data Subjects;
- d. carry out any reasonable request from the other to amend, transfer or delete any Personal Data (to the extent applicable); and
- e. notify the other promptly about any enquiries from a Regulator in relation to Personal Data and cooperate promptly and thoroughly with such Regulator, to the extent required under Applicable Data Protection Law.

### 5. OBLIGATIONS OF DATA DISCLOSER

**5.1** The Data Discloser warrants and undertakes that:

- a. Personal Data have been collected, Processed, and transferred in accordance with Applicable Data Protection Laws, as applicable to the Data Discloser;
- b. it has obtained all consents, authorizations, approvals and rights and provided all notices necessary, including as required by Applicable Data Protection Law, to provide the Personal Data to the Data Receiver and permit the Data Receiver to use the Personal Data in accordance with this DPA;
- c. it has used reasonable efforts to determine that the Data Receiver is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Module A;
- d. it has taken all steps required by Applicable Data Protection Law to avoid “selling” Personal Data to Data Receiver under this Module A (as defined in such laws), including transferring Personal Data at the direction of the relevant individual, or otherwise taken all steps required to comply with obligations relating to “selling” under such Applicable Data Protection Law; and



e. the Data Discloser shall provide a copy of this Module A and associated Schedules to the Regulator where required.

## 6. OBLIGATIONS OF DATA RECEIVER

### 6.1 Data Receiver warrants and undertakes that:

- a. it will comply with all relevant obligations of Applicable Data Protection Law, including by providing the same level of privacy protections required of controllers and businesses by Applicable Data Protection Law;
- b. it will have in place appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the data to be protected including those in the Security Standards, and shall ensure that those measures continue to provide an appropriate level of security;
- c. in the event of a Personal Data Breach, it shall take appropriate measures to address the Personal Data Breach, and shall (if the breach is likely to result in a risk to individuals) notify the Data Discloser and cooperate with the Data Discloser in relation to any required notifications to the Regulator and/ or to relevant Data Subjects.
- d. it will have in place procedures so that any third party it authorises to have access to Personal Data, including Data Processors, will respect and maintain the confidentiality and security of Personal Data. Any person acting under the authority of the Data Receiver, including a Data Processor, shall be obligated to Process Personal Data only on instructions from the Data Receiver. This provision does not apply to persons authorised or required by law or regulation to have access to Personal Data;
- e. it shall notify the Data Receiver promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The Data Receiver shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. The Data Receiver will provide relevant information about disclosure requests to the Data Discloser, including in relation to its legality review and any challenges to the request;
- f. it will inform the Data Discloser if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Module A;
- g. it will Process Personal Data for purposes described in Schedule B (*Description of Transfer*), and has the legal authority to give the warranties and fulfil the undertakings set out in this Module A;
- h. it shall put in place appropriate technical or organisational measures in order to retain Personal Data for no longer than necessary for the purposes for which it is processed; and
- i. it will keep appropriate documentation of the Processing it carries out under this Module A, and shall make such documentation available to the relevant Regulator(s).



## 7. EXPORT OF PERSONAL DATA

**7.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 1: Controller to Controller, set out in Schedule D-1, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser, who shall comply with the data exporter's obligations set out in Schedule D-1, and the applicable Data Receiver, who shall comply with the data importer's obligations set out in Schedule D-1, for that particular transfer of Personal Data for that particular transfer of Personal Data. In relation to any onward transfer of such Personal Data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 1: Controller to Controller set out in Schedule D-1; or (ii) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E, in respect of that Personal Data.

**7.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser. In relation to any onward transfer of such Personal Data by the Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the obligations set out in the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses set out in Schedule D-2, in respect of that Personal Data.

**7.3** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure,. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply mutatis mutandis for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another data importer, the receiving data importer shall comply with the same data importer obligations.

## MODULE B – TRANSFERS FROM DATA CONTROLLER TO DATA PROCESSOR

## 8. APPLICATION OF THIS MODULE B

- 8.1** The Parties agree that this Module B applies in each case and only where Personal Data is transferred from Partner (acting as a Data Controller) to Tencent (acting as a Data Processor).
- 8.2** The details of the transfers (as well as the Personal Data) covered by this Module B are specified in Schedule B which form an integral part of this Module B.
- 8.3** In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, as relevant, clause 12 shall govern the terms of the transfer and clauses 9, 10 and 11 shall not apply.
- 8.4** Nothing in this DPA shall relieve Partner or Tencent of liabilities imposed by virtue of their roles in the Processing relationship.

## 9. OBLIGATIONS OF RESELLER

**9.1** Partner agrees and warrants that:

- a. it has used reasonable efforts to determine that Tencent is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Module B;
- b. it has obtained all consents, authorizations, approvals and rights and provided all notices necessary, including as required by Applicable US Data Protection Law, to provide the Personal Data to Tencent and permit Tencent to use the Personal Data in accordance with this DPA;
- c. it has disclosed the Personal Data to Tencent for the limited purposes set forth in Schedule B; and
- d. the Processing, including the transfer itself, of Personal Data has been and will continue to be carried out in accordance with the relevant provisions of Applicable Data Protection Law (and, where applicable, has been notified to the relevant authorities of the country in which Partner is established).

**9.2** Partner warrants that it has no reason to believe that any applicable local laws, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent Tencent from fulfilling its obligations under this Module B.

## 10. OBLIGATIONS OF TENCENT

**10.1** Tencent agrees and warrants that it will:

- a. Process Personal Data only on documented instructions of Partner and this DPA for the limited purposes set forth in Schedule B and in compliance with Applicable US Data Protection Law;
- b. not retain, use or disclose Personal Data (i) outside of the direct business relationship between Partner and Tencent or as otherwise permitted by Applicable Data Protection Law, or (ii) for any purpose other than for the limited purposes set forth in Schedule B;
- c. not combine Personal Data received from or on behalf of Partner with any Personal Data that may be collected from Tencent's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Applicable Data Protection Law;

- d. ensure that persons authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- e. take all technical and organisational security measures required by Applicable Data Protection Law relating to data security, and shall ensure that those measures continue to provide an appropriate level of security;
- f. taking into account the nature of the Processing, assist Partner by implementing appropriate technical and organisational measures, insofar as this is practicable, for the fulfilment of Partner's obligation to respond to requests for exercising the Data Subject's rights laid down in Applicable Data Protection Law;
- g. notify (as applicable) and assist Partner in ensuring compliance with data security, Personal Data Breach, data protection impact assessments, and engaging in other consultations, pursuant to Applicable Data Protection Law, taking into account the nature of Processing and the information available to Tencent;
- h. inform Partner if it becomes aware that any of Personal Data is inaccurate or out of date, and cooperate with Partner to erase or rectify the relevant Personal Data;
- i. notify Partner promptly if Tencent makes a determination that it can no longer meet its obligations under Applicable US Data Protection Law;
- j. permit Partner to take reasonable and appropriate steps to help ensure that Tencent uses Personal Data in a manner consistent with Partner's obligations under Applicable US Data Protection Law and to stop and remediate any unauthorized use of Personal Data;
- k. notify Partner promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. Tencent shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. Tencent will provide relevant information about disclosure requests to Partner, including in relation to its legality review and any challenges to the request;
- l. inform Partner if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Module B; and
- m. keep appropriate documentation of the Processing it carries out under this Module B, and make available to Partner (and any relevant Regulator) information sufficient to demonstrate compliance with Applicable Data Protection Law and allow for and contribute to audits, including inspections, conducted by Partner.

## 11. SUB-CONTRACTING

**11.1** Tencent may authorize any sub-processor to Process the Personal Data on its behalf provided that, where (and to the extent) required by Applicable Data Protection Laws, Tencent enters into a written agreement with the sub-processor containing terms which are substantially the same as those contained in this DPA. Partner hereby grants Tencent general written authorisation to engage sub-processors listed at <https://www.tencentcloud.com/services/thirdParties>. Tencent shall, to the extent required by Applicable Data

Protection Laws, inform Partner of any intended changes concerning the addition or replacement of the sub-processors. In such a case, Partner will have fourteen (14) days from the date of receipt of the notice to approve or reject the change. In the event of no response from Partner, the sub-processor will be deemed accepted. If Partner rejects the replacement sub-processor, Tencent may terminate the DPA with immediate effect on written notice to Partner. Tencent shall remain fully responsible to Partner for the performance of any sub-processor's obligations under its contract with the Partner.

## 12. EXPORT OF PERSONAL DATA

**12.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**12.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**12.3** In relation to any onward transfer of the Personal Data by Tencent to another party, Tencent shall comply with the relevant obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E; or (ii) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2.

**12.4** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations.

## MODULE C – TRANSFERS FROM A DATA PROCESSOR TO A DATA CONTROLLER

## 13. APPLICATION OF THIS MODULE C

**13.1** The Parties agree that this Module C applies in each case and only where Personal Data is transferred from Partner (acting as a Data Processor) to Tencent (acting as a Data Controller).

**13.2** The details of the transfers (as well as Personal Data) covered by this Module C are specified in Schedule B which form an integral part of this Module C.

**13.3** In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, clause 15 shall govern the terms of the transfer and clause 14 shall not apply.

## 14. OBLIGATIONS OF PARTNER

**14.1** Partner shall comply with the terms of clause 10 of Module B, and references to “Tencent” shall be read as a reference to “Partner”, and references to “Partner” shall be read as references to “Tencent”, for such purposes, in relation to any such Processing.

**14.2** Before Processing Personal Data, Partner shall implement, and ensure that its authorised personnel comply with, appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as well as ensuring that those measures continue to provide an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing as set out in Schedule C, or otherwise agreed and documented between Tencent and Partner from time to time, and shall continue to comply with them during the term of this DPA. Such measures shall include, as appropriate to the risk:

- a. the pseudonymisation and encryption of Personal Data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

**14.3** In the event that Partner directly receives a request from a Data Subject regarding Data Subject's Personal Data, or for the rectification or erasure of such Personal Data, or any other request or query from a Data Subject relating to its own Personal Data (including Data Subjects' exercising rights under Applicable Data Protection Laws, such as rights of objection, restriction of processing, data portability or the right not to be subject to automated decision making) (a “**Data Subject Request**”), Partner will:

- a. notify Tencent immediately of the Data Subject Request (without responding to that Data Subject Request, unless it has been otherwise authorised by Tencent to do so);
- b. provide details of the Data Subject Request (and any other relevant information Tencent may reasonably request) to Tencent within 3 business days of receipt of the Data Subject Request; and

c. provide such assistance to Tencent as Tencent may require for the purposes of responding to the Data Subject Request and to enable Tencent to comply with all obligations which arise as a result thereof.

**14.4** In the event there is, or Partner reasonably believes that there is, any Personal Data Breach in respect of Personal Data which is Processed by Partner under or in connection with this DPA, then upon becoming aware of such Personal Data Breach, Partner shall:

a. immediately notify Tencent in writing of all known details of the Personal Data Breach relating to the Personal Data, including:

i. a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects and records concerned;

ii. the name and contact details of the data protection officer or other contact point where more information can be obtained;

iii. a description of the likely consequences of the Personal Data Breach; and

iv. a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;

b. provide Tencent with regular status updates on any Personal Data Breach (including actions taken to resolve the incident) and share additional information related to the breach as soon as more details become available;

c. mitigate any harmful effect that is known to Partner of a use or disclosure of the Personal Data in violation of this DPA or in connection with a Personal Data Breach;

d. assist Tencent in remediating or mitigating any potential damage from a Personal Data Breach.

e. within 4 weeks of closure of the incident, provide Tencent a written report describing the Personal Data Breach, the root cause analysis, actions taken by Partner during its response and Partner's plans for future actions to prevent a similar Personal Data Breach from occurring;

f. not disclose to third parties (including Regulators) any information about a Personal Data Breach involving the Personal Data without prior written and express permission from Tencent for such disclosure; and

g. assist Tencent with notifying the Personal Data Breach to any Regulator or the Data Subject in accordance with, and in the timeframe required by, the Applicable Data Protection Laws.

**14.5** Partner shall not subcontract to any third party any of its obligations to Process Personal Data under this Module C unless all of the following provisions of this clause have first been complied with:

a. Partner has supplied to Tencent such information as Tencent may require to ascertain that such subcontractor has the ability to comply with Partner's obligations set out in this DPA and with Tencent's instructions;

b. Partner has obtained the prior written consent of Tencent; and

c. the proposed subcontractor has entered into a contract with Partner which requires the subcontractor to take adequate technical and organisational measures to safeguard the security and integrity of the relevant Personal Data and only Process data in accordance with the documented instructions of Tencent (including as set out in such contract with the proposed subcontractor), and which contains obligations on the relevant subcontractor which are no less onerous than the obligations on the Partner in, and which is no less protective of the Personal Data than, the terms of this DPA. The Partner shall provide, at Tencent's request, a copy of such subcontractor contract, and subsequent amendments, to Tencent.

**14.6** In the event that Tencent consents to subcontracting the Processing of Personal Data, Partner remains liable for the Processing under the terms of this DPA. The Partner shall notify Tencent of any failure by a subcontractor to fulfil its obligations under the relevant subcontractor contract.

**14.7** Partner will not, without the consent of Tencent, either:

- a. Process Personal Data in any Third Country; or
- b. permit any third party including its subcontractors to Process Personal Data in any Third Country.

**14.8** Partner shall permit Tencent at any time upon seven (7) days' notice, to be given in writing, to have access to the appropriate part of Partner's premises, systems, equipment, and other materials and data Processing facilities to enable Tencent (or its designated representative) to inspect or audit the same for the purposes of monitoring compliance with Partner's obligations under this DPA. Such inspection shall:

- a. be carried out by Tencent or an inspection body composed of independent members and in possession of the required professional qualifications and bound by a duty of confidentiality, selected by Tencent, where applicable, in agreement with the Regulator; and
- b. not relieve Partner of any of its obligations under this DPA.

## 15. EXPORT OF PERSONAL DATA

**15.1** In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 4 : Processor to Controller set out in Schedule F, which incorporate the provisions of Schedule B, and which together will form contractual terms between Tencent and Partner for that particular transfer of Personal Data.

**15.2** In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, set out in Schedule D-2, which incorporates the provisions of Schedule B and Schedule C, and which together will form contractual terms between Partner and Tencent for that particular transfer of Personal Data.

**15.3** In the case of a Relevant Data Export other than from the EEA or UK, the Parties shall ensure that such transfer is carried out, to the extent required by Applicable Data Protection Laws, using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this DPA); (b) a description of the Processing of Personal Data contemplated under this DPA; and (c) a description of technical and organisational measures to be implemented by the data importer, the Parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule B, and the description of technical and organisational measures set out in Schedule C, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations.



# MISCELLANEOUS (APPLICABLE TO ALL MODULES)

## 16. COOPERATION WITH REGULATORS

**16.1** The Parties agree that they shall and, where applicable, shall procure that their representatives shall cooperate, on request, with any relevant Regulator in the performance of its tasks pursuant to Applicable Data Protection Law.

## 17. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR A REGULATOR

In respect of any action or omission under this DPA:

- a. in the event of a dispute or claim brought by a Data Subject or a Regulator concerning the Processing of Personal Data against Tencent, Partner will inform Tencent about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion;
- b. Partner agrees to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by a Regulator. If they do participate in the proceedings, Partner may elect to do so remotely (such as by telephone or other electronic means); and
- c. each Party shall abide by a decision, as applicable, of a competent court of Tencent's country of establishment; of a competent court of the relevant Data Subject's country of habitual residence; or of the Regulator which is final and against which no further appeal is possible.

## 18. LIABILITY

**18.1** Without prejudice to any other rights or remedies that Tencent may have, Partner hereby acknowledges and agrees that a person with rights under this DPA may be irreparably harmed by any breach of its terms and that damages alone may not be an adequate remedy. Accordingly, a person bringing a claim under this DPA shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this DPA.

**18.2** Partner agrees that it will (in addition to, and without affecting, any other rights or remedies that Tencent may have whether under statute, common law or otherwise) indemnify, defend and hold harmless Tencent, its affiliates, and their respective employees, officers and directors (the "Tencent Parties") on demand from and against all claims, liabilities, costs, expenses, loss or damage incurred by a Tencent Party (including consequential losses, loss of profit



and loss of reputation and all interest, penalties and legal and other professional costs and expenses) arising directly or indirectly from a breach of Applicable Data Protection Law or this DPA by Partner or enforcement of any rights under it.

## 19. TERMINATION

**19.1** Termination of this DPA shall be governed by the applicable provisions in the relevant provisions in the Reseller Agreement.

**19.2** Upon termination of this DPA:

- a. each Party shall, except to the extent it acts as a Data Controller of such Personal Data, at the other Party's option, either forthwith:
  - i. return all of the Personal Data and any copies thereof which it is Processing or has Processed upon behalf of that Party. The return of the Personal Data shall result in the full deletion of the Personal Data existent in the IT equipment and systems used by the Party; or
  - ii. destroy all of the Personal Data and any copies thereof which it has Processed on behalf of that Party promptly and in any case within 14 days of being requested to do so by that Party. The Party shall certify the deletion of such data in writing to the other Party; and
  - iii. cease Processing Personal Data on behalf of the other Party under this DPA.

## 20. MISCELLANEOUS

Applicable clauses in relation to Assignment, Variation, Further Assurance, Invalidity, Waiver and Notices of the applicable Reseller Agreement shall apply *mutatis mutandis* to this DPA.

## 21. SERVICE-SPECIFIC TERMS

The Parties agree that certain Additional Terms may apply to certain services provided by or on behalf of Tencent from time to time in connection with the Partner program, and that such Additional Terms shall be deemed to be incorporated into this DPA.

## 22. ENTIRE AGREEMENT

These terms are the final and complete expression of all agreements between Partner and Tencent regarding Processing of Personal Data and supersede all prior oral and written agreements regarding these matter. In the event of any conflict between this DPA, the Reseller Agreement, or the Additional Terms, this DPA shall prevail to the extent

of the inconsistency solely to the extent such inconsistency relates to the Processing of Personal Data or any Applicable Data Protection Law.

## 23. COUNTERPARTS

This DPA may be entered into in any number of counterparts, all of which taken together shall constitute one and the same instrument.

## 24. GOVERNING LAW

**24.1** Subject to clause 24.2, this DPA shall be governed by Singapore law.

**24.2** The law governing Module A (Transfers between Data Controllers), 2 (Transfers from a Data Controller to a Data Processor), in respect of each transfer, be the law of the country in which the Data Discloser is established. The law governing Section 3 (Transfers from a Processor to a Controller) of this DPA shall, in respect of each transfer, be the law of the country in which the Data Receiver is established.

**24.3** Any dispute shall be referred to, and finally resolved by, arbitration administered by the Singapore International Arbitration Centre in accordance with the Arbitration Rules of the Singapore International Arbitration Centre for the time being in force when the notice of arbitration is submitted. The tribunal shall consist of one arbitrator. The seat of arbitration shall be Singapore and the language to be used in the arbitral proceedings shall be English.

## SCHEDULE A: LIST OF PARTIES

### Module A (Transfers between Controllers)

**Data Exporter and Importer(s) - Tencent:**

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Contact: cloudlegalnotices@tencent.com

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor):  
Controller

**Data Exporter and Importer(s) – Partner:**

Name: The relevant entity that entered into the Tencent Cloud Partner Program Terms and Conditions and the relevant Reseller Agreement with Tencent, who acting as Data Controller, agrees to receive Personal Data from the Partner disclosing the data.

Address: The address provided to Tencent when signing up to act as a reseller of Tencent cloud services. Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Reseller of Tencent Role (controller/processor): Controller

**Module B (Transfers from a Data Controller (Partner) to a Data Processor (Tencent))****Data exporter(s) –Partner:**

Name: The relevant Party that entered into the Tencent Cloud Partner Program Terms and Conditions and the relevant Partner Agreement with Tencent, who acting as Data Controller transfers Personal Data to Tencent. Address: The address provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Partner of Tencent Role (controller/processor): Controller

**Data importer(s) –Tencent:**

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Contact: cloudlegalnotices@tencent.com

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor): Processor

**Module C (Transfers from a Data Processor (Partner) to a Data Controller (Tencent))****Data exporter(s) –Partner:**

Name: The relevant Party that entered into the Tencent Cloud Partner Program Terms and Conditions and the relevant Partner Agreement with Tencent, who acting as Data Processor transfers Personal Data to Tencent.

Address: The address provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Contact person's name, position and contact details: The details provided to Tencent when signing up to act as a reseller of Tencent cloud services.

Activities relevant to the data transferred under these Clauses: Partner of Tencent Role (controller/processor):  
Processor

**Data importer(s) –Tencent:**

**Tencent Cloud Europe B.V.**, a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands., if Partner is located in European Economic Area, UK and Switzerland

**Tencent Cloud LLC**, a Delaware corporation registered company located at Claremont 2747 Park Blvd, Palo Alto, CA 94306., if Partner is located in North America

**Tencent Korea Yuhan Hoesa**, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, South Korea, if Partner is located in South Korea

**Aceville Pte Ltd**, a Singapore-registered company located at 30 Raffles Place, #12-01, Oxley @ Raffles, Singapore 048622., if Partner is located in the rest of the world except People's Republic of China

Activities relevant to the data transferred under these Clauses: Cloud service provider Role (controller/processor):  
Controller

## SCHEDULE B: DESCRIPTION OF TRANSFERS

*Categories of data subjects whose personal data is transferred*

Individuals employed by or representing the Partner Partner's customer(s)

*Categories of personal data transferred*

Name, Email address, address, business registration number (and photo), job title, mobile number, payment details (bank name, account name, bank account, swift code), invoice information (Payer Account ID, Owner Account ID, Operator Account ID), and any other personal data made available by or on behalf of Partner/Partner's customer(s), or otherwise accessible directly or indirectly via the Partner Console.

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

No sensitive personal data transferred

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

For the duration of the DPA

*Nature of the processing*

Partner will act as a reseller of Tencent cloud services for certain customers. Partner shall administer and manage resell activities relating to its end users through the functions and tools provided through Partner Console or via other

processes authorized or designated by Tencent and this will involve processing personal data.

*Purpose(s) of the data transfer and further processing*

To facilitate the reselling of Tencent Services by the Partner, including (without limitation and in each case to the extent the relevant services, features, support or functions are provided):

making available or accessible, directly or indirectly, Personal Data via the Partner Console

provision of integrated / value-added services by the Partner to its customers (if applicable)

customer account creation via email invite sent by Partner on the Tencent Cloud console

placement of orders / Purchase Orders for Tencent Services

fulfilment of orders / Purchase Orders (i.e. performance of Tencent Services)

billing (for Tencent to issue invoices to Partner)

payment by Partner to Tencent

for Tencent to respond to requests for and to provide after-sales customer support

access to online training materials and support from Tencent

access to dedicated online documents and support from Tencent

provision of certification training by Tencent

provision of certification vouchers by Tencent

assigning dedicated solution architect(s) for support

usage of Tencent's Partner Badge by Partner

Partner company listing in Tencent's Partner Directory

Usage of logo featured on Tencent's Partner Portal

participation in Tencent's marketing activities (details subject to Tencent's approval)

joint case study opportunities (details subject to Tencent's agreement)

joint press release development (details subject to Tencent's agreement)

opportunities for co-branding and co-marketing activities

marketing development fund (details subject to Tencent's agreement)

issuing of Premier Partner Award(s)

issuing of Partner voucher benefits (details subject to Tencent's agreement)

joint customer development with Tencent's sales team (details subject to Tencent's agreement)

rebate of order amount

assigning a dedicated partner manager for support

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

The retention period will follow the data retention policy as set out in the Privacy Policy on the Tencent website.

*For transfer to (sub-)processors, also specify subject matter, nature and duration of the processing*

N/A

*Identify the competent supervisory authority/ies in accordance with Clause 13 of Schedules D, E and F*

The Netherlands

## SCHEDULE C: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Where applicable this Schedule C also forms part of the Standard Contractual Clauses.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

\\1. **Data security.** The data importer shall design and implement the following measures to protect customer's data against unauthorized access:

standards for data categorisation and classification;

a set of authentication and access control capabilities at the physical, network, system and application levels; and  
a mechanism for detecting big data-based abnormal behaviour.

\\2. **Network security.** The data importer shall implement stringent rules on internal network isolation to achieve access control and border protection for internal networks (including office networks, development networks, testing networks and production networks) by way of physical and logical isolation.

\\3. **Physical and environmental security.** Stringent infrastructure and environment access controls shall be implemented for data centers based on relevant regional security requirements. An access control matrix is established, based on the types of data center personnel and their respective access privileges, to ensure effective management and control of access and operations by data center personnel.

\\4. **Incident management.** The data importer shall operate active and real-time service monitoring, combined with a rapid response and handling mechanism, that enables prompt detection and handling of security incidents.

\\5. **Compliance with standards.** The data importer shall comply with the standards listed in Tencent's Compliance Center page, and as updated from time to time.

## SCHEDULE D-1: STANDARD CONTRACTUAL CLAUSES

### MODULE 1: CONTROLLER TO CONTROLLER TRANSFER

#### Section I

##### Clause 1: Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

### **Clause 2: Effect and invariability of the Clauses**

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### **Clause 3: Third-party beneficiaries**

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii. Clause 8 - Clause 8.5 (e) and Clause 8.9(b);

iii. Clause 12 - Clause 12(a) and (d);

iv. Clause 13;

v. Clause 15.1(c), (d) and (e);

vi. Clause 16(e);

vii. Clause 18 - Clause 18(a) and (b).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### **Clause 4: Interpretation**

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### **Clause 5: Hierarchy**



In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

**Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**Section II – OBLIGATIONS OF THE PARTIES****Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- i. where it has obtained the data subject's prior consent;
- ii. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iii. where necessary in order to protect the vital interests of the data subject or of another natural person.

**8.2 Transparency**

- a. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
  - i. of its identity and contact details;
  - ii. of the categories of personal data processed;
  - iii. of the right to obtain a copy of these Clauses;
  - iv. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- b. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a



disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

c. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

d. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### 8.3 Accuracy and data minimisation

a. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

b. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

c. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

### 8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

### 8.5 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

c. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures

to mitigate its possible adverse effects.

e. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

f. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

g. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

## 8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

## 8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- i. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

- iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### **8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

#### **8.9 Documentation and compliance**

- a. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- b. The data importer shall make such documentation available to the competent supervisory authority on request.

#### **Clause 9: Use of sub-processors Clause 10: Data subject rights**

- a. The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- b. In particular, upon request by the data subject the data importer shall, free of charge:
  - i. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
  - ii. rectify inaccurate or incomplete data concerning the data subject;
  - iii. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

- c. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- d. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the law of the country of destination, provided that such law lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
- i. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  - ii. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- e. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- f. The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- g. If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

#### **Clause 11: Redress**

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
- i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**Clause 12: Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

**Clause 13: Supervision**

- a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES****Clause 14: Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to

disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### **Clause 15: Obligations of the data importer in case of access by public authorities**



### 15.1 Notification

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### 15.2 Review of legality and data minimisation

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## Section IV – FINAL PROVISIONS

**Clause 16: Non-compliance with the Clauses and termination**

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
- i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - ii. the data importer is in substantial or persistent breach of these Clauses; or
  - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17: Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands (*specify Member State*).

**Clause 18: Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of The Netherlands (*specify Member State*).
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.



**APPENDIX TO SCHEDULE D-1 (SCCS MODULE 1)****ANNEX I****A. LIST OF PARTIES**

See Schedule A to the DPA

**B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA

**C. COMPETENT SUPERVISORY AUTHORITY**

See Schedule B to the DPA

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

See Schedule C to the DPA

# SCHEDULE D-2:INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the UK Information Commissioner's Office for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

**PART 1: TABLES****TABLE 1: PARTIES**

<b>Start date</b>	<b>See effective date of the DPA</b>	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	<b>See Schedule A of the DPA</b>	
<b>Key Contact</b>	<b>See Schedule A of the DPA</b>	

**TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES**

<b>AddendumEU SCCs</b>	<b>The Approved EU SCCs, including the Appendix Information, set out in Schedule D-1, Schedule E or Schedule F to the DPA, as applicable</b>
------------------------	--

**TABLE 3: APPENDIX INFORMATION**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: <b>See Schedule A to the DPA</b>	
Annex 1B: Description of Transfer: <b>See Schedule B to the DPA</b>	
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: <b>See Schedule C to the DPA</b>	
Annex III: List of Sub processors (Modules 2 and 3 only): <b>N/A</b>	

**TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES**

<b>Ending this Addendum when the Approved Addendum changes</b>	Which Parties may end this Addendum as set out in Section 19: Neither Party
--	---

## Part 2: Mandatory Clauses

### Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

- Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

<b>Addendum</b>	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
<b>Addendum EU SCCs</b>	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
<b>Appendix Information</b>	As set out in Table 3.
<b>Appropriate Safeguards</b>	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on

	standard data protection clauses under Article 46(2)(d) UK GDPR.
<b>Approved Addendum</b>	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022.
<b>Approved EU SCCs</b>	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
<b>ICO</b>	The Information Commissioner.
<b>Restricted Transfer</b>	A transfer which is covered by Chapter V of the UK GDPR.
<b>UK</b>	The United Kingdom of Great Britain and Northern Ireland.
<b>UK Data Protection Laws</b>	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
<b>UK GDPR</b>	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

#### Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the

inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

#### **Incorporation of and changes to the EU SCCs**

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

- a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
- b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

- c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

- d. Clause 8.7(i) of Module A is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

- f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

- g. References to Regulation (EU) 2018/1725 are removed;
- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- j. Clause 13(a) and Part C of Annex I are not used;
- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with:  
“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply.”;
- m. Clause 17 is replaced with:  
“These Clauses are governed by the laws of England and Wales.”;
- n. Clause 18 is replaced with:  
“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

#### **Amendments to this Addendum**

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a. its direct costs of performing its obligations under the Addendum; and/or
- b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing

written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

## SCHEDULE E: STANDARD CONTRACTUAL CLAUSES

### MODULE 2: CONTROLLER TO PROCESSOR TRANSFER

#### Section I

##### Clause 1: Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

- i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### Clause 2: Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

##### Clause 3: Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- ii. Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
- iii. Clause 9 - Clause 9(a), (c), (d) and (e);
- iv. Clause 12 - Clause 12(a), (d) and (f);
- v. Clause 13;
- vi. Clause 15.1(c), (d) and (e);
- vii. Clause 16(e);
- viii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### **Clause 4: Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **Section II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Instructions**

- a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.



b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

## 8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

## 8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

## 8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

## 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

## 8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved



in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

- a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### Clause 9: Use of sub-processors

- a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least twenty business days' in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### **Clause 10: Data subject rights**

- a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **Clause 11: Redress**

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### **Clause 12: Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13: Supervision**

- a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority,

including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### **Clause 14: Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if

it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### **15.2 Review of legality and data minimisation**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has



decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **Section IV – FINAL PROVISIONS**

##### **Clause 16: Non-compliance with the Clauses and termination**

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17: Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands.

**Clause 18: Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of The Netherlands (specify Member State).
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

## APPENDIX TO SCHEDULE E (SCCS MODULE B)

**ANNEX I****A. LIST OF PARTIES**

See Schedule A to the DPA

**B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA

**C. COMPETENT SUPERVISORY AUTHORITY**

See Schedule B to the DPA

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

See Schedule C to the DPA

## SCHEDULE F: STANDARD CONTRACTUAL CLAUSES

### MODULE 4: PROCESSOR TO CONTROLLER TRANSFER

**Section I****Clause 1: Purpose and scope**

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.



b. The Parties:

- i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

**Clause 2: Effect and invariability of the Clauses**

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

**Clause 3: Third-party beneficiaries**

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- ii. Clause 8 - Clause 8.1 (b) and Clause 8.3(b);
- iii. Clause 15.1(c), (d) and (e);
- iv. Clause 16(e);
- v. Clause 18.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4: Interpretation**

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**Clause 5: Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6: Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7: Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

### **Section II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8: Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Instructions**

- a. The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- b. The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- c. The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- d. After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

##### **8.2 Security of processing**

- a. The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- b. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under

these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

c. The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### **8.3 Documentation and compliance**

a. The Parties shall be able to demonstrate compliance with these Clauses.

b. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

### **Clause 9: Use of sub-processors Clause 10: Data subject rights**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

### **Clause 11: Redress**

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

### **Clause 12: Liability**

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

### **Clause 13: Supervision**

## **Section III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

### **Clause 14: Local laws and practices affecting compliance with the Clauses**

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the

essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15: Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **15.2 Review of legality and data minimisation**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **Section IV – FINAL PROVISIONS**

**Clause 16: Non-compliance with the Clauses and termination**

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17: Governing law**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands (*specify country*).

**Clause 18: Choice of forum and jurisdiction**

Any dispute arising from these Clauses shall be resolved by the courts of The Netherlands (*specify country*).

**APPENDIX TO SCHEDULE F (SCCS MODULE 4)****ANNEX I**

---

**A. LIST OF PARTIES**

See Schedule A to the DPA

**B. DESCRIPTION OF TRANSFER**

See Schedule B to the DPA

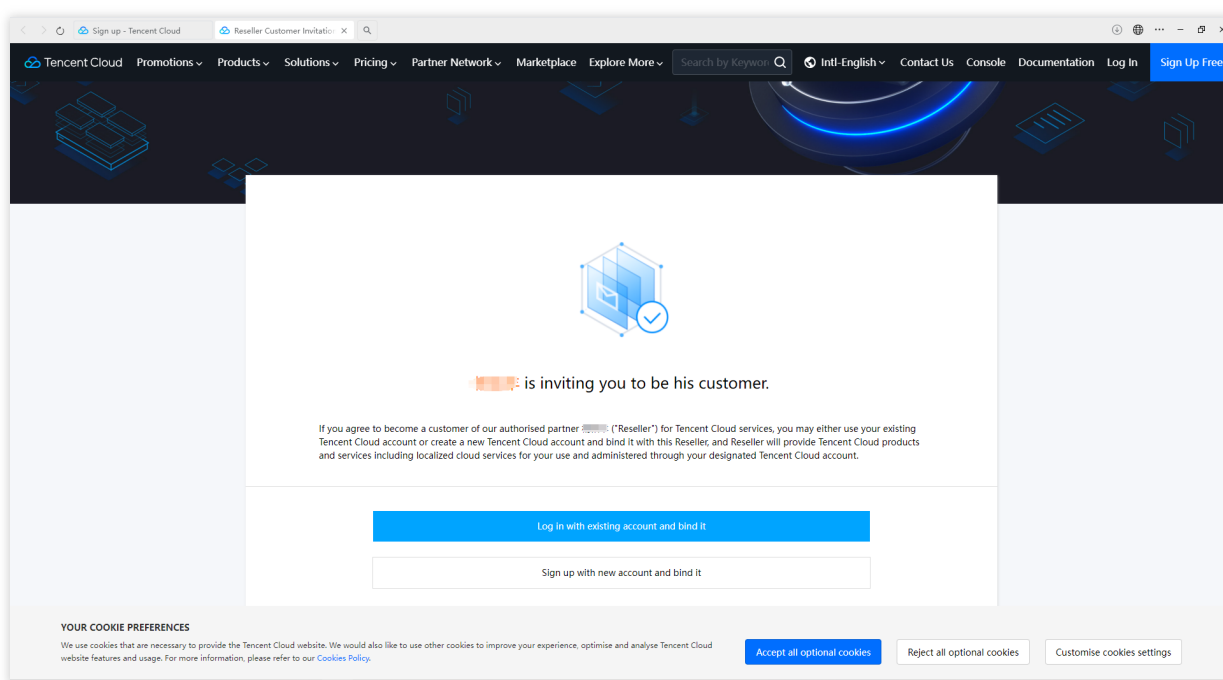
# 子客

## 受邀绑定成为子客

最近更新时间：2024-05-10 10:28:36

### 1. 绑定方式

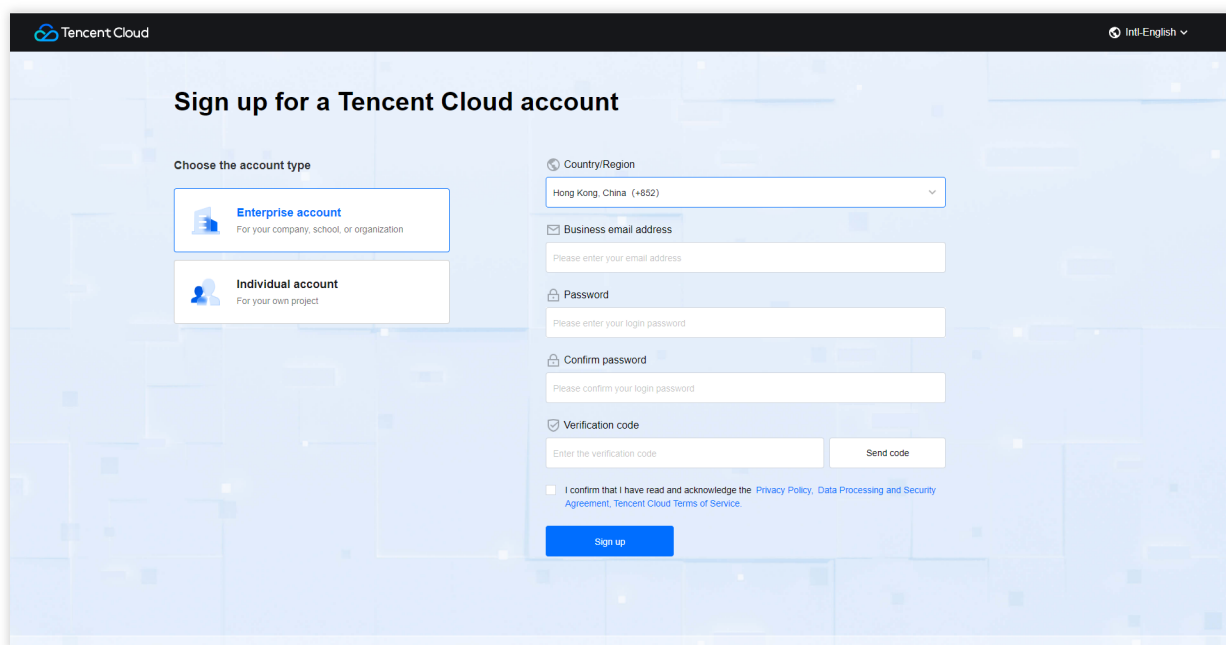
点击经销商的邀请链接，选择“登录已有账号”或者“注册新账号”绑定成为子客。



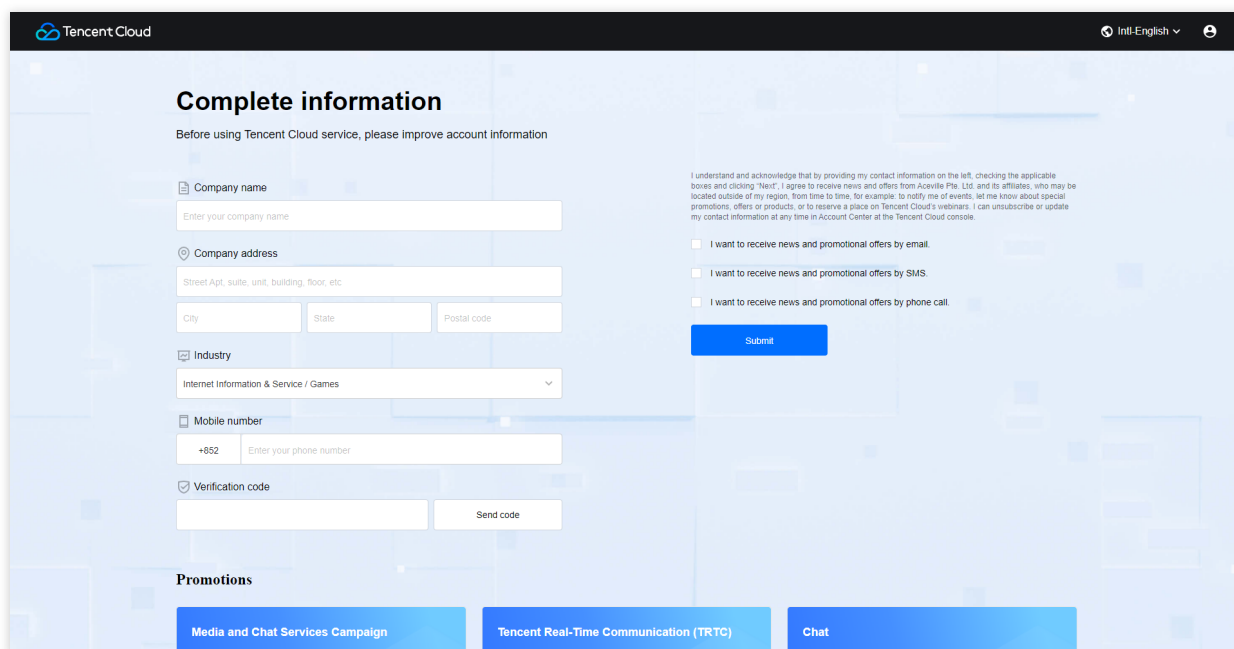
### 2. 账号注册

第一步：点击经销商的邀请链接，进入注册页面，填写注册信息。（必须通过邀请链接进入）





第二步：完善账号信息，填写企业名称、地址、手机号等，提交信息后，等待经销商审核，审核通过后成功绑定经销商，即可登录控制台。



# 购买产品

最近更新时间：2022-07-11 19:10:41

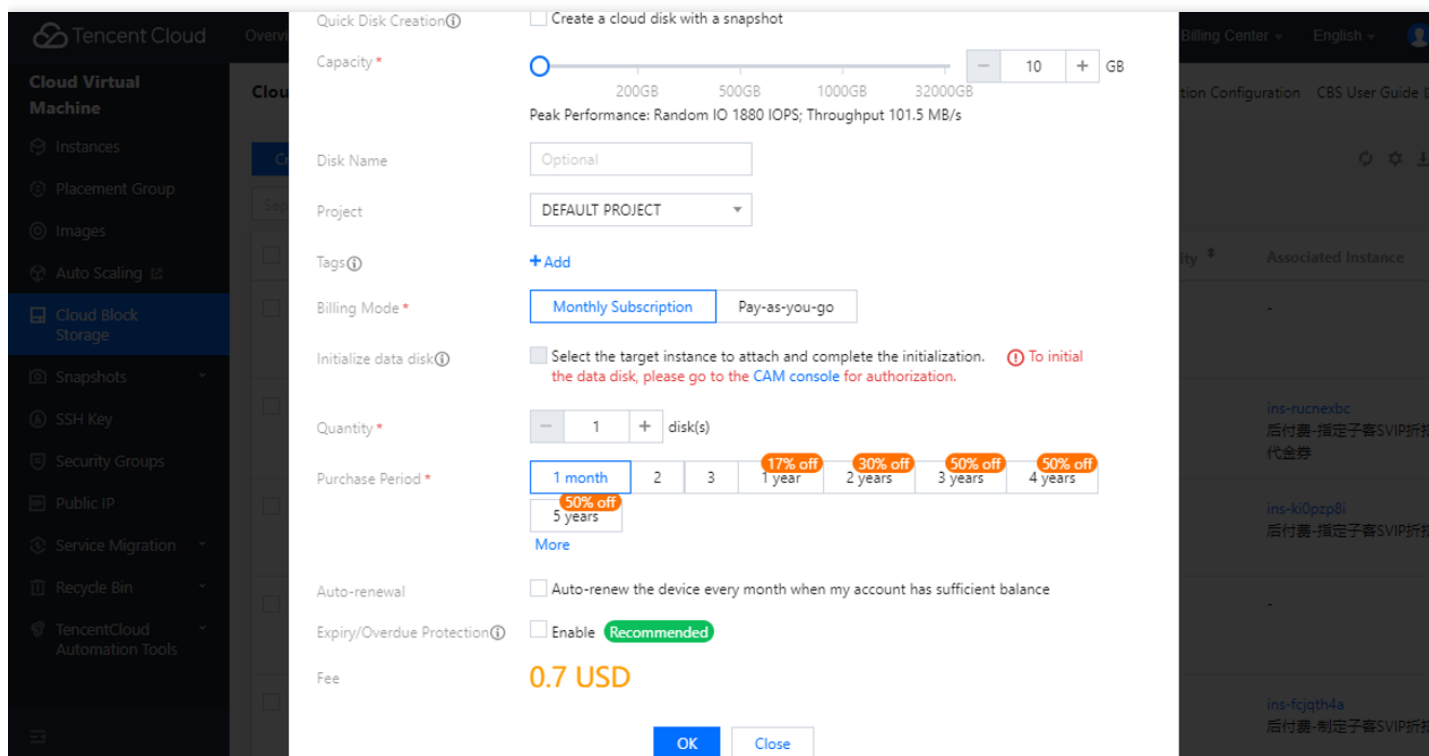
## 购买产品

经销商的子客可以登录腾讯云控制台购买产品，包含包年包月和按量付费产品。

### 操作步骤

#### 包年包月产品，以购买云硬盘为例

1、根据您的业务需求选择 云硬盘的 配置信息，并点击确定。



## 2、查看商品清单

Please confirm the following product information | [Go Back to Modify Configuration](#)

Product List

cbs

0.70 USD

Disk Usage: Data Disk

Disk Size: 10 GB

Disk Type: Premium Cloud Disk

Disk Name: Unnamed

Disk Backup Quota: 0

Availability Zone: ap-guangzhou-3

Unit Price: 0.70USD/month

Quantity: 1

Payment Mode: Prepaid

Term: 1month

Check the Fees

cbs x1

0.70USD

Subtotal:

0.70USD

Total

0.70 USD

Submit Order

## 3、下单和支付。

注意：

- 如果子客可用额度不足，会报错如下。请子客联系经销商，给经销商还款或由经销商提高子客的额度。
- 处理之后，子客不需要再次下单。经销商可以在合作伙伴控制台针对子客的“已下单待支付”订单，进行代付处理。

Please confirm the following product information

Order 20220701073000019459201

cbs

0.70 USD

Disk Usage: Data Disk

Disk Size: 10 GB

Disk Type: Premium Cloud Disk

Disk Name: Unnamed

Disk Backup Quota: 0

Availability Zone: ap-guangzhou-3

Check the Fees

cbs x1

0.70USD

Subtotal:

0.70USD


Total

0.70 USD

Pay Now

Please Select a Payment Method

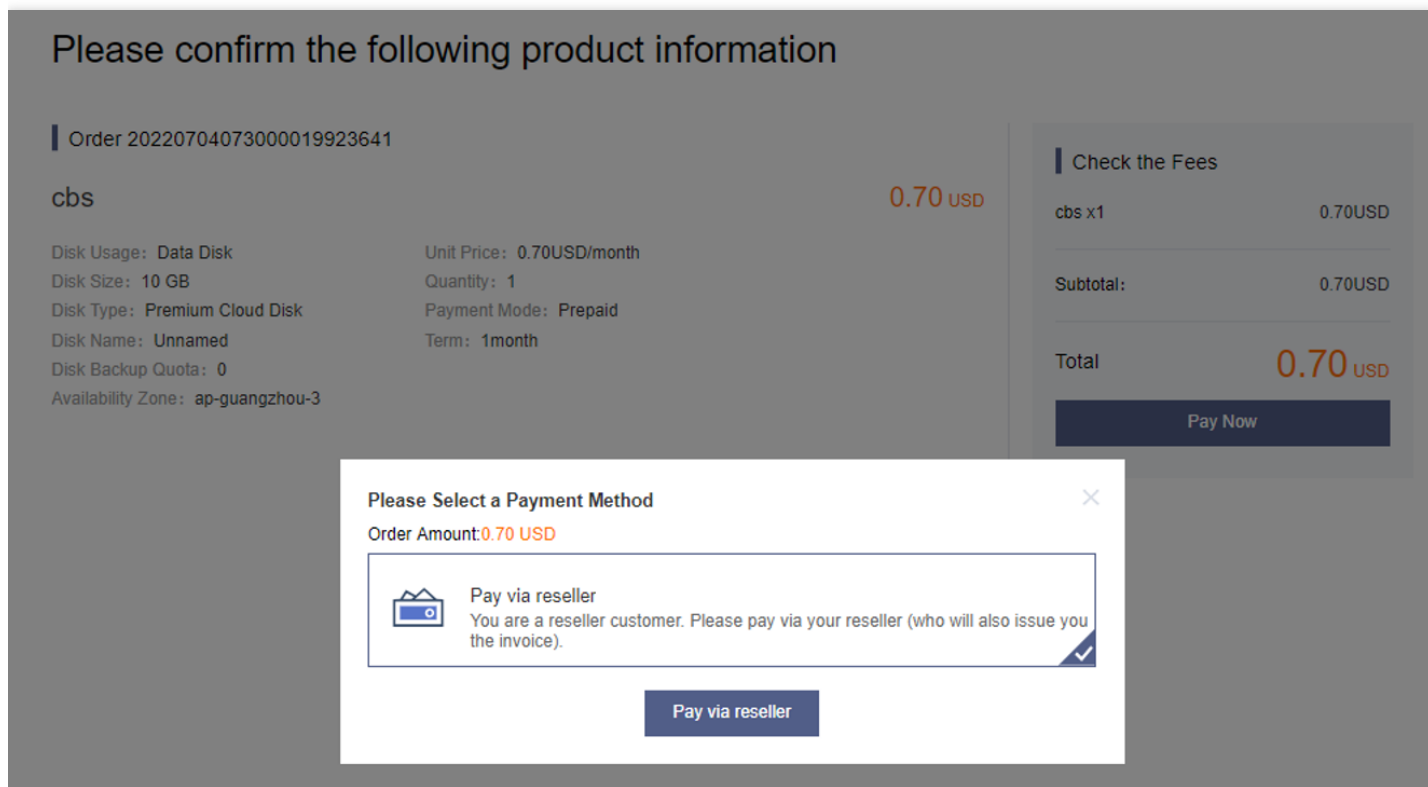
Order Amount: 0.70 USD

 Pay by Credit

You have insufficient available credit. Please contact your reseller to raise your credit limit and pay via your reseller.

OK

如果子客额度足够，则选择由经销商代付。



#### 4、查看支付结果。

经销商额度足够时，订单会自动代付成功。子客可以到对应的产品控制台查看对应的资源实例。

注意：

如果经销商额度不足，则会支付失败。请子客联系经销商处理。子客不需要再次下单，经销商自身提高额度之后，可以在合作伙伴控制台针对子客的“已下单待支付”订单，进行代付处理。



## Payment succeeded

Payment via reseller successful

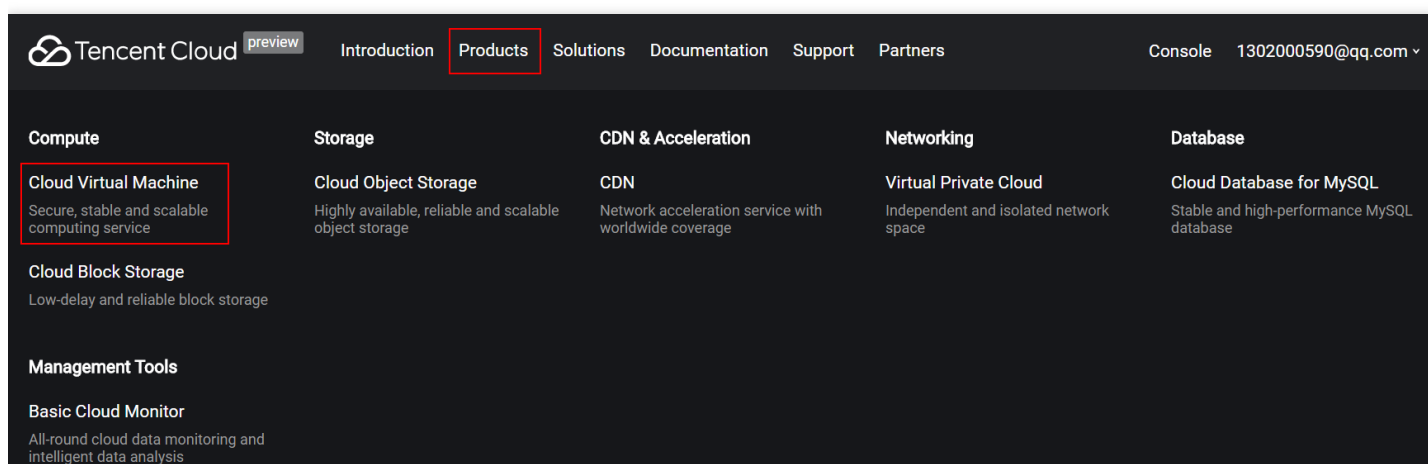
[Go to Console](#)

说明：

针对包年包月产品的退订，请子客提交工单处理。暂不支持包年包月的升配、降配处理。

### 按量付费产品，以购买CVM为例

1、在云产品导航栏中，选择您要购买的服务。在这种情况下，它将是CVM。



2、进入产品概览页面后，您可以查看产品详情，单击体验购买产品。

Tencent Cloud

preview

Introduction

Products

Solutions

Documentation

Support

Partners

Console

1302000590@qq.com

Compute

Cloud Virtual Machine

Cloud Block Storage

Storage

Database

Networking

Management Tools

Cloud Virtual Machine

Cloud Virtual Machines (CVM) provide adjustable compute capacities, allowing you to estimate compute scale easily. Within a few minutes, you can purchase a virtual machine with your desired configurations, and conduct fast expansion as required with the help of images.

Experience

CVM

### 3、根据您的业务需求选择 CVM 配置信息。

1. Select the region and model

2. Select an image

3. Select storage and network

4. Set information

Billing Mode

Postpaid

Region

Guangzhou

Shanghai

Beijing

Toronto

Availability Zone

Toronto Zone 1

Cloud Services in different regions cannot interwork with each other through the private network. Select the region nearest to your customer to reduce the access latency and improve the downloading speed. [View My CVM Region](#) [Detailed Comparison](#)

Model

Model	vCPU	MEM	Support Cloud Disks	Fee
<input checked="" type="radio"/> StandardS1	1-core	2G	No	0.05 USD/ hours up
<input type="radio"/> StandardS1	1-core	4G	No	0.07 USD/ hours up
<input type="radio"/> StandardS1	1-core	8G	No	0.12 USD/ hours up
<input type="radio"/> StandardS1	2-core	4G	No	0.10 USD/ hours up

Next: Select an image

The initial price covers only the CPU and MEM fees. The system disk, data disk, image and bandwidth fees are NOT included.

4、选择配置后，检查CVM信息并进行确认。然后点击立即购买。

1. Select the region and model

2. Select an image

3. Select storage and network

4. Set information

Password

.....

The password for Linux servers should contain 8-16 characters, including 2 of the following types: [a-z, A-Z] , [0-9] and [()~!@#\$%^&\*~+=\_[]:;'<>.,?/]

Confirm Password

.....

Security Groups

Open port 22 on Linux CVMs-2017070316...

Preview Rules

Operation Guide

To open other ports, you can [create a security group](#)

Security Service

☒ FREE subscription

Install components to activate security services (anti-DDoS, WAF, server protection)[Details](#)

Cloud Monitoring

☒ FREE subscription

FREE cloud service monitoring, analysis, alarming, and server monitoring metrics (component installation required)[Details](#)

Fee:

Configuration Fee

0.06 USD/hr (Tiered pricing [Pricing Details](#) )

Network Fee

0.08 USD/GB

Back

Buy Now

5、子客可用额度 $\geq 0$ ,对应经销商可用额度 $\geq 0$ ,且足够覆盖冻结金额，会开通成功；

开通后，您刚刚购买的CVM将显示在您腾讯云控制台的云虚拟机页面。您可以查看产品的状态。如果状态为“正在运行”，则可以使用刚购买的 CVM。

注意：

如果开通失败，有可能是子客或经销商的可用额度不足，请子客联系经销商还款或提高额度，再重新进行开通。

Tencent Cloud

Console HomeProducts

130200059...Billing CenterTicket

Cloud Virtual Machine

Cloud Virtual Machine

Guangzhou(7)Shanghai(0)Beijing(0)Toronto(3)

+ NewStart upShutdownRestartRenewReset passwordMore actions

Use '|' to split more than one keyword, and press

ID/Name	Monitor/St...	Availabilit...	Model	Configuration	Primary IP	Project	Operation
<input checked="" type="checkbox"/> ins-55qsj9tr Unnamed	Running	Toronto Zone1	S1	1-core 2GB 1Mbps System disk:Local disk Network: Basic ...	45.113.71.180(Public) 10.212.196.234(Priva...	Default Project	<a href="#">Log In</a> <a href="#">More</a>
<input type="checkbox"/> ins-8t7n5tzip Unnamed	Running	Toronto Zone1	S1	1-core 2GB 1Mbps System disk:Local disk Network: Basic ...	45.113.69.210(Public) 10.212.197.51(Private)	Default Project	<a href="#">Log In</a> <a href="#">More</a>
<input type="checkbox"/> ins-rvmsu8u1 Unnamed	Running	Toronto Zone1	S1	1-core 2GB 1Mbps System disk:Local disk Network: Basic ...	45.113.71.84(Public) 10.212.196.60(Private)	Default Project	<a href="#">Log In</a> <a href="#">More</a>



# 账户管理

## 代金券

最近更新时间：2024-06-14 15:17:28

## 代金券

### 说明：

系统自动优先扣减代金券，再扣减信用

申请退款时，代金券不支持退还，具体规则请参见[云服务退货说明](#)

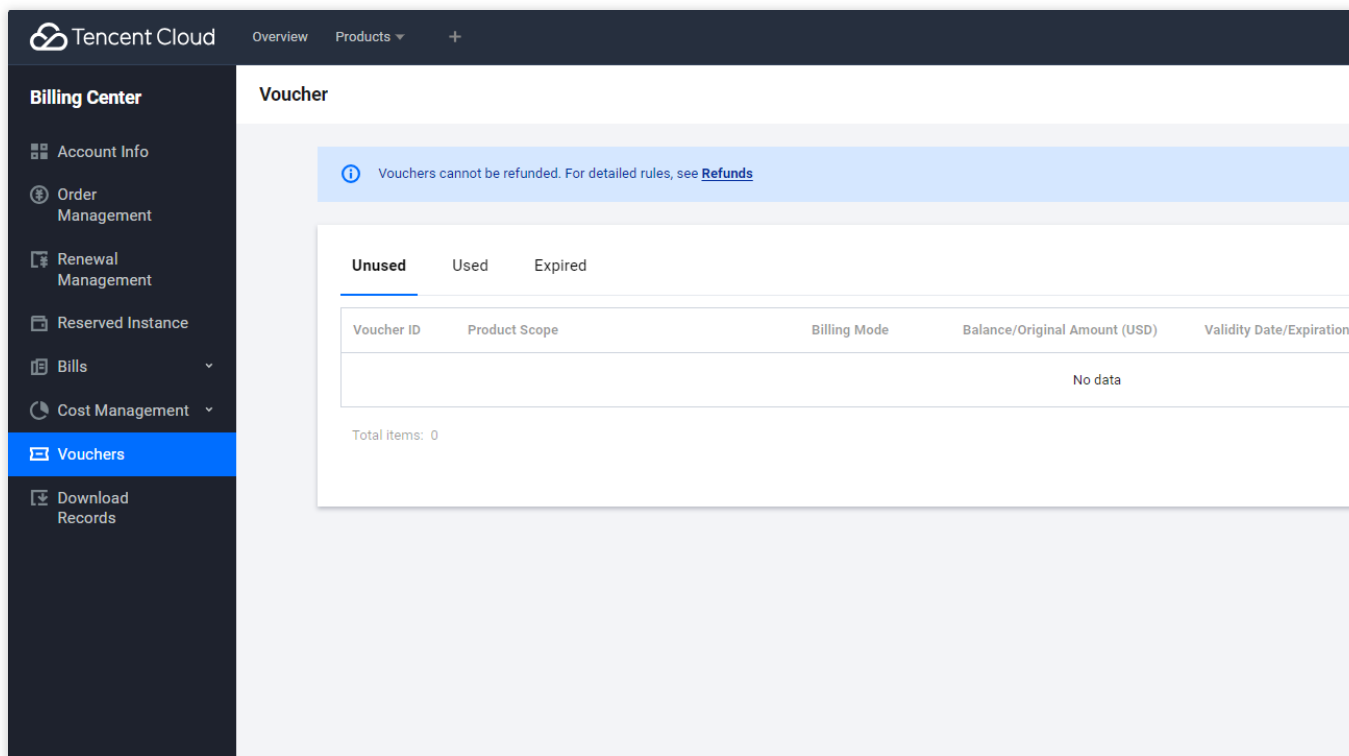
### 1、代金券的申请

子客的代金券，均由经销商进行分配管理，如果子客需代金券，请联系经销商。

### 2、代金券的查看

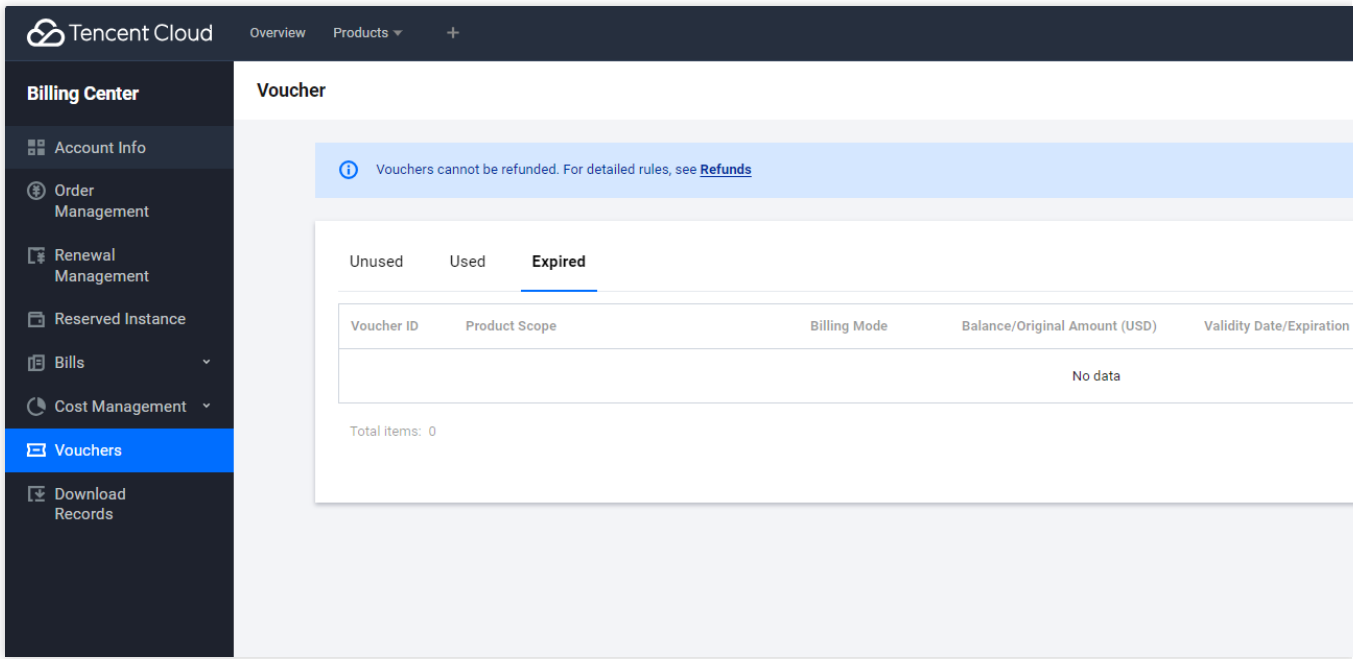
#### （1）代金券概览

经销商分配子客代金券后，子客可通过[Billing Center](#)查看代金券。



#### （2）代金券列表

已使用、未使用、已过期代金券，子客可通过[代金券](#)查看。



### 3、代金券的使用

子客下单页面，不显示代金券，系统会自动扣减代金券，可查看使用记录。

# 信用额度

最近更新时间：2022-07-08 17:12:58

## 信用额度

### 1. 信用额度申请

子客信用额度均有经销商进行分配管理，如需要调整信用额度，请联系您的经销商。（注：您的信用额度全权由经销商分配，不与腾讯云产生资金关联）

### 2. 信用额度查看

子客可登录[控制台-费用中心/账户信息](#)查看自己信用额度。可用信用额度=总信用额度-已使用信用额度

The screenshot shows the Tencent Cloud Billing Center interface. On the left is a navigation menu with options like Billing Center, Account Info, Order Management, Renewal Management, Bill Details, Vouchers, and Download Records. The main content area is titled 'Account Info' and contains a notice about credit limits. Below the notice, there are two summary cards: 'Available Credit' showing 4.62 USD, and 'Vouchers' showing 1 voucher worth 15.00 USD. At the bottom, a table shows 'Total Credit' as 20.84 USD and 'Used Credit' as 16.22 USD.

Item	Value
Available Credit	4.62 USD
Total Credit	20.84 USD
Used Credit	16.22 USD
Vouchers	1 voucher (15.00 USD)

说明：

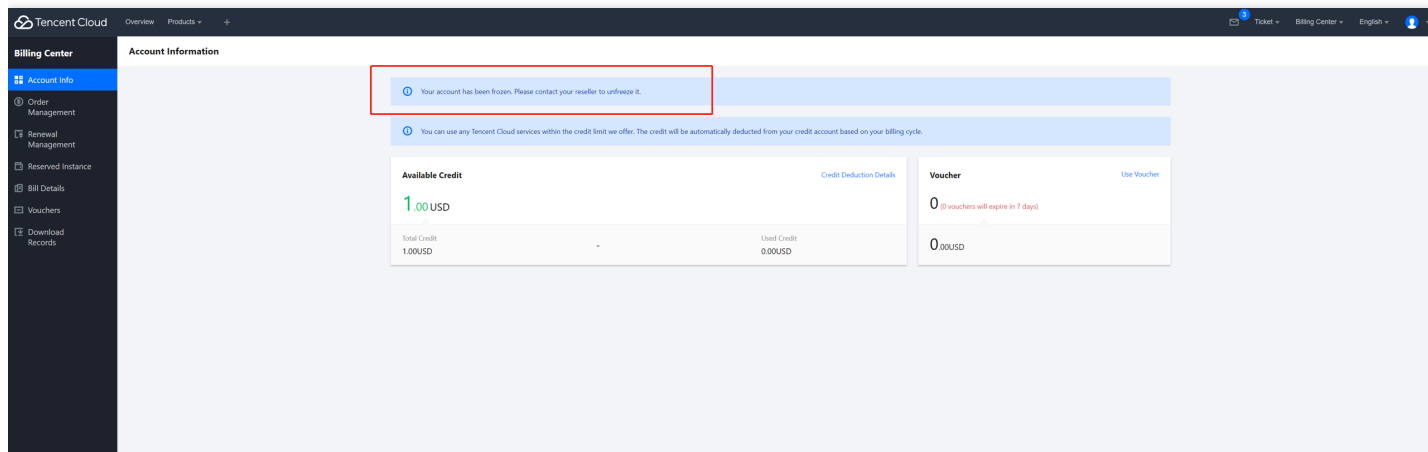
若您的历史账单已经回款至经销商，请联系您的经销商进行线上确认回款操作，已回款的账单金额会返还至您的可用信用度中。

# 账户冻结

最近更新时间：2022-12-21 11:57:39

## 1. 账户冻结状态

子客账户被经销商冻结后，您的账户首页将会出现账户冻结的提示。



## 2. 账户冻结影响

账户将无法进行新购、续费、资源升配、付费模式互转等操作，已购买的预付费资源如未到期可以继续使用，已开通的后付费资源将按照[子客停服规则](#)立即停服，您的资源使用会受到影响。如需恢复服务，请尽快联系您的经销商恢复账户，避免产品立即停服对您客户业务造成影响。

# 账户资产变化的影响

## 对新购的影响

最近更新时间：2022-07-08 17:15:14

### 对新购的影响

子客的账户资产，分为信用额度、代金券两部分，对子客新购产品影响如下：

#### 1、购买预付费产品

【不可新购产品】情况：

(1) 子客可用信用额度 $<0$ ，此时子客在停服流程中，不允许新购产品。

指引：子客需联系合作伙伴，进行信用额度增加分配，恢复服务。

(2) 子客可用信用额度+子客可用代金券 $<$ 订单额度，此时子客账户资产不足，不允许新购产品。

指引：子客需联系合作伙伴，增加信用额度或者代金券。

说明：

经销商可用信用额度不足，无法代付子客订单额度，此时子客也不允许新购产品。

#### 2、购买后付费产品

【不可新购产品】情况：

(1) 子客可用信用额度 $<0$ ，此时子客在停服流程中，不允许新购产品。

指引：子客需联系合作伙伴，进行信用额度增加分配，恢复服务。

(2) 子客可用信用额度+子客可用代金券 $<$ 经销商冻结金额，此时子客账户资产不足，不允许新购产品。

指引：子客需联系合作伙伴，增加信用额度或者代金券。

说明：

经销商冻结金额，当子客开通后付费产品时，会冻结经销商信用额度。

# 对停服和恢复的影响

最近更新时间：2023-06-13 20:51:29

## 对停服和恢复的影响

子客的账户资产，分为信用额度、代金券两部分，对子客停服和恢复影响如下：

### 1、对停服的影响

当资产额度不够的情况，会触发子客的资源停服，子客和经销商均会收到停服通知。

- (1) 停服触发：可用信用额度【 $\geq 0$ 】变为【 $< 0$ 】。
- (2) 停服流程：根据不同产品的生命周期，会陆续停服。
- (3) 处理指引：如果接到停服通知，可联系经销商进行信用、代金券调整，恢复资源使用。

说明：

- 如果子客开通欠费不停服特权，则不会停服。
- 联系销售经理可申请开通子客欠费停服规则缩短停服期，具体规则请参考[子客欠费停服规则](#)说明。

### 2、对恢复的影响

当子客资产额度恢复，会触发子客的资源恢复，子客和经销商均会收到恢复通知。

- (1) 恢复触发：可用信用额度【 $< 0$ 】变为【 $\geq 0$ 】。
- (2) 恢复流程：根据不同产品的恢复流程，会陆续恢复子客资源。

# 账单管理

## 子客账单

最近更新时间：2024-07-04 15:49:34

### 子客账单

#### 查看账单

##### 说明：

账单出账时间约1个小时，预付费产品账单在购买后的约1小时产生，后付费产品账单在产品结算周期后约1小时后产生。

当月账单有可能因为实时推送网络原因出现漏单，准确的账单以月账单为准（于次月5号可进行查看）。

子客账单不显示代金券扣减信息。

涉及到线下购买的产品，将由产品团队出经销账单，交于渠道经理。

该界面信息仅展示系统升级后的账信息，您的历史账单请至[历史账单](#)页查询。

第一步：子客可登录[控制台-费用中心](#)查看自己帐单。

Tencent Cloud

OverviewProducts+

Billing Center

Account Info

Order Management

Renewal Management

Billing Details

Vouchers

Bill Details

2022-06

All products

Please choose one product

Please choose one subproduct

All Projects

All Zones

All Billing Modes

All Transaction Types

☐ Do not display \$0 trans

Instance ID	Instance Name	Product Name	Billing Mode	Project Name
ins-fcjqth4a			Pay-As-You-Go resources	default
ins-fcjqth4a			Pay-As-You-Go resources	default
ins-ki0pzp8i			Pay-As-You-Go resources	default
ins-ki0pzp8i			Pay-As-You-Go resources	default

第二步：可以根据页面顶部日历筛选账单月份。

Bill Details

2022-06

Bill Details

The current month's final bill for resource consumption will be generated on the 3rd day of the upcoming month. Prior to this date, the expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. For more details, see User Guide of Current Bills.

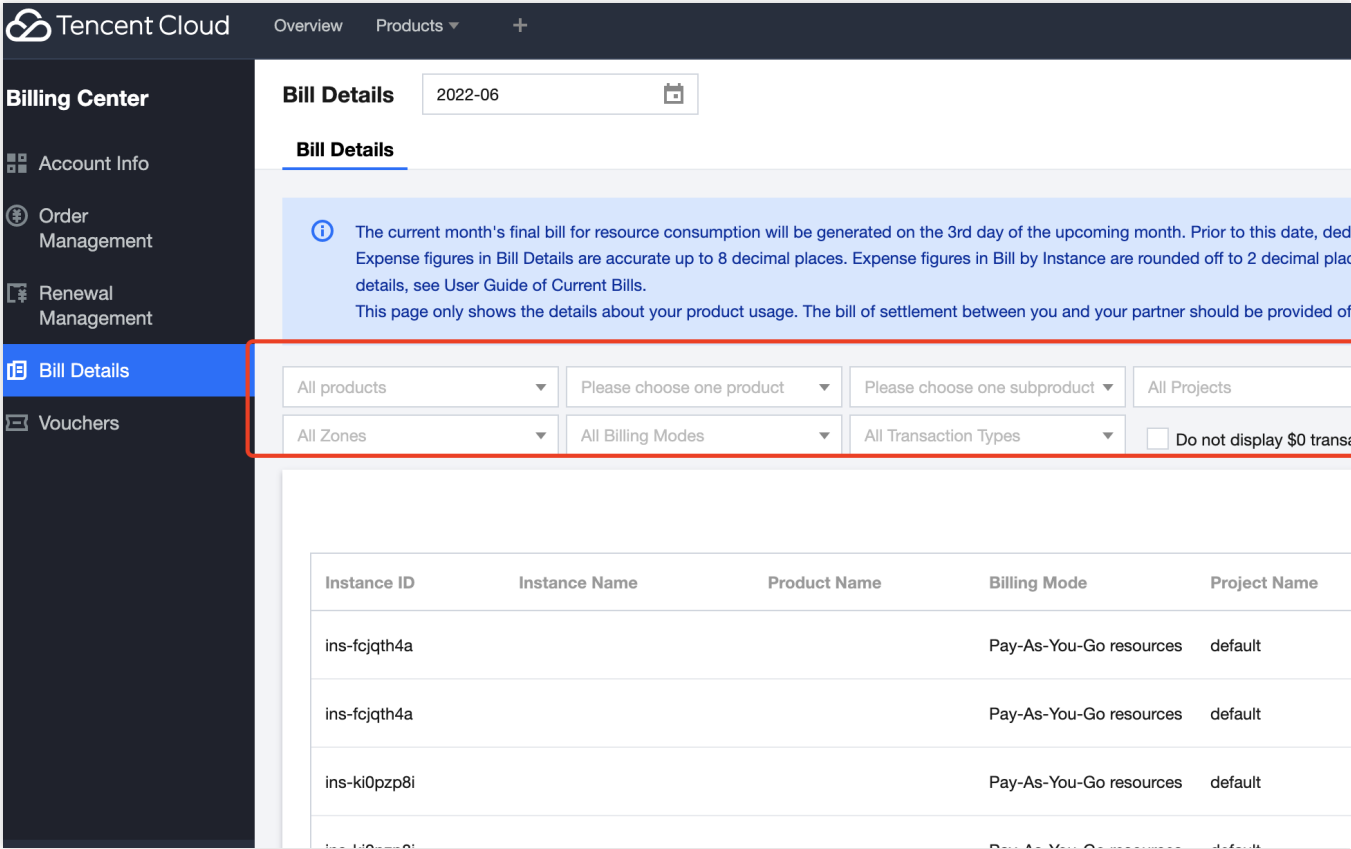
This page only shows the details about your product usage. The bill of settlement between you and your partner should be provided on the 3rd day of the upcoming month.

第三步：筛选区域可以根据不同的产品、项目、地域等进行账单内容筛选。

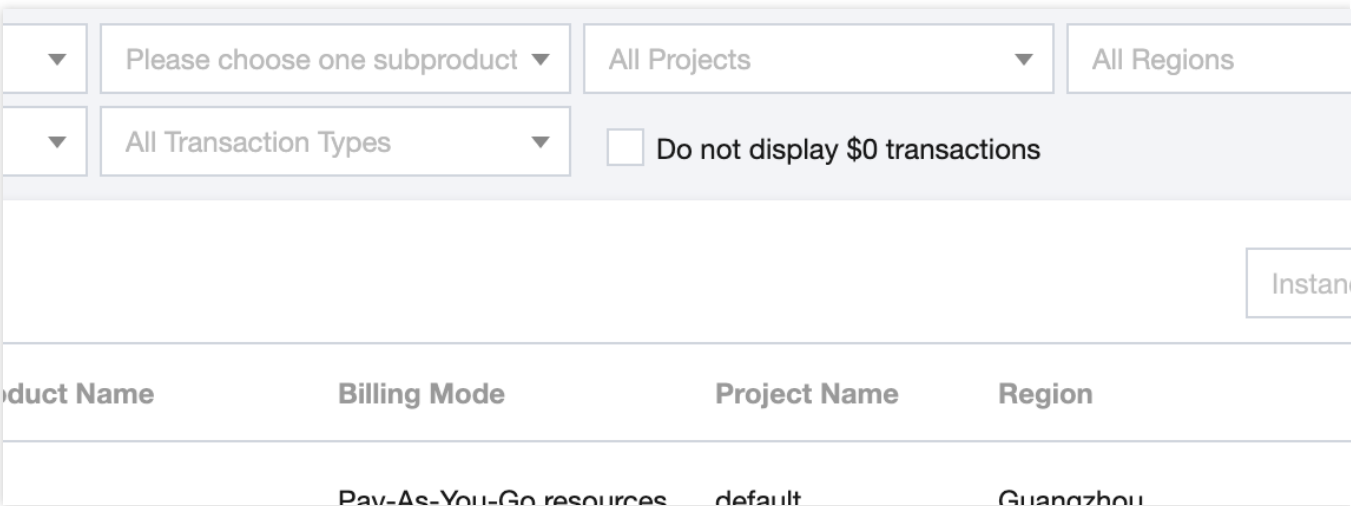
版权所有：腾讯云计算（北京）有限责任公司

第396 共442页





第四步：子客可点击列表上方“设置”按钮进行列表界面字段显示设置。



Custom Field Settings

<input checked="" type="checkbox"/> Instance ID	<input checked="" type="checkbox"/> Availability Zone	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Instance Name	<input checked="" type="checkbox"/> Subproduct Name	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Transaction Type	<input checked="" type="checkbox"/>
<input type="checkbox"/> Payer Account ID	<input checked="" type="checkbox"/> Transaction ID	<input checked="" type="checkbox"/>
<input type="checkbox"/> Owner Account ID	<input checked="" type="checkbox"/> Transaction Time	<input checked="" type="checkbox"/>
<input type="checkbox"/> Operator Account ID	<input checked="" type="checkbox"/> Usage Start Time	
<input checked="" type="checkbox"/> Billing Mode	<input checked="" type="checkbox"/> Usage End Time	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Project Name	<input checked="" type="checkbox"/> Component Type	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Region	<input checked="" type="checkbox"/> Component Name	<input checked="" type="checkbox"/>
		<input checked="" type="checkbox"/>

OK

Cancel

# 账单详情

最近更新时间：2022-11-23 11:39:32

## 账单详情

字段名称	字段说明
Instance ID	实例ID，可以在各产品控制台查看
Instance Name	资源别名，由用户为资源自助设置，未设置则为空
Product Name	云产品大类，产品四层的第1层，如云服务器CVM、云数据库MySQL
Payer Account ID	支付者账号ID，用户在腾讯云的唯一账号标识，此处是经销商的ID
Owner Account ID	资源归属者账号ID，此处是子客的ID
Operator Account ID	操作者账号ID，下单购买或开通产品的用户，此处是子客的ID
Reseller Account ID	管理者账号ID，为资源归属者的直接管理经销商ID。
Billing Mode	资源的计费模式，包年包月或按量计费
Project Name	资源所属项目，由用户为资源自助分配，未分配则为默认项目
Region	资源所属地域，如华南地区（广州）
Availability Zone	资源所属可用区，如广州三区
Subproduct Name	云产品子类，产品四层的第2层，如云服务器CVM-标准型S1
Transaction Type	资源的购买、开通、续费、退费等交易行为，具体枚举值可参见页面下方《关键字段枚举值说明》
Transaction ID	交易唯一标识
Transaction Time	资源扣费时间
Usage Start Time	资源开始使用时间
Usage End Time	资源结束使用时间
Component Type	组件类型的名称，产品四层的第3层，如CPU、内存、带宽、系统盘等
Component Name	组件的名称，产品四层的第4层，如内存-标准型S2、高性能云硬盘-存储空间等
Component List Price	组件的官网原始单价

字段名称	字段说明
Component Price Measurement Unit	组件刊例价对应的价格单位
Component Usage	组件的用量
Component Usage Unit	组件用量对应的单位
Usage Duration	资源使用的时长
Duration Unit	资源使用的时长单位
Reserved Instances	用量匹配到的RI ID，比如：s2-RI-1234567890
Original Cost	资源的原始总价，等于刊例价 * 用量 * 时长
Currency	组件结算使用的货币种类，此处是美元

字段名称	字段说明
Transaction Type	枚举值如下： Purchase Renewal Modify Refund Deduction Hourly settlement Daily settlement Monthly settlement Offline project deduction Offline deduction adjust-CR adjust-DR One-off RI Fee Spot Hourly RI fee New monthly subscription Monthly subscription renewal Monthly subscription specification adjustment Monthly subscription specification adjustment Monthly subscription refund

# 下载账单

最近更新时间：2022-07-08 17:22:35

## 账单下载

子客可在账单界面列表右上方点击下载按钮对月账单进行全量下载。

注意：

- 由于当月账单实时变化，暂时不提供下载功能。
- 历史月账单下载时会下载该月全量、全字段数据（界面筛选及定制字段不对下载有影响）。

Tencent Cloud

OverviewProducts+28

TicketBilling CenterEnglish

Billing Center

Account Info

Order Management

Renewal Management

Billing Details

Vouchers

Bill Details2022-06

Bill Details

The current month's final bill for resource consumption will be generated on the 3rd day of the upcoming month. Prior to this date, deductions are not final and are for reference purposes only. Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more details, see User Guide of Current Bills. This page only shows the details about your product usage. The bill of settlement between you and your partner should be provided offline by your partner, which is currently unavailable on the page.

All productsPlease choose one productPlease choose one subproductAll ProjectsAll Regions

All ZonesAll Billing ModesAll Transaction Types

☐ Do not display \$0 transactions

Instance ID/Instance Name

☆

Download

Instance ID	Instance Name	Product Name	Billing Mode	Project Name	Region	Availability Zone	Subproduct
eip-ebxja2li		Cloud Public IP	Pay-As-You-Go resources	default	Guangzhou	unknown zone	
ins-ki0pzp8i		Cloud Virtual Machine(CVM)	Pay-As-You-Go resources	default	Guangzhou	Guangzhou Zon...	CVM Stan...
ins-fcjqth4a		Cloud Virtual Machine(CVM)	Pay-As-You-Go resources	default	Guangzhou	Guangzhou Zon...	CVM Stan...
ins-1l8p8n6		Cloud Virtual	Pay-As-You-Go resources	default	Guangzhou	Guangzhou Zon...	CVM Stan...

版权所有：腾讯云计算（北京）有限责任公司

第401 共442页

# 续费管理

最近更新时间：2022-07-11 19:15:17

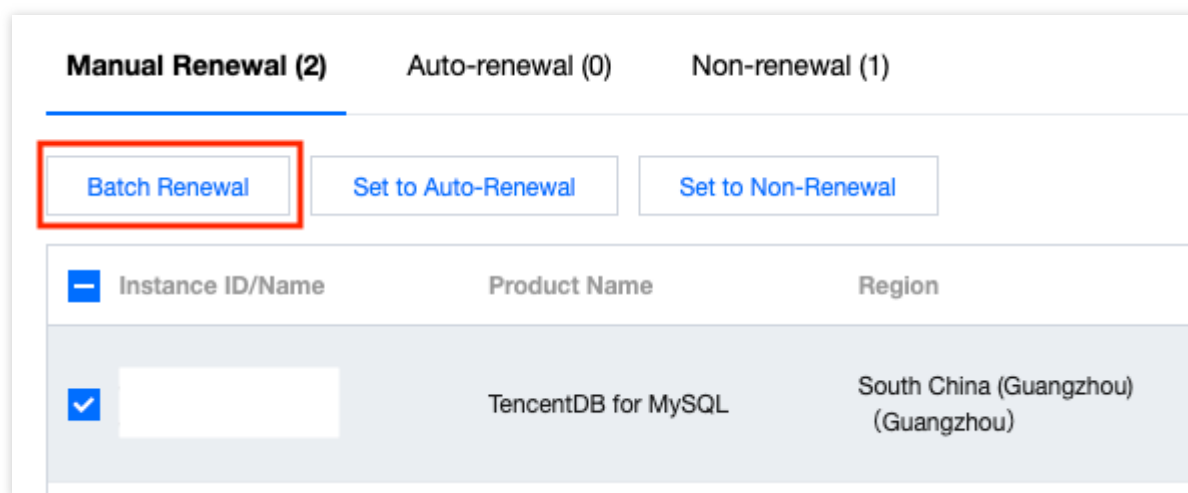
## 续费管理

子客可以对自己的包年包月的资源进行续费。

### 操作步骤

- 1、使用经销商账号登录腾讯云；
- 2、进入菜单Billing Center -> Renewal；
- 3、选中资源，即可对资源进行续费操作。为了方便子客对资源的查找，子客可以根据到期时间范围、产品类别、地域等对资源进行筛选。
- 4、批量资源续费

- 勾选需要续费的资源，单击批量续费，即可对资源进行续费。



- 当您的资源较多时，您可以跨页选中全部资源，批量提交续费。

### 5、自动续费

如果您打算长期使用资源，您可以将资源设置自动续费。已设置自动续费的资源，即可在自动续费项进行管理。

**Manual Renewal (2)**    Auto-renewal (0)    Non-renewal (1)

Batch Renewal

Set to Auto-Renewal

Set to Non-Renewal

<input type="checkbox"/>	Instance ID/Name	Product Name	Region
<input checked="" type="checkbox"/>		TencentDB for MySQL	South China (Guangzhou) (Guangzhou)

- 已设置自动续费的资源，我们会在到期当日为您进行续费。续费时刻可能会超过您的资源到期时刻，但保证在到期当日。请尽量不在资源临近到期/回收时调整自动续费标识。
- 到期当日，若您的账户可用余额不足以进行资源的自动续费，我们会在到期后至停服前，每天进行一次扫描，只要您的账户可用余额充足，我们会马上为您标记自动续费的资源进行续费操作。
- 已停服的资源不会执行自动续费，也不会展示在续费管理页中。
- 已设置自动续费的资源也可以取消自动续费。取消了自动续费的资源，我们将恢复对其正常的到期检查与提醒。

## 6、到期不续费

如果您的资源到期后不再继续使用，您可以将资源设置到期不续费。已设置到期不续费的资源，可以在到期不续费项里管理。

**Manual Renewal (2)**    Auto-renewal (0)    Non-renewal (1)

Batch Renewal

Set to Auto-Renewal

Set to Non-Renewal

<input type="checkbox"/>	Instance ID/Name	Product Name	Region
<input checked="" type="checkbox"/>		TencentDB for MySQL	South China (Guangzhou) (Guangzhou)

- 对您到期不续的资源，我们不会发送任何到期提醒。
- 到期不续的资源，您可以恢复为手动续费或自动续费。恢复后，我们会恢复对其正常的到期检查及短信、邮件的提醒。

## 7、续费提醒

如果您的资源预算需要较长的时间来申请，我们支持您对续费提醒进行时间上的自定义设置。

- 您可以对即将到期的资源和设置了自动续费的资源设置提前7天 - 3个月的提醒。
- 当资源即将到期、账户可用余额不够为自动续费的资源续费时，平台提供站内信、短信、邮件三种通知渠道，您可以选择全部或部分通知渠道。
- 当您取消全部通知渠道时，我们不会为您发送通知。
- 这些设置只对您当前登录的账号 ID有效，不影响其他协作者。
- 如果您希望修改接收提醒的短信和邮件，您可以前往 [用户管理](#) 页面进行修改。



# 协议管理

## 业务相关

# TENCENT CLOUD RESELLER CUSTOMER TERMS OF SERVICE

最近更新时间：2024-03-04 14:23:52

Updated 2024-02-06

Welcome, and thank you for your interest in Tencent Cloud services. The Tencent Cloud services, their related websites, networks, applications, software and other services and related documentation provided by Tencent are collectively referred to as the **“Tencent Services”**. These Terms of Service are a legally binding contract between you and Tencent in connection with the Tencent Services that are offered to you by a Tencent Cloud authorized distributor or reseller partner (**“Tencent Cloud Partner”**) or an authorized reseller of a Tencent Cloud Partner (**“Second-Level Reseller”**), and from whom you purchased a subscription to such Tencent Services (**“Services”**) and your use of the Services. If you purchased Tencent Services directly from Tencent, these Terms of Service are not applicable to you and you are subject to the Tencent Cloud Terms of Service instead. If you were previously a direct customer of Tencent Services and have now decided to purchase subscriptions to Tencent Services from a Tencent Cloud Partner or Second-Level Reseller instead, these Terms of Service shall apply to you and supersede the Tencent Cloud Terms of Services with immediate effect. For the purposes of these Terms of Service, **“Tencent,” “we,” “our,”** and **“us”** refer to the applicable Tencent contracting entity set forth in Section 3. **“Affiliate”** or **“Affiliates”** means any entity that directly or indirectly Controls, is Controlled by, or is directly or indirectly under common Control with a party, where **“Control”** means control of greater than fifty percent of the voting rights or equity interests of a party or by way of contract, management agreement, voting trust, or otherwise.

### PLEASE READ THE FOLLOWING TERMS CAREFULLY.

**BY CLICKING “I ACCEPT”, PURCHASING THE SERVICES FROM OUR AUTHORIZED PARTNER AND/OR REGISTERING A TENCENT CLOUD ACCOUNT TO ACCESS AND USE THE SERVICES, YOU AGREE THAT YOU HAVE READ AND UNDERSTOOD, AND, AS A CONDITION TO YOUR USE OF THE SERVICES, YOU AGREE TO BE BOUND BY, THE FOLLOWING TERMS AND CONDITIONS, INCLUDING the then-current additional terms applicable to the Services posted online here, including the Privacy Policy, Data Processing and Security Agreement, Acceptable Use Policy, Copyright Policy, the PRC Service Region Terms, the North America Terms, the EEA Consumer Terms, the Germany Terms, the South Korea Terms, any Service-specific terms, and the Service Level Agreement and any other region-specific terms (collectively, **“Additional Terms,”** and together with these Terms of Service, the **“Terms”**).** The Additional Terms do not include the Privacy Policy or the Cookies Policy

(both of which are also available here). Please see our Privacy Policy or the Cookies Policy and Data Processing and Security Agreement for further information regarding our use of your Personal Data (as defined in the Data Processing and Security Agreement) submitted to or via the Services. If you are not eligible, or do not agree to the Terms, then you do not have Tencent's permission to use the Services. YOUR USE OF THE SERVICES, AND TENCENT'S PROVISION OF THE SERVICES TO YOU, CONSTITUTES AN AGREEMENT BY TENCENT AND BY YOU TO BE BOUND BY THESE TERMS.

**1.THE SERVICES AND APPLICATIONS.** The Services subscriptions that you purchase are those specified in the purchase order or purchase agreement between you and the Tencent Cloud Partner or Second-Level Reseller (as the case may be) and the Services may be further described at <http://www.tencentcloud.com>, and include: (a) the documentation for the Services (as may be updated from time to time) in the form generally made available by Tencent to its customers for use with the Services; (b) the APIs, mobile applications, and Software provided by Tencent in connection with the Services; and (c) any additional subscriptions to the Services purchased by you. The Services may allow you to create applications using the Services or run applications on the Services, including any source code written by you to be used with the Services or otherwise hosted on Tencent Cloud ("**Applications**").

**2.ELIGIBILITY.** You must be at least 14 years old to use the Services. By agreeing to these Terms, you represent and warrant to us that: (a) you are at least 14 years old; (b) you have not previously been suspended or removed from the Services; and (c) your registration and your use of the Services is in compliance with any and all applicable laws and regulations. If you are an entity, organization, or company, the individual accepting these Terms on your behalf represents and warrants that they have authority to bind you to these Terms and you agree to be bound by these Terms.

### 3. CONTRACTING ENTITY; GOVERNING LAW

(a)The country specified in your registered billing information determines: (i) the Tencent entity with which you are contracting under these Terms and (ii) the governing law that applies to these Terms and your use of the Services, as set forth in the table below. Notwithstanding anything to the contrary under these Terms, you acknowledge and agree that Services may be provided by one of our Affiliates to the extent deemed appropriate by us, for example, where required to comply with applicable laws and regulations or in accordance with Tencent's internal structuring of its operations in the applicable region. In particular, when the Services are provided in the PRC region, you acknowledge and agree that, in compliance with applicable PRC laws and regulations, the Services will be provided by Tencent Cloud Computing (Beijing) Co., Ltd.. "**PRC**" means the People's Republic of China, and for the purpose of these Terms only, does not include the Hong Kong Special Administrative Region, Macau Special Administrative Region, and Taiwan.

Your Location	Tencent Contracting Entity	Governing Law
European Economic Area, Switzerland and UK	Tencent Cloud Europe B.V., a Dutch registered company located at Buitenveldertselaan 1-5, 1082 VA, Amsterdam, the Netherlands	England and Wales
North America	Tencent Cloud LLC, a Delaware registered company located at	California,

	Claremont 2747 Park Blvd, Palo Alto, CA 94306.	USA
South Korea	Tencent Korea Yuhan Hoesa, 152, Taeheran-ro, Gangnam-gu (Gangnam Finance Center, Yeoksam-dong), Seoul, Korea	Singapore
Rest of the world	Tencent Cloud International Pte. Ltd, a Singapore-registered company located at 10 Anson Road, #21-07, International Plaza, Singapore 079903.	Singapore

(b) The country specified in your registered billing information with Tencent Cloud Partner or Second-Level Reseller may cause additional or different terms to apply as follows. For example, if your use of the Services is subject to consumer protections as determined under applicable laws, additional terms apply, as set forth in the EEA Consumer Terms, the Germany Terms, South Korea Terms and other region specific terms. If the country specified in your registered billing information with Tencent Cloud Partner or Second-Level Reseller is in North America, you shall be subject to the North America Terms below. If you wish to use the Services in the PRC region, you shall be subject to the terms of the PRC Service Region Terms. In addition to the above, additional or different terms may apply to your use based on applicable local laws.

#### 4. USE OF SERVICES

(a) Accounts and Registration. You are required to register a Tencent Cloud account authorized to access the Services (“**Account**”) before you can access the Services. When you register for an Account, you may be required to provide us with some information, such as your name, postal address, email address, and/or other contact information. You agree that the information you provide to us is accurate and that you will keep it accurate and up-to-date at all times. Where the option is available, you may also register for an Account through a third party platform account. You agree that you shall additionally comply with any applicable terms and conditions of that third party platform. We may deny you the right to create an account. You are responsible for safeguarding any and all Account details and access credentials, and you shall be responsible for any use of the Account or Services and all activities that occur under your Account, regardless of whether the activities are authorized or undertaken by you, your employees or a third party (including your contractors, agents and/or End Users), and including in circumstances due to your failure to properly safeguard such Account details and access credentials. Except to the extent caused by our breach of these Terms, Tencent and its Affiliates are not responsible for any unauthorized access to your account. Any breach of these Terms or any use of your Account by anyone will be treated as if the breach or use had been carried out by you, and will not relieve you of your obligations to us.

(b) End Users Access and License. Any entities or individuals that access the Services under your Account or an Application are referred to in these Terms as “**End Users**.” You shall and shall ensure that your authorized End Users may access and use the Services in accordance with these Terms during the Term (defined below in Section 9). Such Services shall be provided during the Term. You and your authorized End Users shall only access the Services via your Account and the use of any Services shall be subject to these Terms. If you become aware of any unauthorized use of your Account or the password for your Account, you will notify Tencent immediately. If you are an entity, organization, or company, you will ensure your employees and contractors to access the Services through your

Account. You are responsible for safeguarding any and all Account details and access credentials. Any breach of these Terms or any use of your Account by anyone to whom you disclose your username or password will be treated as if the breach or use had been carried out by you, and will not relieve you of your obligations to us. Tencent may provide downloadable tools, software development kits, sample code, APIs, or other computer software including those provided in connection with the Services or with the use of your Account (and any periodic updates thereto from time to time) ("**Software**"). You acknowledge that Tencent or its licensors own all rights, titles and interest in and to the Services and the Software. Subject to your and your authorized End Users' compliance with these Terms, Tencent grants, or shall procure the grant, to you and your authorized End Users a limited, non-exclusive, non-transferable, non-sublicensable and revocable license to use the Software in a manner not exceeding any applicable usage limitation or term, and within the designated territory for use or receipt of Services, and only in connection with the Services. To the extent that any Software comes with an end user license agreement, terms of service or other similar agreement governing the use of such Software, you agree that you will strictly comply with such agreement. Other than as specified in the foregoing, no other rights are granted to you under these Terms to use the Services (including any Software offered in connection therewith).

(c) Service Regions. Certain Services allow you to select a geographically defined service region in which User Data (as defined below) is stored in order to provide the Services (a "**Service Region**"). Where a Service Region applies, Tencent will, upon your request, store User Data in the Service Region you select when User Data is being used for the provision of those Services. If your selected Service Region is the PRC, then the PRC Service Region Terms below apply with respect to those Services for which the PRC is the selected Service Region.

(d) Suspension of Services. If you become aware or reasonably suspect that any Application (including an End User's use of an Application) or User Data violates these Terms, including the Additional Terms, you will immediately suspend the Application, remove the User Data, and suspend access by End Users. If you fail to take such action after Tencent sends notice of any violation, Tencent may suspend or disable the Application and disable your Account until that violation is remediated to Tencent's satisfaction. In the event that Tencent determines that a violation could: (a) disrupt the Services; (b) disrupt use of the Services by a third party; (c) disrupt the Tencent network or servers used to provide the Services; or (d) allow unauthorized third party access to the Services, then Tencent or its Affiliates may immediately without prior notice to you, suspend your Account or the offending Application or End User account, to the minimum extent required to prevent or resolve that violation. "**Affiliate**" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party, where "Control" means control of greater than fifty percent of the voting rights or equity interests of a party or by way of contract, management agreement, voting trust, or otherwise.

(e) Service Modifications or Discontinuation. Tencent may discontinue or make any changes to the Services (or any part thereof) at any time without incurring liability to you. Tencent may choose to, without limitation, discontinue, limit, restrict, change or remove the Services, any Service component, or availability of the Services (or any portion or component thereof) in any specific Service Region, territory or industry sector or field of business. If Tencent discontinues or makes any changes to the Services that would materially decrease the functionality of those Services, Tencent will use commercially reasonable efforts to inform you of the change with reasonable advance notice before it goes into effect, provided that you have subscribed to be informed about those changes. Tencent may make the

change, and will not be obligated to provide notice, if the discontinuation or change is necessary to address an emergency or threat to the security or integrity of the Services or Tencent, comply with or respond to litigation, address Intellectual Property Rights concerns, or comply with the law or government requests. Tencent may provide periodic updates to the Software or Services provided by Tencent from time to time (“**Updates**”). Tencent may also make new features or functionality available from time to time through the Services and add new services to the Services from time to time (by adding them at the URL set forth under that definition), the use of which may be contingent upon your agreement to additional requirements.

(f) Security and Privacy. Tencent’s security and privacy practices are available in the Additional Terms, the Privacy Policy and the Cookies Policy. You shall configure and use the Services in a way that meets your security requirements.

(g) Third Party Applications. You are solely responsible for any software, tools or applications used by you in connection with your use of the Services (“**Third Party Software**”), including third party software made available or offered in connection with the Services. Tencent is not responsible for and is not liable for any damages or losses arising from the use of the Third Party Software, and Tencent does not endorse, support or guarantee the quality, reliability, or suitability of any Third Party Software. You agree that the use and making available of any Third Party Software is at your own risk. You shall comply with and ensure that your End Users will comply with any terms and conditions applicable to Third Party Software. Tencent does not provide any technical support for any Third Party Software. Please contact the relevant supplying third party for technical support.

(h) Access to Your Device. In order for Tencent to provide the Services, Tencent may require access to and use of a device you own or control. For example, Tencent may need to access a device's processor and storage to complete a Software installation. Tencent may provide further information regarding how Tencent Cloud accesses the relevant device within Tencent Cloud. You agree to facilitate and/or give Tencent access to the device for these purposes, and you acknowledge that if you do not provide access, Tencent may not be able to provide you with the Services (or certain features within the Services). You acknowledge that Tencent may use or access Personal Data within the device in the course of providing Tencent Cloud, as set out further in the Privacy Policy. To the extent the Data Processing and Security Agreement applies to the use or access of that Personal Data, you agree that Tencent may use or access that Personal Data in accordance with the Data Processing and Security Agreement.

## 5. FEES AND PAYMENTS

(a) All fees and payments in relation to your use of the Services (“**Fees**”) are subject to the agreement between you and the Tencent Cloud Partner or Second-Level Reseller with whom you entered into for the subscription to the Services. You agree that you are solely responsible for payment of all Fees and all taxes associated with any such payments.

(b) Any dispute in relation to the invoiced Fees for the Services is solely a matter to be resolved between you and the Tencent Cloud Partner or Second-Level Reseller with whom you have entered into agreement. You hereby agree Tencent may provide information relating to your use of the Services to either party upon request to help resolve any dispute in relation to the invoiced Fees.

## 6. TECHNICAL SUPPORT AND SERVICE LEVELS

- (a) SLAs. Tencent will use commercially reasonable efforts to provide any related Services in accordance with the relevant and then-current services level agreement(s) ("SLA"), if any, set forth in the Additional Terms. The parties acknowledge and agree that, regardless of anything to the contrary in these Terms, your sole and exclusive remedy for a breach of an SLA is the receipt of any applicable service credits as set forth and pursuant to the applicable SLA.
- (b) Support for Services. Except to the extent required by applicable laws with respect to consumers, Tencent is under no obligation to provide technical support or other services unless you have purchased Tencent Cloud support services as part of the subscription. You acknowledge and agree that technical support or other services may require you to pay additional costs and other fees.
- (c) Support for Applications. You are responsible for the operation, integration and technical support of your Applications.

## 7. YOUR OBLIGATIONS

- (a) Compliance. You are solely responsible for your Applications and User Data and for making sure your Applications and User Data comply with these Terms (including the Additional Terms) and that use of the same in connection with the Services complies with applicable laws.. Tencent reserves the right to review all Applications to ensure your compliance with these Terms. You acknowledge and agree that you are responsible for all use of the Services by End Users, End Users' access to Applications and User Data, activities under Accounts, and for otherwise ensuring that each End User complies with these Terms.
- (b) Privacy. You acknowledge and agree that you are solely responsible for the processing of any Personal Data in respect of End Users and any persons whose Personal Data is contained in the User Data, and shall protect the privacy of the End Users and such persons, and shall comply with all applicable laws and regulations in respect of the same (including by making such disclosures, and obtaining such consents, as are necessary to ensure the Personal Data of End Users or any persons whose Personal Data is contained in User Data may be processed by the Services). You shall be solely responsible for any access, monitoring, use, or disclosure of Personal Data submitted by End Users through the Services. To the extent any Personal Data is contained in any User Data, the parties agree that the processing of such Personal Data shall be undertaken in accordance with the Data Processing and Security Agreement. You agree that you shall not make available any User Data for processing in the Services unless lawfully permitted to do so.
- (c) Restrictions. You will not, and will not allow your Affiliates, employees, and contractors and any third parties under your control, management, supervision, or otherwise to: (a) copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any or all of the source code of the Services (except to the extent such a restriction is expressly prohibited by applicable law, and where you are permitted by law to so reverse engineer, you will contact Tencent to obtain the desired information prior to such reverse engineering); (b) use the Services for the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage; (c) use the Services as benchmarking or in any manner that is competitive with the Services; (d) sublicense, resell, or distribute any or all of the Services separate from any integrated Application; or (e) access the Services in a manner intended to avoid incurring Fees or otherwise avoiding usage limitations. To the extent you choose a Service Region that includes the United States, you will not, and will not allow your Affiliates, employees, and contractors and any third parties under your control, management, supervision, or otherwise to: (a) process or store any User Data that is



subject to the International Traffic in Arms Regulations maintained by the United States Department of State; and/or (b) process or store any User Data that is subject to the Health Insurance Portability and Accountability Act of 1996 as it may be amended from time to time, or any regulations issued under it.

## 8. INTELLECTUAL PROPERTY RIGHTS AND USER DATA

(a) Tencent Cloud Intellectual Property Rights. You agree that all Intellectual Property Rights in and to the Services, as between you and Tencent, will be owned by Tencent, or Tencent's licensors, as the case may be. Except as expressly set forth in these Terms and to the extent permissible under applicable law, Tencent does not grant to you any licenses or other rights, implied or otherwise, in or to Tencent's Intellectual Property Rights. "**Intellectual Property Rights**" means all current and future worldwide rights under patent, copyright, trade secret, trademark, or moral rights laws, and other similar rights.

(b) Tencent Confidential Information. "**Tencent Confidential Information**" means information that Tencent (or an Affiliate) discloses to you under these Terms, and that is marked as confidential or should reasonably be considered confidential based on the nature of the information and the circumstances of its disclosure. You will not disclose the Tencent Confidential Information except to those of your Affiliates, employees, and contractors who need to know the Tencent Confidential Information for the purposes of exercising your rights and performing your obligations under these Terms, and who have agreed in writing to confidentiality obligations that are at least as protective as these Terms. You will, and will take appropriate measures to ensure that your Affiliates, employees, and contractors: (a) take at least reasonable care to protect the confidentiality of the Tencent Confidential Information; and (b) do not use the Tencent Confidential Information for any purpose other than to exercise your rights and perform your obligations under these Terms. However, you may also disclose Tencent Confidential Information to the extent required by applicable laws, regulations, or government orders; provided that you use commercially reasonable efforts, if legally permitted, to: (i) promptly notify Tencent of those disclosure requirements before disclosing the Tencent Confidential Information; and (ii) provide to Tencent any information reasonably requested to assist Tencent in seeking a protective order or other confidential treatment for that Tencent Confidential Information.

(c) Feedback. If you provide Tencent or its Affiliates with any suggestions, ideas, comments, or other feedback about the Services ("**Feedback**"), Tencent and its Affiliates may use and otherwise exploit that Feedback without restriction and without obligation to you; provided, however, Tencent will not publicly disclose Feedback in a way that is identifiable to you

(d) User Data.

(i) "**User Data**" means any data, information, media or other content submitted by you or on behalf of you or your End Users to the Services, including but not limited to any Personal Data, but excluding any data provided to Tencent or its Affiliates as part of your general Account. (ii) Tencent will access and process User Data only in connection with the provision of the Services and otherwise in accordance with these Terms and as described in our Privacy Policy. You hereby grant to Tencent a non-exclusive, sublicensable license to access, copy, and use User Data to provide the Services, and/or otherwise use such User Data in accordance with these Terms.

(iii) You acknowledge and agree that Tencent may disclose User Data to third parties with or without notice to you: (1) to comply with applicable laws or protect Tencent's rights; or (2) to comply with court orders, a lawful government or law enforcement request, or other legal processes. Tencent may also block or remove User Data as required by

applicable laws, in which case Tencent will make reasonable commercial efforts to promptly notify you if legally permissible.

(iv) You are solely responsible for maintaining and backing up User Data. You represent and warrant that: (1) you have all rights required to provide User Data to Tencent, for Tencent to use the User Data as provided for in these Terms and for you to use in connection with your use of the Services; and (2) User Data, and your use of User Data through the Services does not violate any laws or rights of any person. You retain any Intellectual Property Rights you may have in User Data.

## 9 TERM AND TERMINATION; SUSPENSION

(a) Term. These Terms will commence when you accept these Terms or first download, install, access, or use the Services and continue (in respect of each Service which you purchase a subscription from Tencent Cloud Partner or Second-Level Reseller) for the corresponding effective term period specified in your agreement with Tencent Cloud Partner or Second-Level Reseller for such subscription to the Service, or otherwise earlier terminated in accordance with this Section 9 (“**Term**”).

(b) Suspension and/or Termination by Tencent. To the extent permitted under applicable law, Tencent may, at its sole discretion, terminate these Terms, or suspend or terminate your access to the Services or any aspect of the Services, immediately upon written notice to you if:

- (i) you violate any provisions of these Terms;
- (ii) you have not paid any Fees or other amounts owed by you to Tencent Cloud Partner or Second-Level Reseller within 30 days after the applicable due date, or the credit balance allocated by Tencent Cloud Partner or Second-Level Reseller in relation to your Tencent Cloud account falls to 0 (zero) or below;
- (iii) Tencent reasonably believes that you or an End User have violated any applicable laws, or engaged in any fraudulent or deceptive activity, in connection with the use of the Services;
- (iv) you enter into liquidation, administrative receivership, bankruptcy or make any voluntary agreement with your creditors or are unable to pay your debts as they fall due;
- (v) your credit balance allocated by Tencent Cloud Partner or Second-Level Reseller in relation to your Tencent Cloud account falls to 0 (zero) or below;
- (vi) the Tencent Cloud Partner or Second-Level Reseller reselling the Services and associated with your Tencent Cloud account may be in breach of the distributor agreement or reseller agreement (as the case may be);
- (vii) Tencent is required to by applicable laws, court orders or requirements imposed by government bodies, or if Tencent otherwise determines that it is reasonable to do so in order to ensure that Tencent does not violate or risk violation of the same; or
- (viii) any current or future regulatory or other requirement (1) subjects Tencent to an obligation not generally applicable to businesses operating in a Service Region; (2) would result in difficulty for Tencent to continue offering the affected Service(s); or (3) Tencent reasonably believes may conflict with these Terms or the Services.

(c) Termination by you. You may terminate your Account and these Terms at any time by following the instructions provided within the Services. Except as set forth in any region-specific terms or Service-specific terms, if you terminate your Account and these Terms, you are not entitled to a refund of any Fees paid to Tencent Cloud Partner or Second-Level Reseller.



(d) Termination by Tencent Cloud Partner or Second-Level Reseller. If your subscription to the Services is terminated by the Tencent Cloud Partner or Second-Level Reseller, your access and use of the corresponding Services will also be terminated at the same time. However, you can continue to use the Services beyond the termination date provided that you forthwith purchase a new subscription to the Services through another Tencent Cloud Partner or Second-Level Reseller or you purchase the Services directly from Tencent, and for either cases, you will be required to enter into an applicable agreement with the Tencent Cloud Partner or Second-Level Reseller or with Tencent (as the case may be).

(e) No Liability for Termination. Except as expressly required by law, if either party terminates these Terms in accordance with the foregoing, neither party will be liable to the other because of the termination, for expenditures or commitments made in connection with these Terms or damages caused by the loss of prospective profits or anticipated sales. Termination will not, however, relieve either party of obligations incurred prior to the effective date of the termination.

(f) Effects of Suspension. If Tencent restricts or suspends your access to any or all of the Services, or otherwise modifies the Services under these Terms: (i) where Services are suspended, you remain responsible for all Fees accrued through the date of suspension (including where the charges were incurred before suspension date but performance of the relevant obligations were after the suspension date); (ii) you remain responsible for any applicable charges for any part of the Services (including any modified parts thereto) to which you have access; and (iii) you will not be entitled to any service credits under any applicable SLA for any period of suspension, modification or restriction.

(g) Effects of Termination.

(i) Upon termination or expiration of these Terms: (1) you will pay Tencent Cloud Partner or Second-Level Resellers any Fees or other amounts owed under these Terms within 30 days of termination or expiration, (2) you will delete the Software and remove from the Services any Application and User Data; (3) your rights under these Terms shall immediately cease; and (4) upon Tencent's request, you will use commercially reasonable efforts to return or destroy all Tencent Confidential Information; and (4) all User Data will be deleted from the Services. Tencent has no obligation to make accessible to you any User Data after the termination of these Terms.

(ii) In addition, the following provisions will survive any termination of these Terms: Sections 1, 3, 5, 7, 8, 9(d), 9(e), 9(f), 9(g), 10 to 13.

## **10.DISCLAIMER**

Disclaimer of Warranties. TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAWS, THE SERVICE AND SOFTWARE ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, AND NEITHER TENCENT NOR ANY OF ITS LICENSORS OR AFFILIATES, PROVIDERS OR DISTRIBUTORS, MAKE, AND TENCENT HEREBY DISCLAIMS ON BEHALF OF ITSELF AND SUCH PERSONS, ANY REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, REGARDING THE TENCENT CLOUD, ANY OTHER SOFTWARE OR SERVICES, OR ANY MEDIA OR OTHER CONTENT SUBMITTED, UPLOADED, STORED, TRANSMITTED OR DISPLAYED BY OR THROUGH THE SERVICES, INCLUDING ANY REPRESENTATION, WARRANTY OR UNDERTAKING:

- (a) THAT THE SERVICES OR SOFTWARE WILL BE UNINTERRUPTED, SECURE, OR ERROR-FREE OR FREE FROM VIRUSES OR OTHER HARMFUL COMPONENTS;
- (b) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE;
- (c) THAT USER DATA WILL NOT BE SUBJECT TO LOSS OR DAMAGE;
- (d) OF NON-INFRINGEMENT;
- (e) THAT THE SERVICES OR SOFTWARE WILL BE SECURE OR COMPATIBLE WITH YOUR OR YOUR END USERS' NETWORKS, SYSTEMS, APPLICATIONS, HARDWARE, OR DEVICES; OR
- (f) THAT THE SERVICES WILL BE OF MERCHANTABLE OR SATISFACTORY QUALITY OR FIT FOR ANY PARTICULAR PURPOSE. FOR THE AVOIDANCE OF DOUBT, THE SERVICES ARE NOT DESIGNED OR INTENDED FOR HIGH RISK ACTIVITIES.

#### **11.LIMITATION OF LIABILITY; INDEMNIFICATION**

(a) Cap on Liability. SUBJECT TO SECTION 11(C) BELOW, TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAWS, THE TOTAL AGGREGATE LIABILITY OF TENCENT AND ITS AFFILIATES, ON THE ONE HAND, AND YOU ON THE OTHER, FOR ALL CLAIMS ARISING IN CONNECTION WITH THESE TERMS, THE SERVICES, AND THE SOFTWARE, UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, AND EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE, WILL BE LIMITED TO THE TOTAL FEES THAT YOU HAVE PAID TO TENCENT CLOUD PARTNER OR SECOND-LEVEL RESELLER IN CONNECTION WITH YOUR USE OF THE SERVICES PURSUANT TO THESE TERMS IN THE 12 MONTHS IMMEDIATELY PRECEDING THE DATE THAT EVENT GIVING RISE TO THE LIABILITY FIRST OCCURRED. HOWEVER, NOTHING LIMITS OR EXCLUDES EITHER PARTY'S LIABILITY FOR ANY MATTERS FOR WHICH LIABILITY CANNOT BE LIMITED OR EXCLUDED UNDER APPLICABLE LAWS.

(b) Disclaimer of Damages. EXCEPT WITH RESPECT TO FEES PAYABLE BY YOU, TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAWS NEITHER TENCENT, NOR ITS AFFILIATES OR THEIR LICENSORS WILL BE LIABLE TO YOU UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF YOU HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES, FOR: (i) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES; OR (ii) UNAVAILABILITY OF THE SERVICES (EXCEPT AS PROVIDED UNDER SECTION 6(a)); (iii) YOUR APPLICATIONS OR INTELLECTUAL PROPERTY RIGHTS; OR (iv) LOSS OF DATA, LOST PROFIT, REVENUE, CUSTOMERS OR OPPORTUNITIES; IN EACH CASE, RELATING TO THE SERVICES AND THESE TERMS.

(c) Unlimited Liabilities. NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS YOUR LIABILITY FOR:

- (i) YOUR PAYMENT OBLIGATIONS UNDER THIS AGREEMENT;
- (ii) YOUR INDEMNIFICATION OBLIGATIONS UNDER SECTION 11(f);
- (iii) YOUR INFRINGEMENT OF OUR, OUR AFFILIATE'S OR LICENSOR'S INTELLECTUAL PROPERTY RIGHTS; OR
- (iv) ANY FRAUDULENT ACTIVITIES OR FRAUDULENT MISREPRESENTATION.

(d) Disclaimer of Certain Liabilities. Without limiting Section 11(a) or 11(b), if the Services are interrupted for any of the reasons set forth below, Tencent will promptly cooperate with the entities involved to resolve the applicable interruption, and to the extent permitted under applicable laws, Tencent disclaims liability for any loss or damages to the extent caused by the following:

- (i) causes attributable to infrastructure operators, including but not limited to technical adjustments made by telecommunications operators, damage to telecommunications/power lines, installation, modification or maintenance of telecommunications networks/power resources by telecommunications/power operators.
- (ii) your use of the Services in a manner not authorized by Tencent; improper operation by you or failures in your computer software, systems, hardware, or telecommunications lines; or
- (iii) any other circumstances not attributable to the fault of, outside the control of, or not reasonably foreseeable by, Tencent.

(e) Tencent Indemnification.

(i) Tencent will defend or, at its option, settle any third party claim, allegation, suit or proceeding (“**Claim**”) brought against you alleging that the use of the Services by you or your End Users in accordance with these Terms infringes a third party patent or copyright. Tencent will have sole control of the defense or settlement negotiations, and Tencent agrees to pay, subject to the limitations set forth in these Terms, any final judgment entered against you and any amounts agreed to in settlement by Tencent as a result of such infringement in any Claim defended by Tencent; provided that you provide Tencent with: (1) prompt written notice of the Claim; (2) sole control over the defense and settlement of the Claim; and (3) all reasonably requested information and assistance, at Tencent’s expense, to settle or defend the Claim.

(ii) In the event that any Claim is brought or, in Tencent’s opinion, likely to be brought, Tencent may, at its sole option and expense: (1) procure for you the right to continue to use the applicable Services; (2) modify the Services, or replace the Services with non-infringing software or services that do not materially impair the functionality of the Services; or (3) if neither of the foregoing is feasible on commercially reasonable terms, terminate these Terms and procure Tencent Cloud Partner or Second-Level Reseller to refund on a pro-rata basis any Fees prepaid by you to Tencent Cloud Partner or Second-Level Reseller for the applicable Services.

(iii) Tencent will have no obligation to you under this Section 11(d) to the extent a Claim arises from: (1) your breach of these Terms; (2) User Data; (3) use of the Software or Services in combination with any products, services, data, software, hardware or business processes not provided by Tencent, if the alleged infringement is based on that combination; (4) use of non-current or unsupported versions of the Services or Software; (5) modifications to the Software or Services by anyone other than Tencent or its Affiliates; or (6) liability arising from your or any End User’s use of the Services after Tencent has notified you to discontinue such use.

(iv) THIS SECTION 11 STATES THE ENTIRE LIABILITY OF TENCENT, AND YOUR SOLE AND EXCLUSIVE REMEDY, WITH RESPECT TO ANY CLAIM OF INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS WITH RESPECT TO THE SERVICES.

(f) Your Indemnification.

(i) You will defend, indemnify and hold harmless Tencent, its Affiliates, and each of their respective agents, licensors, employees, officers and directors from and against any Claims to the extent they arise out of or in relation to:

(1) your Application, product, service or User Data, including without limitation, their alleged infringement or misappropriation of the Intellectual Property Rights of any third party;

(2) you or your End Users' use of the Services or Software, including without limitation any (A) alleged violation of Data Protection Laws (as defined in the Data Processing and Security Agreement) by you, your End User(s), Tencent, or its Affiliate(s) in connection with such use; (B) alleged violation of any other applicable laws and regulations by you, your End Users, Tencent, or its Affiliates in connection with such use; (C) alleged violation of third party rights by you, your End Users, Tencent, or its Affiliates; and/or (D) such use that would constitute a violation of these Terms; and/or

(3) the use of any products, services, data, software, hardware or business processes not provided by or on behalf of Tencent or its Affiliates.

(ii) Tencent will provide you with: (1) prompt written notice of any Claims; and (2) reasonable assistance, at your expense, to defend or settle the Claim. Tencent and its Affiliates retain the right to appoint additional counsel of their choice to participate in defending or settling the Claims, in which case the counsel retained by you will consult with the counsel appointed by Tencent or its Affiliates and will give them the opportunity to provide comments on defense and settlement strategies.

(iii) At your option, you may settle any such Claims, provided that any settlement requiring Tencent or its Affiliates or their agents, licensors, employees, officers or directors to admit liability, pay money, or take or refrain from taking any action will require Tencent's or the Affiliate's prior written consent (not to be unreasonably withheld, conditioned, or delayed).

(iv) Without limiting the foregoing, you agree to pay any final judgment entered against Tencent or its Affiliates or their licensors, employees, officers and directors including without limitation any damages, costs, penalties, fees, disgorgement, restitution, and interest, or in the event of settlement, any settlement amounts agreed to by you, as a result of those Claims. You also agree to reimburse us for any costs and reasonable attorney's fees spent responding to any third-party subpoena, legal order or other processes associated with such Claims.

(g) Independent Allocations of Risk. EACH PROVISION OF THESE TERMS THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES IS INTENDED TO ALLOCATE THE RISKS OF THESE TERMS BETWEEN YOU AND TENCENT. THIS ALLOCATION IS REFLECTED IN THE FEES CHARGED BY TENCENT TO YOU AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN YOU AND TENCENT. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THESE TERMS, AND EACH OF THESE PROVISIONS WILL APPLY EVEN IF THE LIMITED REMEDIES IN THESE TERMS HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

## 12. TRADE COMPLIANCE

(a) Your Status. You represent and warrant that neither you, nor any of your officers, directors, shareholders, agents or employees, are:

(i) listed in any list of designated persons maintained by the United States (including, without limitation, the list of "Specially Designated Nationals" as maintained by the Office of Foreign Assets Control of the U.S. Treasury Department, the PRC, the United Nations Security Council, the United Kingdom (including the Consolidated List of Financial Sanctions Targets as maintained by His Majesty's Treasury), the European Union and any Member State thereof (including the Consolidated List of Persons, Groups and Entities Subject to Financial Sanctions), or any other

list of restricted persons maintained by any authority with jurisdiction over you (any person so listed being a “Restricted Person”);

(ii) organized under the laws of, operating from or located or resident in a country or territory that is the target of comprehensive sanctions (as of the date of last update of these Terms, including Iran, Cuba, North Korea, Syria and the Crimea/Sevastopol region and the so-called Donetsk and Luhansk People’s Republics (collectively “Sanctioned Territories”)); or

(iii) controlled or owned by 50 percent or more (directly or indirectly) in the aggregate by one or more Restricted Persons.

(b) Trade Compliance. In connection with your use of the Services, you will comply with all applicable export controls and economic sanctions laws and regulations of the United Nations, PRC, United States, European Union including its member states, the United Kingdom and other applicable government authorities including without limitation the U.S Export Administration Regulations (“EAR”) and the economic sanctions rules and regulations implemented under statutory authority and/or the U.S. President’s Executive Orders and administered by the U.S. Treasury Department’s Office of Foreign Assets Control (collectively, “Trade Laws”). You agree not to engage in any activities in connection with the use of the Services that would violate Trade Laws or that would risk placing Tencent in breach of any Trade Laws. You are solely responsible for compliance with Trade Laws related to the manner in which you choose to use the Services, including: (i) your transfer and processing of User Data; (ii) the provision of User Data to End Users; and (iii) specifying the Service Region in which any of the foregoing occur. For the avoidance of doubt, these Terms require you to, and you are solely responsible for complying with Trade Laws in the use of the Services by you and your End Users.

(c) Trade Compliance Event. (i) If you become a Restricted Person or controlled or owned by 50% or more (directly or indirectly) in the aggregate, by one or more Restricted Person; (ii) if provision of or use of the Services becomes otherwise restricted or prohibited as a consequence of the imposition of sanctions or by operation of Trade Laws; (iii) if Tencent determines at its sole discretion that a breach of the foregoing Sections 12(a) or (b) by you has occurred or is at risk or occurring; or (iv) if Tencent reasonably believes that you or your End User are, or are at risk, of being in violation of Trade Laws or are engaging in activities that would risk placing Tencent in breach of any Trade Laws, Tencent shall not be obliged to perform any of its obligations under these Terms or continue to provide the Services and shall be entitled, in its sole discretion, to terminate these Terms and the provision of the Services with immediate effect, without liability. Tencent is also entitled to, at its sole discretion, take any other remedial actions or relevant actions against you as it deems appropriate in light of the circumstances, including but not limited to, requesting you to remove any content that is subject to export control.

### 13.GENERAL

(a) Independent Contractors. The relationship of the parties established by these Terms is that of independent contractors, and nothing contained in these Terms should be construed to give either party the power to (i) act as an agent or (ii) direct or control the day-to-day activities of the other. Financial and other obligations associated with each party’s business are the sole responsibility of that party.

(b) Non-Assignability and Binding Effect. Neither party may assign or otherwise transfer, by operation of law or otherwise, its rights or obligations under these Terms without the prior written consent of the other party, except that

Tencent may freely assign or otherwise transfer these Terms without your consent: (i) in connection with a merger, acquisition or sale of all or substantially all of Tencent's assets; or (ii) to any Affiliate or as part of a corporate reorganization. Upon such assignment or transfer taking effect, the successor or permitted assigns (as the case may be) shall assume assignor/transferor's liability and assignor/transferor is released from the same. Any attempted assignment or transfer in violation of the foregoing restriction will be void. Subject to the foregoing, these Terms will be binding upon and inure to the benefit of the parties and their successors and permitted assigns.

(c) Consent to Electronic Communications. By using the Services, you consent to receiving certain electronic communications from us as further described in our Privacy Policy. Please read our Privacy Policy to learn more about our electronic communications practices. You agree that any notices, agreements, disclosures, or other communications that we send to you electronically, whether by e-mail, through the Services platform, or otherwise, will satisfy any legal communication requirements, including that those communications be in writing.

(d) Force Majeure. If the performance of these Terms is prevented, delayed, hindered or restricted, or Tencent breaches these Terms due to an event of force majeure, including but not limited to: (i) natural disasters; (ii) acts of government; (iii) promulgation or change of laws, regulations or policies (including Trade Laws, sanctions, restrictive measures or regulations); (iv) strikes or unrest; or (v) any significant change of circumstances (including changes in applicable laws which would render provision of Services potentially illegal or different from that contemplated by the parties at time of the acceptance of these Terms or first download, install, access, or use the Services), foreseeable or otherwise, in no case shall Tencent be liable for the breach of these Terms, or be otherwise liable for any such failure or delay in the performance of such obligations. If any of the abovementioned events persists for more than 15 calendar days, Tencent may terminate these Terms, without assuming any liability, by immediate written notice to you.

(e) Governing Law and Dispute Resolution. Except as provided in the North America Terms, EEA Consumer Terms, PRC Service Region Terms, Germany Terms, South Korea Terms or other region-specific or Service-specific terms, any claims for equitable relief may be brought any court of competent jurisdiction even if the parties have chosen an exclusive venue below. These Terms are governed by the jurisdiction set forth in Section 3. Unless the North America Terms, EEA Consumer Terms, PRC Service Region Terms, Germany Terms, South Korea Terms or other region-specific or Service-specific terms specify otherwise, all claims arising out of or relating to these Terms or the Services, will be resolved by arbitration administered by the Singapore International Arbitration Centre in accordance with the Arbitration Rules of the Singapore International Arbitration Centre in force when the notice of arbitration is submitted. The seat of the arbitration will be Singapore and the language will be English. All proceedings will be confidential and there will be one arbitrator only.

(f) Waiver and Severability. The waiver by either party of any breach of these Terms does not waive any other breach. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under these Terms. If any part of these Terms is unenforceable, the remaining portions of these Terms will remain in full force and effect.

(g) No Third-Party Beneficiaries. These Terms are not intended to confer any benefits on any third party except to the extent that it expressly states that it does. End Users are not a third party beneficiaries to these Terms.

(h) Entire Agreement. These Terms and the Additional Terms are the final and complete expression of all agreements between you and Tencent regarding their subject matter and supersede all prior oral and written agreements



regarding these matters. The Additional Terms referred to in these Terms are incorporated by this reference. In the event of any conflict between the terms of the main terms and conditions of these Terms and the Additional Terms, these main terms and conditions will control, followed by the Additional Terms. However, the terms and conditions of the PRC Service Region Terms, the North America Terms, the EEA Consumer Terms, the Germany Terms or the South Korea Terms will control, if applicable.

(i) Modification of these Terms, the Privacy Policy and the Cookies Policy. Tencent may amend these Terms, including the Additional Terms, from time to time by posting updated versions to the Tencent Cloud site. Unless specifically provided in these Terms or the Additional Terms, or otherwise indicated by Tencent, the amended terms will take effect within 30 calendar days after they are posted. Notwithstanding the foregoing, any changes relating to Tencent's Services or product functionalities shall take effect immediately. Tencent will use reasonable efforts to notify you of the changes, but you are responsible for periodically checking these Terms, including the Additional Terms, for any modifications. Your continued use of the Services constitutes your acceptance of any amended Terms. Amended terms are not applicable retroactively.

(j) Language. All communications and notices in relation to these Terms shall be made or given in either English or Chinese. Notwithstanding the foregoing, to the extent any translations of these Terms are made, the English version shall prevail.

(k) Publicity. You agree that Tencent may refer to you as a customer of Tencent and use your name and logo in Tencent's marketing materials and websites. Except as otherwise permitted by law, you shall not issue any press release or make any other public communication with respect to these Terms, or the fact that Tencent is providing Services for you. You shall not use Tencent's trademarks, service marks, service or trade names, logos ("**Tencent Marks**"); or identify Tencent as a supplier of the Services without prior written consent of Tencent. Notwithstanding the permission granted, unless otherwise agreed by Tencent in writing, your limited permission to identify Tencent for such purposes and for the use of Tencent's Marks shall terminate as soon as these Terms expire or are terminated, whichever is sooner. Your use of the Tencent Marks shall be subject to any terms, conditions, or guidelines that Tencent may issue from time to time.

(l) Notice. Any notice required or permitted to be given under these Terms will be effective if it is in writing and sent by certified or registered mail, or insured courier, return receipt requested, to the appropriate party at the address set forth above (in the case of Tencent) and the registered billing address or any other address registered with us (in your case) and with the appropriate postage affixed. Either party may change its address for receipt of notice by notice to the other party in accordance with this Section. Notwithstanding the foregoing, any notices, communications, or disclosures sent electronically by Tencent through email, the platform for the Services or otherwise, shall be deemed a valid and binding notice required or permitted to be given under these Terms.

## TENCENT CLOUD PRC SERVICE REGION TERMS

To the extent you have purchased a subscription to Services from a Tencent Cloud Partner or Second-Level Reseller subject to the Tencent Cloud Reseller Customer Terms of Service ("Terms") for which the PRC is the Service Region, such Services shall be provided by Tencent Cloud Computing (Beijing) Co., Ltd. ("**Tencent Cloud Beijing**") and subject to the terms of these PRC Service Region Terms as well as any applicable PRC laws and regulations. Any terms used but not defined in these PRC Service Region Terms have the meaning given to them in the Terms.

1. You hereby acknowledge and agree that (a) whilst Tencent Cloud Beijing shall provide the Services hereunder in accordance with these Terms and PRC Service Region Terms, it will not otherwise be responsible for your product, service, content and data used in connection with the Services; and (b) you have obtained, and shall maintain for the term of the Terms all applicable and valid regulatory, legal, and/or governmental licenses, filings, recordings, approvals, permits, etc. as may be required by any applicable PRC laws and regulations for the use of the Services and for your business operations using the Services in the PRC Region.

**2. Prohibited Conduct. When using Services in the PRC,** you must comply with all applicable PRC laws, regulations, rules and policies, and safeguard cybersecurity. You must not engage in, or facilitate, any activities that constitute a violation of such applicable laws, regulations, rules and policies, including but not limited to:

- (a) activities that contravene the Basic Principles of the Constitution of the PRC, jeopardize national security, reputation or interests; incite subversion of state power; overthrow the socialist system; incite division of state and sabotage national unity; advocate terrorism or extremism; incite ethnic hatred or discrimination; undermine the national religion policy and/or promote cults or feudal superstitions;
- (b) deceptive, false or misleading practices, or practices that infringe the intellectual property rights or legitimate rights and interests of others, such as using “private servers” or “plug-ins”;
- (c) the posting, publishing or dissemination of spam or unlawful content that disrupt national order, jeopardize national security, or advocate for feudal superstitions, obscenity, pornography or vulgarity;
- (d) violation of operating rules relating to networks, devices or services linked to the Tencent Cloud network; unlawful or unauthorized access, misappropriation, interference or surveillance any actual or attempted sabotage of network security, including but not limited to performing malicious scanning of websites and servers, hacking into a system, or unlawfully accessing data by using viruses, Trojans or malicious codes, phishing and so forth;
- (f) any actual or attempted modification of system configuration set by Tencent or any actual or attempted sabotage of system security; using technological means to undermine or disrupt the operation or others' use of the Services; any actual or attempted disruption of the normal operation of any products of Tencent or any part or functions thereof in any way, or the production, posting or dissemination of such tools or methods;
- (g) you being frequently attacked (including but not limited to DDoS attacks) as a result of the provision of Services, including but not limited to "DNS resolution", "security services", "domain name proxy" and "reverse proxy", and failing to correct your practices in a timely manner, or failing to eliminate the effects as requested by Tencent, thereby causing an impact on the Services platform or on others;
- (h) activities violating the “Seven Bottom Lines”, where the “Seven Bottom Lines ” refers to the baseline standards in the following seven areas: laws and regulations, socialist system, national interests, citizens' legitimate rights and interests, national order, moral risks, and information veracity, as promulgated by the competent authorities, and which may be updated or amended from time to time; and
- (i) any other illegal or non-compliant practices, including but not limited to illegal activities such as gambling, violence, murder, terrorism, instigating crime, defamation, abuse, disruption of internet security and order, etc.

**3. Your Information.**

(a) You shall provide truthful, legitimate and valid information (the "Information") in accordance with the registration procedures for the Services, including but not limited to your name, contact, email, telephone number, mailing



address, industrial and commercial registration documents and so forth. If any change occurs to the Information, you shall promptly notify Tencent of such change.

(b) To ensure account and transaction security, Tencent shall be entitled to require you to carry out real-name authentication at any time, and you shall cooperate accordingly. You agree that Tencent Cloud may authenticate your Information with third parties, and you authorize Tencent to obtain all necessary information relating to your use of the Services.

(c) In order to reasonably protect your interests and those of your users and other right holders, Tencent shall be entitled to put in place processes and systems specifically devoted to dealing with infringement and complaints, and you shall comply with such processes and systems. If Tencent receives a complaint or report from a third party against you, Tencent shall be entitled to disclose your information (including but not limited to your registered name, identification, contacts, telephone number and so forth) to the complainant as necessary and urge you to consult with the complainant, with a view to promptly resolving such complaint or dispute and protecting the legitimate rights and interests of all parties concerned. You shall extend your cooperation; failure to do so may affect your use of the Services.

**4. Security.** You will not install or use any pirated software on the Services, and must take security measures to protect your computer information systems as required under applicable PRC laws, regulations, rules, including but not limited to installing any required State-approved security products specifically designed for computer information systems.

**5. Remedies.** If Tencent discovers, on its own or based on information provided by the competent authorities or complaints filed by rights holders, that you have violated applicable PRC laws, regulations or rules, or breached the Terms, including these PRC Service Region Terms, Tencent will be entitled to take any one or more of the following actions at its own discretion:

- (a) demand that you immediately remove or modify the content in question;
- (b) immediately remove or block the content in question or disable the links in question;
- (c) restrict or suspend the provision of the Services to you (including but not limited to directly taking your services offline and withdrawing the relevant resources or setting restrictions on your operations under your Account(s));
- (d) in case of serious violations or breaches, Tencent will have the right to terminate the provision of Services to you and terminate the Terms (including but not limited to directly taking all of your services offline and withdrawing the relevant resources). The Fees already paid by you for any unused service period will be credited to Tencent as liquidated damages; and
- (e) pursuing other liabilities against you in accordance any applicable PRC laws and regulations.

Tencent shall not be responsible or held liable for any damages or losses, including but without limitation to the suspension of your business operations, deletion of data, etc., arising from the actions taken by Tencent hereunder due to your breach of these Terms and PRC Service Region Terms. You shall indemnify and hold harmless Tencent, its Affiliates, and each of their respective licensors, employees, officers and directors in respect of any damages or losses arising as a result of your breach of these Terms and PRC Service Region Terms.

**6. Cooperation with Authorities.** In accordance with any applicable PRC laws or regulations, or otherwise in compliance with the inquiry, request, order, or direction of any PRC governmental authorities, regulators, judicial,

administrative or other competent authorities, and notwithstanding any confidentiality obligations or non-disclosure obligations whether set forth in these Terms or otherwise, Tencent will be entitled to render cooperation to the aforementioned authorities and regulators in respect of any inquiries, investigations, proceedings or otherwise, including providing the relevant information to such regulators and authorities, to facilitate the resolution of complaints and disputes in a timely manner and protect the legitimate rights and interests of all parties concerned.

**7. Governing Law.** The provision of Section 13(e) and the provisions of Section 3 concerning governing law of the Terms are hereby deleted and restated as follows:

The formation, validity, effectiveness, performance and interpretation of, and dispute resolution in relation to, these Terms will be governed by the laws of the PRC (excluding the conflicts of law provisions). In the event of any dispute arising out of these Terms, the parties will first attempt to resolve the dispute through consultations in good faith; if the parties fail to resolve the dispute through such consultations, either party may refer the dispute or conflict to the People's Court in Nanshan District, Shenzhen.

### **TENCENT CLOUD NORTH AMERICA TERMS**

To the extent you wish to purchase a subscription to Services from a Tencent Cloud Partner or Second-Level Reseller in North America and you are subject to the Tencent Cloud Reseller Customer Terms of Service (“**Terms**”) and the country specified in your registered billing information with Tencent Cloud Partner or Second-Level Reseller is in North America, you shall be subject to the terms of these North America Terms. Any terms used but not defined in these North America Terms have the meaning given to them in the Terms.

#### **TENCENT CLOUD NORTH AMERICA TERMS**

To the extent you wish to purchase a subscription to Services from a Tencent Cloud Partner or Second-Level Reseller in North America and you are subject to the Tencent Cloud Reseller Customer Terms of Service (“Terms”) and the country specified in your registered billing information with Tencent Cloud Partner or Second-Level Reseller is in North America, you shall be subject to the terms of these North America Terms. Any terms used but not defined in these North America Terms have the meaning given to them in the Terms.

#### **1. Dispute Resolution and Arbitration**

(a) Except for the right of either party to apply to any court of competent jurisdiction for a temporary restraining order, a preliminary injunction, or other equitable relief to preserve the status quo or prevent irreparable harm, any dispute, controversy or claim arising in any way out of or in connection with the Terms, including the existence, validity, interpretation, performance, breach or termination of the Terms, or any dispute regarding pre-contractual or non-contractual rights or obligations arising out of or relating to it (“**Dispute**”) will be referred to and finally resolved by binding arbitration. Arbitration is less formal than a lawsuit in court. Arbitration uses a neutral arbitrator instead of a judge or jury, may allow for more limited discovery than in court, and can be subject to very limited review by courts. Arbitrators can award the same damages and relief that a court can award. This agreement to arbitrate disputes includes all claims arising out of or relating to any aspect of these Terms, whether based in contract, tort, statute, fraud, misrepresentation, or any other legal theory, and regardless of whether a claim arises during or after the termination of these Terms. YOU UNDERSTAND AND AGREE THAT, BY ENTERING INTO THESE TERMS, YOU AND TENCENT ARE EACH WAIVING THE RIGHT TO A TRIAL BY JURY OR TO PARTICIPATE IN A CLASS ACTION.

(b) Any arbitration between you and Tencent will be administered by the American Arbitration Association (“**AAA**”) under its rules in force when the Notice of Arbitration is submitted in accordance with those Rules (“**Rules**”), which Rules are deemed to be incorporated by reference into this clause and as may be amended by the rest of this clause. The Rules and filing forms are available online at [www.adr.org](http://www.adr.org) or by calling the AAA at 1-800-778-7879. The Federal Arbitration Act and federal arbitration law apply to the Terms. All arbitration proceedings between the parties will be confidential unless otherwise agreed by the parties in writing.

(c) Tencent will reimburse you for your payment of the filing fee, unless your claim is for more than \$10,000, in which case the payment of any fees will be decided by the Rules. Any arbitration hearing will take place at a location to be agreed upon in Santa Clara County, California, but if the claim is for \$10,000 or less, you may choose whether the arbitration will be conducted: (a) solely on the basis of documents submitted to the arbitrator; (b) through a non-appearance based telephone hearing; or (c) by an in-person hearing as established by the Rules in the county (or parish) of your billing address. The arbitration tribunal will consist of three arbitrators to be appointed in accordance with the Rules. Arbitration will be conducted in English. Judgment upon the award rendered by the arbitrators may be entered in any court of competent jurisdiction.

(d) YOU AND TENCENT AGREE THAT EACH MAY BRING CLAIMS AGAINST THE OTHER ONLY IN YOUR OR ITS INDIVIDUAL CAPACITY AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE PROCEEDING. Further, unless both you and Tencent agree otherwise, the arbitrator may not consolidate more than one person’s claims, and may not otherwise preside over any form of a representative or class proceeding.

## 2. Third Party Connectivity Services

The Services provided to you may include broadband data connectivity services that connect your location(s) to Tencent Cloud (the “Third Party Connectivity Services”). Tencent acts as a network manager and obtains the Third Party Connectivity Services on your behalf as an element of the Services you receive. The Third Party Connectivity Services are provided by one or more broadband service provider(s) subject to the terms and conditions of such provider(s). The Third Party Connectivity Services are subject to certain performance limitations that impact your use of the same. You may contact Tencent at [cloudlegalnotices@tencent.com](mailto:cloudlegalnotices@tencent.com) to obtain additional information about the Third Party Connectivity Services that are being used as an element of your Services, including the provider(s)’ network practices, performance characteristics, and applicable commercial terms. Tencent passes through any costs for the Third Party Connectivity Services from the provider(s) to you and may charge a network manager fee as part of the Services offered.

## TENCENT CLOUD EUROPEAN ECONOMIC AREA, SWITZERLAND AND UK (“EEA”) CONSUMER TERMS

If you are not a business user and you are purchasing the Services for personal use, to the extent you wish to purchase a subscription to Services from a Tencent Cloud Partner or Second-Level Reseller in EEA and you are subject to the Tencent Cloud Reseller Customer Terms of Service (“**Terms**”) and the country specified in your registered billing information with Tencent Cloud Partner or Second-Level Reseller is in EEA, such Services shall be subject to the terms of these EEA Consumer Terms. Any terms used but not defined in these EEA Consumer Terms have the meaning given to them in the Terms.

## 1. Governing Law

These terms shall be governed by English law, except that (if you are a consumer and not a business user) and if you live in a country (which, for these purposes, includes Scotland or Northern Ireland) of the European Union other than England, there may be certain mandatory applicable laws of your country which apply for your benefit and protection in addition to or instead of certain provisions of English law and those mandatory laws will apply.

You agree that any dispute between you and us regarding these terms or the Services will only be dealt with by the English courts, except that if you are a consumer and not a business user) and if you live in a country (which, for these purposes, includes Scotland or Northern Ireland of the European Union other than England, you can choose to bring legal proceedings either in your country or in England, but if we bring legal proceedings, we may only do so in your country. If you are a consumer within the EEA, to the extent there is any conflict, this provision shall take precedence over any term in the front-end of these Terms.

If you reside in EEA you may also have recourse to a mediation procedure body designated by us or an alternative dispute resolution process. The European Commission provides consumers with an online dispute settlement platform accessible at the following address: <http://ec.europa.eu/consumers/odr/>.

## **2.Cancellation Right**

You normally have the right to cancel the Services within 14 days after the date the Services start being provided. However, you acknowledge that we start provision of the Services immediately following acceptance of your selection of the Services (which, by selecting the Service, you request us to do) and that you will have no right to change your mind and cancel under the Consumer Contracts Regulations once the Services have been fully carried out. If you cancel before the Services have been fully carried out (and within the 14-day period) then the charge you paid to Tencent Cloud Partner or Second-Level Reseller (and which Tencent Cloud Partner or Second-Level Reseller will deduct from any refund otherwise due to you) will be proportionate to the Services that have been used by the time you cancel, and will not exceed our reasonable costs of providing the Services up until that point.

To cancel the Services, you must clearly inform us, preferably:

by contacting customer service by submitting a work order through the console at <https://console.tencentcloud.com/workorder/category>, giving us your name, address, and account information; or  
Nothing in this section affects your legal rights.

## **3.Refunds policy**

If you cancel the Services within the 14-day cooling-off period (see above), we will notify Tencent Cloud Partner or Second-Level Reseller and Tencent Cloud Partner or Second-Level Reseller shall process your refund request in accordance with the Tencent Cloud Partner's or Second-Level Reseller's refund policies and applicable laws in the EEA.

## **4.Defective Services**

If any Services you order are defective (in other words, they do not comply with the requirements of these Terms), you may have one or more legal remedies available to you, depending on when you make us aware of the problem, in accordance with your legal rights. If you believe the Services are defective, you should inform us as soon as possible by contacting customer service by submitting a work order through the console at <https://console.tencentcloud.com/workorder/category>, giving your name, address and account information. Nothing in this section affects your legal rights.

## 5.France Specific Terms

If you are a consumer residing in France, please note that the exclusion and limitation of liability provisions included in Sections 11(a) and 11(b) of the Terms above, will not apply to you.

### TENCENT CLOUD GERMANY TERMS

To the extent you wish to purchase a subscription to Services from a Tencent Cloud Partner or Second-Level Reseller in Germany and you are subject to the Tencent Cloud Reseller Customer Terms of Service (“Terms”) and the country specified in your registered billing information with Tencent Cloud Partner or Second-Level Reseller is Germany, you shall be subject to the terms of these Germany Terms, which prevail over the general Tencent Cloud Reseller Customer Terms of Service in case of any contradictions. Any Terms used but not defined in these Germany Terms have the meaning given to them in the Terms.

**1. Privacy Policy.** Our Privacy Policy does not form part of the Terms. It only serves for informational purposes and provides information on how we process personal data within the scope of the Services.

**2. Changes to the Service and/or the Terms.** We reserve the right to change the Service and/or the Terms. We will notify you of the changed conditions by email at least six (6) weeks before their effective date and will indicate the intended application of these new Terms. If you do not object to the application of the new Terms within this period of time or if you continue to use the Services after the changed Terms have entered into force, the new Terms will be considered to have been accepted. We will notify you of the importance of the six (6) week period, the right to object, and the legal consequences of silence. If you do not accept the new Service and/or Terms, which are essential for the continued provision of our Services, we may terminate our contractual relationship with you.

**3. Third Party Software.** No terms and conditions applicable to Third Party Software form part of the Terms. You are not bound by any terms and conditions applicable to Third Party Software by these Terms.

**4. Limitation of Liability, Indemnification.** Notwithstanding Section 11 of the Tencent Cloud Reseller Customer Terms of Service, the following applies to you:

(a) For damages with respect to injury to health, body or life caused by Tencent, Tencent’s representatives or Tencent’s agents in the performance of the contractual obligations, we are fully liable.

(b) Tencent is fully liable for damages caused wilfully or by gross negligence by Tencent, Tencent’s representatives or Tencent’s agents in the performance of the contractual obligations. The same applies to damages which result from the absence of a quality which was guaranteed by Tencent or to damages which result from malicious action.

(c) If damages, except for such cases covered by Sections 4(a), 4(b) or 4(d), with respect to a breach of a contractual core duty are caused by slight negligence, Tencent is liable only for the amount of the total fees that you have paid to Tencent under these terms in the twelve (12) months immediately preceding the date that event giving rise to the liability first occurred. Contractual core duties, generally, are such duties whose accomplishment enables proper performance of an agreement in the first place and whose performance a contractual party regularly may rely on.

(d) Tencent’s liability based on the German Product Liability Act remains unaffected.

(e) Any further liability of Tencent is excluded.

(f) The limitation period for claims for damages against Tencent expires after one (1) year, except for such cases covered by sections 4(a), 4(b), or 4(d).

**5. Inapplicable Clauses.** The following Section of the Tencent Cloud Reseller Customer Terms of Service do not apply to you: Section 9(b)(iv), Section 9(d), Section 10, and Section 12(g).

**6. Consent to Electronic Communications.** Notwithstanding Section 12(c) of the Tencent Cloud Reseller Customer Terms of Service, we will ask you for a separate consent to receiving certain electronic communications from us.

**7. Term and Termination.** Irrespective of Section 9 of the Tencent Cloud Reseller Customer Terms of Service, Tencent may terminate the Terms at any time and for any and no reason upon providing to you 30 days' written notice.

**8. Governing Law.** Notwithstanding Section 3(a) of the Tencent Cloud Reseller Customer Terms of Service, if you use our Services as a consumer, the governing law that applies to the Terms is German law.

## **TENCENT CLOUD SOUTH KOREA TERMS**

To the extent you wish to purchase a subscription to Services from a Tencent Cloud Partner or Second-Level Reseller in South Korea and you are subject to the Tencent Cloud Reseller Customer Terms of Service ("Terms") and the country specified in your registered billing information with Tencent Cloud Partner or Second-Level Reseller is South Korea, you shall be subject to the terms of these South Korea Terms, which prevail over the general Tencent Cloud Reseller Customer Terms of Service in case of any conflict or inconsistency. Any terms used but not defined in these South Korea Terms have the meaning given to them in the Terms.

### **1. Eligibility**

Section 2 concerning eligibility of Terms is hereby restated as follows: You must be at least 19 years old to use the Services. By agreeing to these Terms (including South Korea Terms, hereinafter the same), you represent and warrant to us that: (a) you are at least 19 years old; (b) you have not previously been suspended or removed from the Services; and (c) your registration and your use of the Services is in compliance with any and all applicable laws and regulations. If you are an entity, organization or company, the individual accepting these Terms on your behalf represents and warrants that they have authority to bind you to these Terms and you agree to be bound by these Terms.

### **2. Changes on Services or Fees**

If Tencent changes the Services or Fees, Tencent will specify the reason for the change, the content of the Services or Fees to be changed, and the date of provision, etc., and post such information on the initial screen of the Service at least 7 days prior to the date of implementation of such change. However, if the change in Service or Fees is unfavorable or material to you, we will notify you at least 30 days in advance and obtain consent from you with respect to the change.

### **3. Cancellation**

(a) If you are an end-user of the Services and a consumer under Act on the Consumer Protection in Electronic Commerce, etc., you may cancel the Services within 7 days after the date of commencement of the Services. However, notwithstanding the above, if the contents of the Services are different from the contents displayed or advertised by Tencent, or if the contents are performed differently from contents specified in the Terms and other agreements related to the Services, you may cancel the Services within three months after the date of commencement of the Services, or within 30 days after the date you knew or could have known such fact.

(b) You may not cancel the Services against Tencent's intention if the Services that Tencent has provided are temporary or with only partial functions.



(c) in order to cancel the Services, you must clearly inform us, preferably by contacting customer service by submitting a work order through the console at <https://console.tencentcloud.com/workorder/category>, giving us your name, address, and account information.

(d) Cancellation will take effect from the date of sending your intention to cancel.

(e) If you cancel, Tencent will delete and terminate your Service without delay and Tencent Cloud Partner or Second-Level Reseller shall refund Fees within 3 days after the date of deletion/termination.

(f) In the event that Tencent Cloud Partner or Second-Level Reseller delays the refund in paragraph (e), Tencent Cloud Partner or Second-Level Reseller will pay you the delayed interest calculated by multiplying the delayed period by the interest rate prescribed by the Act on the Consumer Protection in Electronic Commerce, Etc. and the Enforcement Decree.

(g) Tencent will request, through Tencent Cloud Partner or Second-Level Reseller, the business operator who provided the Payment Method used to pay the Fees to suspend or cancel the charge for the Fees without delay. However, if Tencent Cloud Partner or Second-Level Reseller has already received Fees from the payment company, it will be refunded to the payment company and notify to you.

(h) If you have used some of the Services, Tencent is entitled to make a claim against you for an amount equivalent to the benefits you have obtained by using the Services or the cost of supplying the Services for you.

(i) Tencent may not claim a penalty or compensation for damages on the grounds of cancellation.

#### **4.Modification of the Terms**

If Tencent intends to amend the Terms, Tencent will post the updated version on the Tencent Cloud website. Updated versions will be effective no earlier than 7 days after the date of posting. Your continued use of the Services after the effective date of the updated Terms constitutes your acceptance of any amended Terms. However, if the modification in the Terms is unfavorable or material to you, we will notify you at least 30 days in advance and obtain consent from you with respect to the modification.

#### **5.Governing Law**

Notwithstanding Section 3(a) of the Terms, if you use our Services as an end-user or consumer, the governing law that applies to the Terms will be Korean Law.

# 合作伙伴学堂

## 合作伙伴学院权限申请

最近更新时间：2022-04-20 16:05:43

### 合作伙伴学院账号权限申请

说明：

合作伙伴可以直接登录学院，如员工需开通学院权限，伙伴可替其申请权限，步骤如下。

第一步：使用合作伙伴账号登录[腾讯云](#)，进入[合作伙伴中心](#)

第二步：点击【申请合作伙伴学院】

Partner Central

Overview

Company Info

Customer Management

Customer Bills

Download Records

Customer Management

+ Invite Customers

Application for Partner Academy Access

Account ID 

Check rejected record

My Customers

Pending Customers

Account ID/Remarks	Name	Mobile	Email	Association Time <div></div>	Credit	Available Credit	Operation
<div></div>				2021-12-01 11:10:24	\$0.00	\$0.00	<a href="#">Setting Credit</a>
<div></div>				2021-11-09 15:16:45	\$0.00	\$0.00	<a href="#">Setting Credit</a>
<div></div>				2021-11-09 12:46:24	\$0.00	\$0.00	<a href="#">Setting Credit</a>
<div></div>				2021-11-08 14:05:03	\$0.00	\$0.00	<a href="#">Setting Credit</a>



第三步：按照提示框要求填写账号申请信息，上传申请资料。

### Application for Partner Academy Access

Account ID

Documents

Notes:  
1. [Download template](#) and fill it out as instructed. [See Certificate Sample](#)  
2. Supported formats of uploaded files include .webp, .bmp, .jpg, .png, .tif, .gif, and .apng, and the size of an image cannot exceed 1 MB.  
3. The review process takes approximately 3 business days. You and your customers will be notified if the application is approved.

☐ I confirm that I have read and agree to the [Tencent Cloud Partner Program Terms and Conditions](#) and [Tencent Cloud International Partner Academy Program Terms of Service](#) .  
☐ I have read and acknowledge the [Tencent Cloud International Partner Academy Privacy Notice](#) .  
☐ I confirm that I have obtained the explicit consent from the applicant employee(s) and/or representative(s) to share their personal information to Tencent in accordance with [Tencent Cloud International Partner Academy Privacy Notice](#), and that they have read and acknowledge the [the Tencent Cloud International Partner Academy Privacy Notice](#).

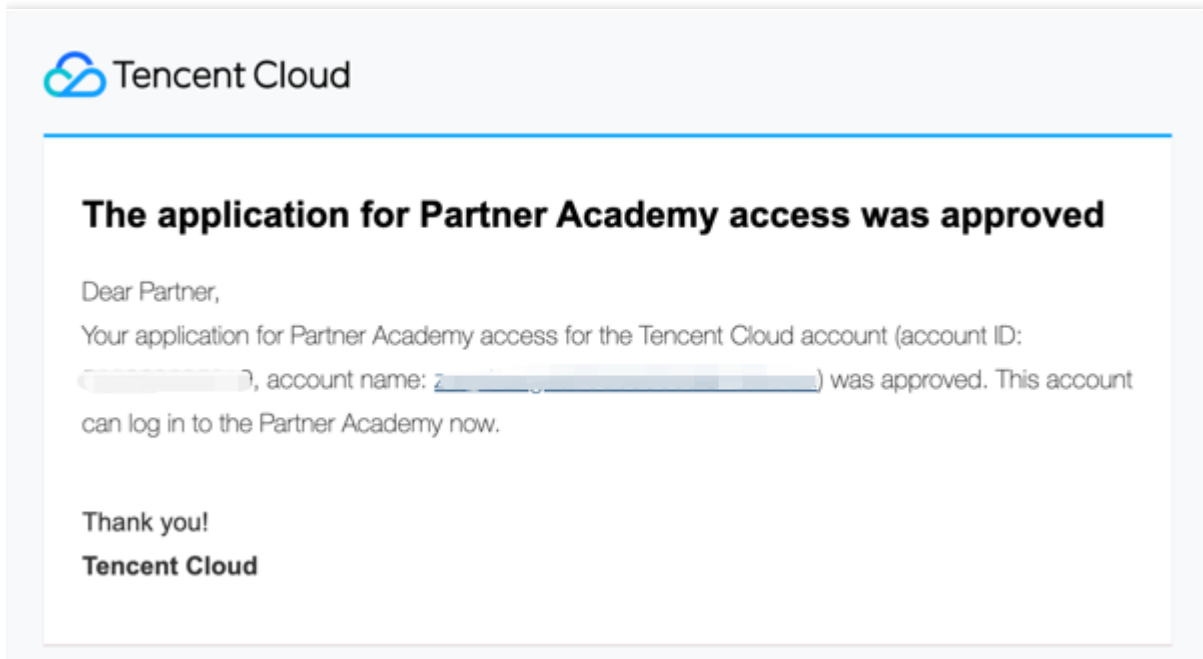
SubmitCancel

说明：

- 必须是腾讯云国际站账号，才能申请合作伙伴学院；
- 已申请或者已有合作伙伴学院权限的账号，请勿重复申请；
- 属于其他合作伙伴或其他合作伙伴子客的账号，请勿申请权限；
- 审核上传证明材料请根据下载模板样式填写；
- 上传单张图片大小不得超过1M；
- 审核大约需要1-2天，审核通过后会以邮件形式通知合作伙伴和客户

第四步：点击【提交】，权限申请提交成功后，等待审批通过。

第五步：收到审批通过通知邮件，权限申请完成。

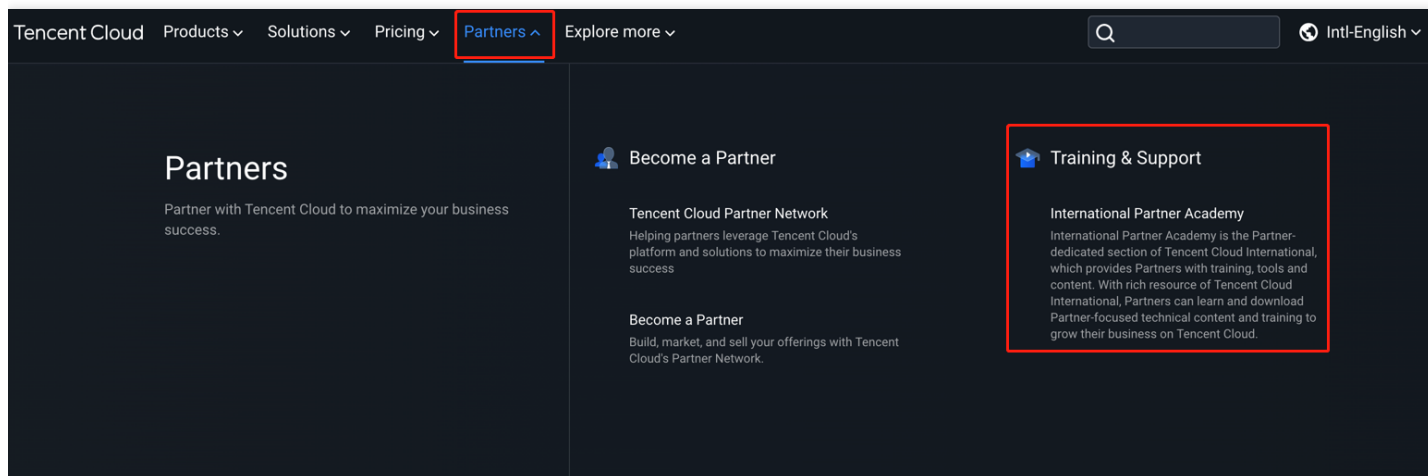


# 登录合作伙伴学院

最近更新时间：2022-05-07 14:38:11

第一步：登录[腾讯云官网](#)；

第二步：点击导航栏【合作伙伴】，进入合作伙伴学院，如下图所示：




说明：

- 需登录腾讯云账号，才可以进入合作伙伴学院，请先登录账号。
- 登录账号必须是国际站合作伙伴主账号，其他账号类型均不可登录。
- 如果不满足合作伙伴主账号的要求，可让合作伙伴代替申请权限，详情请查看[权限申请](#)。


第三步：成功登录合作伙伴学院后，界面自动跳转到学院首页。

Partner Academy
Home
Library
Courses

Search




Recommended Courses




Powering Growth in China - English & Chinese Sessions

2 sections 2 learned



Chapter 1 - Tencent Cloud Solutions Architect Professional

3 sections 3 learned



Chapter 1 - Tencent Cloud SysOps Associate

5 sections 0 learned

Latest Documents

- Lighthouse\_v1.0\_EN-US 2022-04-28 20:40
- EdgeOne\_v1.0\_EN-US 2022-04-28 20:16
- TRTC\_v1.0\_EN-US 2022-03-24 17:44
- TRTC\_One-Pager\_v1.0\_EN-US 2022-03-24 17:44
- Cloud Monitor\_v1.0\_EN-US 2022-03-24 17:43

LibraryCategory

- Solutions
- Security
- Developer Serv...
- Compute and ...
- Enterprise App...
- Storage
- Artificial Intellig...
- Database
- Middleware an...
- Networking an...
- Video Services

Noticeboard

WELCOME TO PARTNER ACADEMY

You can learn our Partner-focused technical content and training to grow your business with Tencent Cloud.

If you have a question related to Partner Academy, please feel free to contact us as below.

[charlixchen@tencent.com](mailto:charlixchen@tencent.com)

[barryccwang@tencent.com](mailto:barryccwang@tencent.com)

My pending (4)

TCI-PA Practitioner
Project · There is no time for the time.
0/7

TCI-PA Solutions Architect Associ...
Project · There is no time for the time.
0/6

TCI-PA SysOps Associate
Project · There is no time for the time.
0/7

# 协议管理

## 腾讯云国际合作伙伴学堂隐私声明

最近更新时间：2022-05-07 12:46:15

### 1.INTRODUCTION

This Notice applies if you have a Tencent Cloud account and would like to access, or apply for access to, the Partner Academy at [lexiangla.com](https://lexiangla.com) ("Partner Academy"). This Notice incorporates the Tencent Cloud privacy policy located at ("[Privacy Policy](#)"). Terms used but not defined in this Notice shall have the meaning given to them in the Privacy Policy. In the event of any conflict between the Privacy Policy and this Notice, this Notice shall apply to the extent of the inconsistency.

### 2.CONTROLLERSHIP

The controller of the personal information described in this Notice is as specified in the Privacy Policy.

### 3.HOW WE USE PERSONAL INFORMATION

We will use the information in the following ways and in accordance with the following legal basis:

#### Application to access Partner Academy

Personal Information	Use	Legal Basis
<b>Partner, Employee and Representative Access Data:</b> Information you provide as part of filling out the application form, including the applicant's name, Tencent Cloud ID, UIN, APPID, relationship with Partner, reason for application (if applicable), and company name.	<ul style="list-style-type: none"><li>We use this information for the purpose of processing your application to, and verify the applicant's eligibility (as the Partner, the Partner's employee or representative, as applicable) to, access the Partner Academy.</li><li>Please note that this data is stored in our TencentDB for MySQL feature.</li></ul>	We process this information as it is necessary for us to perform our contract with you.

#### Access to Partner Academy

Personal Information	Use	Legal Basis
<b>Sign-Up Data:</b> User ID	<ul style="list-style-type: none"><li>We use this information for the purpose of verifying whether you (and/or employee(s) and representative(s), as applicable) have access to Partner Academy.</li><li>Please note that this data is stored and backed up in our TencentDB for MySQL feature.</li></ul>	We process this information as it is necessary for us to perform our contract with you.
<b>Verification Data:</b> Open ID	<ul style="list-style-type: none"><li>We use this information for the purpose of verifying whether you (and/or employee(s) and representative(s), as applicable) have access to Partner Academy.</li><li>Please note that this data is stored and backed up in our TencentDB for MySQL feature.</li><li>Please note that this data will be hashed before it is also shared with the Partner Academy for this purpose and for account management.</li></ul>	We process this information as it is necessary for us to perform our contract with you.

## 4.HOW WE STORE AND SHARE PERSONAL INFORMATION

As specified in the Privacy Policy. Additionally, we will hash verification data before sharing it with **Shenzhen Tencent Computer System Co. Ltd.** for the purpose stated above.

## 5.DATA RETENTION

We will retain personal information in accordance with the following:

Personal Information	Retention Policy
<b>Partner, Employee and Representative Access Data</b>	This data is held for so long as an account exists. Information is erased within thirty (30) days of the date the account is deleted.
<b>Sign-Up Data</b>	This data is held for so long as an account exists. Information is erased within thirty (30) days of the date the account is deleted.
<b>Verification Data</b>	This data is held for so long as you have access to the Platform Academy, and then erased within 30 days.

# 腾讯云国际合作伙伴学堂服务条款

最近更新时间：2022-05-07 12:47:10

To the extent you have accepted the terms and conditions to govern your participation in Tencent Cloud International Partners Program (“[Tencent Cloud International Partner Terms](#)”), and you wish to receive services under the Tencent Cloud International Partner Academy Program, these Tencent Cloud International Partner Academy Program Terms (“**Terms**”) will govern your access to and use of the Tencent Cloud International Partner Academy Program, and related services provided or received on or via the Tencent Cloud International Partner Academy Program (collectively, the “**Program**”). By accessing or using the Program, or by ticking “I Agree” or “I Accept” in the application form, you confirm that you have read and understood, and you agree to be bound by, these Terms. For the purposes of these Terms, “**Tencent**”, “**we**”, “**our**” and “**us**” refer to the applicable entities as listed in the Tencent Cloud International Partner Terms. These Terms prevail over the general [Tencent Cloud International Partner Terms](#) in case of any conflict or inconsistency. Any term used but not defined in these Terms have the meaning given to them in the Tencent Cloud International Partner Terms, and any term in the Tencent Cloud International Partner Terms that has not been explicitly modified in these Tencent Cloud International Partner Academy Program Terms shall remain in full force and effect between you and Tencent

## 1. Program Content Offering.

By registering for and accessing a Program account, Tencent might offer you text, images, audio, video, or other content (excluding software) related to the Program (“Program Content Offering”), through the [Tencent Cloud International Partner Academy Program](#) site. Subject to your compliance with the Terms, Tencent grants you a limited, revocable, worldwide, non-exclusive, non-sublicensable, and non-transferrable license to view, download, and distribute (only for those materials we have made explicitly available for download) the Program Content Offering solely for the purpose of marketing Tencent Cloud services to your customers. You may not modify, alter, create derivative works of, license, sublicense, sell, resell or otherwise misuse any Program Content Offering unless expressly permitted by Tencent. Tencent and/or its licensors shall own and reserve all right, title, and interest in and to the Program Content Offering, and related intellectual property rights, and except as expressly described herein, no rights to the Program Content Offering, or related intellectual property rights are transferred or licensed pursuant to the Terms.

## 2. Account and Registration.

When you register for a Program account (“Account”) (whether in your capacity as a Partner and/or for and on behalf of your employees and representatives), you may be required to provide us with some information, such as your (and/or your employees’ and representatives’) name, postal address, email address, and other contact information. You agree that the information you provide to us (whether in your capacity as a Partner and/or of your employees and representatives, as applicable) is accurate and that you will keep it accurate and up-to-date at all times. You warrant and agree that you have obtained all necessary consents from the applicable employees and representatives to share

their personal information for purposes of the Program (including to apply for access to the Program and register for an Account).

We may deny you the right to create an account. Any entities or individuals that access the Program under your Account, and any of your employees and representatives who are authorized to access the Program with their own Account, are referred to in these Terms as “End Users.” You and your authorized End Users may access and use the Program Content Offering in accordance with these Terms during the Term (as defined below). If you or your End Users become aware of any unauthorized use of your or your End Users’ Account or the password for your or your End Users’ Account, you will notify Tencent as promptly as possible. You are responsible for safeguarding any and all of your and your End Users’ Account details and access credentials. Any breach of these Terms or any use of your and/or your End Users’ Account by anyone to whom you disclose your username or password will be treated as if the breach or use had been carried out by you, and will not relieve you of your obligations to us.

### **3. Modification of Program.**

Tencent will have the right to modify the features of, cease the offering of, amend the terms and conditions of, or make any other adjustments or modifications to the Program, any time as deemed necessary without prior written notice to you.

### **4. Feedback.**

If you provide Tencent or its Affiliates with any suggestions, ideas, comments, or other feedback about the Program (including the Program Content Offering) (“Feedback”), Tencent and its Affiliates may use and otherwise exploit that Feedback without restriction and without obligation to you; provided, however, Tencent will not publicly disclose Feedback in a way that is identifiable to you.

### **5. Disclaimers.**

THE PROGRAM CONTENT OFFERING IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TENCENT SPECIFICALLY DISCLAIM ANY AND ALL WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. TENCENT FURTHER DISCLAIM ANY AND ALL LIABILITY RELATED TO YOUR ACCESS OR USE OF PROGRAM CONTENT OFFERING OR ANY RELATED CONTENT OR YOUR PARTICIPATION IN THE PROGRAM. YOU ACKNOWLEDGE AND AGREE THAT ANY ACCESS TO OR USE OF THE PROGRAM CONTENT OFFERING OR ANY PARTICIPATION IN THE PROGRAM IS AT YOUR OWN RISK.

### **6. Limitation of Liability.**

(A) TO THE MAXIMUM EXTENT PERMITTED BY LAW, TENCENT SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, OR ANY LOSS OF PROFITS OR REVENUES, WHETHER INCURRED DIRECTLY OR INDIRECTLY, OR ANY LOSS OF DATA, USE, GOODWILL, OR OTHER INTANGIBLE LOSSES, RESULTING FROM YOUR AND/OR YOUR END USERS’ ACCESS TO OR



USE OF OR INABILITY TO ACCESS OR USE THE PROGRAM CONTENT OFFERING OR YOUR AND/OR YOUR END USERS' PARTICIPATION IN THE PROGRAM. IN NO EVENT SHALL TENCENT'S AGGREGATE LIABILITY FOR ALL CLAIMS RELATED TO THE PROGRAM EXCEED ONE HUNDRED U.S. DOLLARS (\$100).

(B) YOU ACKNOWLEDGE AND AGREE THAT THE DISCLAIMERS AND THE LIMITATIONS OF LIABILITY SET FORTH IN THIS TERMS OF USE REFLECT A REASONABLE AND FAIR ALLOCATION OF RISK BETWEEN YOU AND TENCENT, AND THAT THESE LIMITATIONS ARE AN ESSENTIAL BASIS TO TENCENT'S ABILITY TO MAKE THE PROGRAM AND/OR THE PROGRAM CONTENT OFFERING AVAILABLE TO YOU ON AN ECONOMICALLY FEASIBLE BASIS.

(C) YOU AGREE THAT ANY CAUSE OF ACTION RELATED TO THE PROGRAM MUST COMMENCE WITHIN ONE (1) YEAR AFTER THE CAUSE OF ACTION ACCRUES. OTHERWISE, SUCH CAUSE OF ACTION IS PERMANENTLY BARRED.

## **7. Indemnification.**

You will indemnify, defend, and hold harmless Tencent, its Affiliates, and each of their respective licensors, employees, officers and directors from any and all claims, liabilities, expenses, and damages, including reasonable attorneys' fees and costs, made by any third party related to: (a) your and your End Users' participation in the Program or use or attempted use of the Program Content Offering in violation of the Terms; or (b) your violation of any law or rights of any third party.

## **8. Term and Termination; Suspension.**

(a) These Terms will commence when you accept these Terms or first download, install, access, or use the Program Content Offering and continue until terminated as set forth in Tencent Cloud International Partner Terms ("Term").

(b) Without prejudice and in addition to its rights and remedies at law or equity, Tencent may suspend or terminate the Terms and/or limit or restrict your rights to participate in the Program or use Program Content Offering, immediately upon written notice to you if, in the reasonable opinion of Tencent, you have engaged in any of the following: (a) breached or prejudiced the Terms; (b) used the Program Content Offering in a way that poses a security risk to the Tencent platform or any third party; (c) used the Program Content Offering in a way that subjects, or will subject, Tencent to liability; (d) engaged in any fraudulent, deceptive or unlawful act; or (e) become the subject of any bankruptcy, reorganization, liquidation, dissolution or similar proceedings.

# 腾讯云国际合作伙伴学堂申请表范例

最近更新时间：2022-05-07 12:48:06

## Application Form

Partner Company Name	Tencent Holdings Ltd.
Tencent Cloud Account ID of Applicant	100000750XXX
<p><input checked="" type="checkbox"/> I confirm that I have read and agree to the <a href="#">Tencent Cloud Partner Program Terms and Conditions</a> and <a href="#">Tencent Cloud International Partner Academy Program Terms of Service</a>.</p> <p><input checked="" type="checkbox"/> I have read and acknowledge the <a href="#">Tencent Cloud International Partner Academy Privacy Notice</a>.</p> <p><input checked="" type="checkbox"/> I confirm that I have obtained the explicit consent from the applicant employee(s) and/or representative(s) to share their personal information to Tencent in accordance with <a href="#">Tencent Cloud International Partner Academy Privacy Notice</a>, and that they have read and acknowledge the <a href="#">Tencent Cloud International Partner Academy Privacy Notice</a>.</p>	
<p>Applicant Signature</p> <p>XXXX</p>	<p>Tencent Cloud Approval Result</p> <p><input type="checkbox"/> Approve</p> <p><input type="checkbox"/> Disapprove</p> <p>Reason of disapprove: _____</p>
<p>Partner Company Chop/Signature</p> <p>XXXX</p>	

- [Tencent Cloud Partner Program Terms and Conditions](#)
- [Tencent Cloud International Partner Academy Program Terms of Service](#)
- [Tencent Cloud International Partner Academy Privacy Notice](#)

# 访问管理

## 访问管理概述

最近更新时间：2022-11-15 12:06:26

注意：

若您不需要对子账户进行渠道合作伙伴相关资源的访问管理，您可以跳过此章节。跳过这些部分不会影响您对文档中其余部分的理解和使用。

如果您在腾讯云中使用到了云服务器（Cloud Virtual Machine, CVM）、私有网络、数据库等服务，这些服务由不同的人管理，但都共享您的云账号密钥，将存在以下问题：

- 您的密钥由多人共享，泄密风险高。
- 您无法限制其它人的访问权限，易产生误操作造成安全风险。

此时，您可以通过子帐号来实现不同的人管理不同的服务，以规避上述问题。默认情况下，子帐号没有使用渠道合作伙伴的权限。因此，我们就需要创建策略来允许子帐号使用他们所需要的资源或权限。

访问管理（Cloud Access Management, CAM）是腾讯云提供的一套 Web 服务，它主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。通过 CAM，您可以创建、管理和销毁用户（组），并通过身份管理和策略管理控制哪些人可以使用哪些腾讯云资源。

当使用 CAM 时，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。

- 有关 CAM 子用户的更多相关使用信息，请参照 [子用户](#)。
- 有关 CAM 策略的更多相关使用信息，请参照 [策略](#)。

# 预设策略

最近更新时间：2023-01-03 18:33:31

注意：

本文档主要介绍 渠道合作伙伴 访问管理功能的相关内容，其他产品访问管理相关内容请参见 [支持 CAM 的产品](#)。

渠道合作伙伴访问管理实质上是子帐号与策略进行绑定，或者说将策略授予子帐号。开发者可以在控制台上直接使用预设策略来实现一些简单的授权操作。

渠道合作伙伴目前提供了以下预设策略：

策略名称	策略描述
QcloudIntlpartnersmgtFullAccess	渠道合作伙伴全读写访问权限
QcloudIntlpartnersmgtReadOnlyaccess	渠道合作伙伴只读访问权限

## 预设策略使用示例

### 新建拥有渠道合作伙伴权限的子帐号

- 以腾讯云 [主帐号](#) 的身份访问 CAM 控制台的 [用户列表](#)，单击**新建用户**。
- 在**新建用户**页面选择**自定义创建**，进入**新建子用户**页面。

说明：

请根据 [CAM 自定义创建子用户](#) 的操作指引完成**设置用户权限**之前的步骤。

- 在“设置用户权限”页面：

- 搜索并勾选预设策略 'Intlpartnersmgt' 。
- 单击\*\*下一步\*\*。

- 在“审阅信息和权限”分栏下单击**完成**，完成子用户的创建，在成功页面下载并保管好孩子用户的登录链接和安全凭证，其中包含的信息如下表：

信息	来源	作用	是否必须保存
----	----	----	--------

信息	来源	作用	是否必须保存
登录链接	在页面中复制	方便登录控制台，省略填写主帐号的步骤	否
用户名	安全凭证 CSV 文件	登录控制台时填写	是
密码	安全凭证 CSV 文件	登录控制台时填写	是
SecretId	安全凭证 CSV 文件	调用服务端 API 时使用，详见 <a href="#">访问密钥</a>	是
SecretKey	安全凭证 CSV 文件	调用服务端 API 时使用，详见 <a href="#">访问密钥</a>	是

5、将上述登录链接和安全凭证提供给被授权方，后者即可使用该子用户对渠道合作伙伴做所有操作，包括访问渠道合作伙伴控制台、请求渠道合作伙伴服务端 API 等。

### 将渠道合作伙伴权限授予已存在的子帐号

- 1、以腾讯云 [主帐号](#) 的身份访问 CAM 控制台的 [用户列表](#)，单击想要进行授权的子帐号。
- 2、单击[用户详情](#)页面权限栏的**添加策略**，如果子帐号的权限**非空**，则单击**关联策略**。
- 3、选择**从策略列表中选取策略关联**，搜索并勾选预设策略 "Intlpartnersmgt"。后续按页面提示完成授权流程即可。

### 解除子帐号的渠道合作伙伴权限

- 1、以腾讯云[主帐号](#)的身份访问 CAM 控制台的[用户列表](#)，单击想要解除授权的子帐号。
- 2、在[用户详情](#)页面权限栏找到预设策略 "Intlpartnersmgt"，单击右侧的**解除**。按页面提示完成解除授权流程即可。

# 支持访问管理的 API 接口

最近更新时间：2022-11-15 12:06:26

## 基本信息

CAM 中产品名	CAM 中简称	授权粒度
渠道合作伙伴	Intlpartnersmgt	操作级

### 说明

云产品的授权粒度按照粒度粗细分为服务级、操作级和资源级三个级别。

- 服务级：定义对服务的整体是否拥有访问权限，分为允许对服务拥有全部操作权限或者拒绝对服务拥有全部操作权限。服务级授权粒度的云产品，不支持对具体的接口进行授权。
- 操作级：定义对服务的特定接口（API）是否拥有访问权限，例如：授权某账号对代金券进行只读操作。
- 资源级：定义对特定资源是否有访问权限，这是最细的授权粒度，例如：授权某账号仅读写操作某个代金券。能支持资源级接口授权的产品，则会被认定为资源级授权粒度。

## 接口授权粒度

- 资源级接口：此类型接口支持对某一个具体特定的资源进行授权。
- 操作级接口：此类型接口不支持对某一个特定的资源进行授权。

资源级接口在鉴权时，云产品会将具体的资源六段式传给 CAM 鉴权，故支持对某一个具体特定的资源进行授权和鉴权。

操作级接口在鉴权时，云产品不会将具体的资源六段式传给 CAM 鉴权，只会传递任意资源 \*。因此授权时策略语法若限定了具体的资源，鉴权时此接口不传递该资源，CAM 会判断此接口不在授权范围，会判断为无权限。