

RiskControlEngine

RCE Policy

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

RCE Policy

Privacy Policy

Data Processing And Security Agreement

RCE Policy

Privacy Policy

Last updated : 2022-03-21 14:48:33

1. INTRODUCTION

This Module applies if you use the Risk Control Engine (“**Feature**”). This Module is incorporated into the privacy policy located at (“[Privacy Policy](#)”). Terms used but not defined in this Module shall have the meaning given to them in the Privacy Policy. In the event of any conflict between the Privacy Policy and this Module, this Module shall apply to the extent of the inconsistency.

2. CONTROLLERSHIP

The controller of the personal information described in this Module is as specified in the Privacy Policy.

3. AVAILABILITY

This Feature is available to users globally but primarily intended for users located in the same country/region as the selected service region for optimal performance.

4. HOW WE USE PERSONAL INFORMATION

We will use the information in the following ways and in accordance with the following legal basis:

Personal Information	Use	Legal Basis
----------------------	-----	-------------

Personal Information	Use	Legal Basis
<p>Contact information: Name, phone number, email, mailing address.</p> <p>Transaction data: emails, items purchased, prices paid, order status, refund information, partial credit card details namely: first 6 numbers of credit card number, validity duration, name of card holder, MD5 of card number.</p> <p>Account information: account and preference information on the website or App.</p>	We use this information to provide you with the functions of the Feature.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
<p>Log and API call information: User IP, call volume, APPID, UIN, time duration-consuming, timestamp.</p>	We use this information to provide you with the functions of the Feature.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
<p>SDK data:</p> <p>1. Browser, device and connection data: Information of personal computer or mobile device accessing a customer's website, including browser, device model and operating system, and unique device identifier.</p> <p>2. Behavioral data: Information about activities on the business website or APP, such as access time and frequency, pages viewed, distribution of swipes on screens and stay time.</p>	We use this information to provide you with the functions of the Feature.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.

5. HOW WE SHARE AND STORE PERSONAL INFORMATION

As specified in the Privacy Policy.

6. DATA RETENTION

We will retain personal information in accordance with the following:

Personal Information	Retention Policy
----------------------	------------------

Personal Information	Retention Policy
<p>Contact information: Name, phone number, email, mailing address.</p> <p>Transaction data: emails, items purchased, prices paid, order status, refund information.</p> <p>Account information: account and preference information on the website or App.</p>	<p>We retain such data for as long as you use the Feature. When your use of the Feature is terminated, we will delete this data within 5 days.</p>
<p>Log and API call information: User IP, call volume, APPID, UIN, time duration-consuming, timestamp.</p>	<p>This data will be automatically deleted after 180 days of first being recorded.</p>
<p>SDK data:</p> <ol style="list-style-type: none">1. Browser, device and connection data: Information of personal computer or mobile device accessing a customer's website, including browser, device model and operating system, and unique device identifier.2. Behavioral data: Information about activities on the business website or APP, such as access time and frequency, pages viewed and stay time.	<p>We retain such data for as long as you use the Feature. When your use of the Feature is terminated, we will delete this data within 5 days.</p>

Data Processing And Security Agreement

Last updated : 2022-03-21 14:48:54

1. BACKGROUND

This Module applies if you use Risk Control Engine (“**Feature**”). This Module is incorporated into the Data Privacy and Security Agreement located at (“**DPSA**”). Terms used but not defined in this Module shall have the meaning given to them in the DPSA. In the event of any conflict between the DPSA and this Module, this Module shall apply to the extent of the inconsistency.

2. PROCESSING

We will process the following data in connection with the Feature:

Personal Information	Use
Log data: API call information: User IP, call volume, APPID, UIN, time duration and timestamp	We use this data for the purposes of providing the Feature to you and enable us to undertake statistical analysis for troubleshooting.
SDK data: 1. Browser, device and connection data: Information of personal computer or mobile device accessing a customer’s website, including browser, device model and operating system, and unique device identifier. 2. Behavioral data: Information about activities on the business website or APP, such as access time and frequency, pages viewed, distribution of swipes on screens and stay time.	We process this data to allow a comprehensive assessment of the risk results and to provide the functionality of the Feature to you.

3. SERVICE REGION

As specified in the DPSA.

4. SUB-PROCESSORS

As specified in the DPSA.

5. DATA RETENTION

We will store personal data processed in connection with the Feature as follows:

Personal Information	Retention Policy
Log Data	Log data will be automatically deleted after 180 days of first being recorded.
SDK Data	We retain such data for as long as you use the Feature. When your use of the Feature is terminated, we will delete this data within 5 days.

You can request deletion of such personal data in accordance with the DPSA.

6. SPECIAL CONDITIONS

You must ensure that this Feature is only used by end users who are of at least the minimum age at which an individual can consent to the processing of their personal data. This may be different depending on the jurisdiction in which an end user is located.