# Tencent Cloud

# Privacy White Paper

2022.10

# Introduction

In recent years, the Internet, cloud computing, artificial intelligence, blockchain and other technologies have accelerated innovation, and the digital economy has increasingly integrated into all fields of social development, becoming a key force to change the global competitive landscape. Many countries around the world have successively released and updated laws and regulations related to personal data and regulated the processing of personal data via regulators and industry associations, so as to effectively protect the information owned by natural persons. Since then, how organizations and institutions deal with data in compliance with laws and regulations has become an urgent challenge and issue to be solved.

In the process of providing services, cloud service providers not only ensure the security of the cloud platform, but also ensure the processing of personal data in compliance with laws and regulations. Tencent Cloud has been adhering to the principle of "tech for good" of Tencent and is committed to building a secure and reliable cloud platform to ensure the protection of customers' personal data on the cloud in a compliant way. At the current stage, Tencent Cloud has a specific security technology team, security compliance team, and legal expert team, which focus on the research of data security and privacy compliance, continue to follow up on global data security and privacy protection related laws and regulations, integrate the relevant requirements into privacy management and practice in a timely manner, and ensure the timeliness of Tencent Cloud's privacy management system and practices.

When talking about the topic of privacy compliance, we always face two issues, "data security" and "privacy compliance". Data security mainly focuses on ensuring the security of data in the whole life cycle via security management and security technology, while privacy compliance pays more attention to compliance management under privacy related laws and regulations and regulatory requirements of various countries, as well as the transparency and compliance of data in the process of use, with the aim of protecting the privacy of natural persons. For the management and practice of Tencent Cloud in "data security", please refer to "Tencent Cloud Security White Paper" and "Tencent Cloud Data Security White Paper". However, in this white paper, only "privacy compliance" is focused on to make the relevant statements.

This white paper will start with how Tencent Cloud practices privacy compliance. On the one hand, it will introduce how Tencent Cloud itself conducts privacy compliance management. On the other hand, it will introduce how Tencent Cloud can help customers meet their applicable privacy compliance obligations under the responsibility sharing model to help customers achieve greater business value.

# Disclaimer

This white paper is intended as a source of information only to Tencent Cloud customers for better understanding. However, the information contained in this white paper should not be construed as legal advice or as a contractual commitment, and shall not amount to, operate as or be construed as any guarantee, representation, warranty or undertaking. This white paper does not substitute or broaden the scope of any provisions of relevant service contracts. This white paper contains statements, which represent assessment by Tencent Cloud, but do not attempt to analyze all relevant issues pertaining to applicable law or customers' business or guarantee any particular outcome or result. This white paper does not entitle any person to sue Tencent Cloud. Any description of internationally recognized standards or laws is of a general nature and is not intended to provide a comprehensive summary thereof.

# CONTEXT

# 1.Tencent Cloud introduction

Tencent Cloud is a cloud computing brand that Tencent strives to build. It provides globally leading cloud computing, artificial intelligence, and other products and services to enterprises, organizations, institutions and individual developers around the world. After accumulating technical expertise for more than 20 years, Tencent has accumulated vast service experience in the rapid development of QQ, WeChat, and other To C products, building a solid cloud computing foundation for Tencent Cloud. Playing a role as the technology base and connector of Tencent's industrial Internet, Tencent Cloud uses its outstanding technical capabilities to create a wide range of industry solutions, build an open and win-win cloud ecosystem, and help all industries and sectors realize digital transformation.

Tencent Cloud has always taken "compliance" as its first priority. Tencent Cloud has a special team of legal experts, who are responsible for continuously following up on laws and regulations on global data security and privacy compliance and integrating the latest applicable compliance requirements into compliance management in a timely manner. Tencent Cloud always adheres to the Privacy by Design & Default (PbD), and strictly integrates privacy compliance requirements into the design and development of products and services to achieve functional compliance of cloud products and services.

## 1.1 Tencent Cloud infrastructures and products

So far, Tencent Cloud has built more than 400 products in different categories, ranging from infrastructures to industry applications, including computing, storage, database, security, big data, artificial intelligence, Internet of things, enterprise applications, industry applications, and developer applications, to provide customers with a full range of cloud solutions.
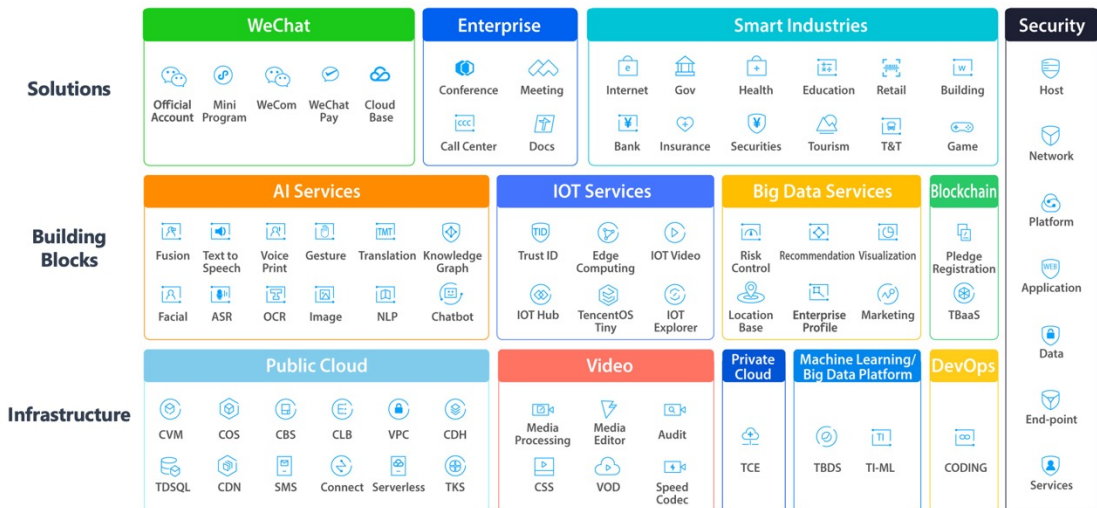


Tencent Cloud Product Matrix

Tencent Cloud also leads in the global cloud computing service providers with its unique cloud capabilities in infrastructures. Tencent Cloud has more than one million servers deployed around the world, more than 2800 acceleration nodes, data storage scale of EB level, and more than 160T bandwidth reserves. In addition, Tencent Cloud has data centers in 26 geographical regions around the world, including Chinese Mainland, Asia Pacific Region, North America and Europe, and operates in 70 availablility zones to provide strong technical support for customers. With the help of Tencent Cloud's globalized data center resources and integrated cloud computing technology capabilities, customers can provide the ability to share information across multiple geographical regions and quickly expand their businesses to a broader market.
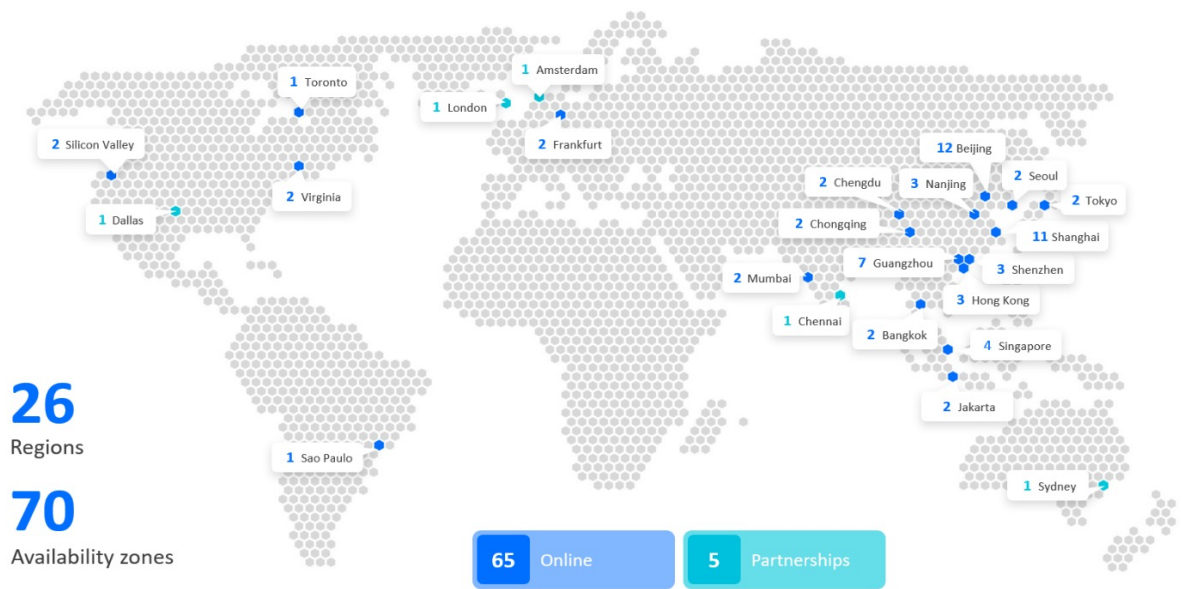
Tencent Cloud IDC Distribution Chart

## 1.2 Tencent Cloud security qualification certification

● **Tencent Cloud has passed a number of authoritative certifications**

Compliance is the basis for the development of Tencent Cloud. Tencent Cloud complies with the compliance requirements of different countries and industries and strives to build cloud services that are trustworthy to customers. Meanwhile, Tencent Cloud also actively participates in the formulation and promotion of industry security standards, adheres to compliance for service, and builds and operates a secure and reliable cloud ecosystem.

Tencent Cloud has established six systems including an information security management system, privacy information management system, quality management system, IT service management system, business continuity management system, and supply chain security management system in accordance with internationally recognized information security and

IT management and control standards, and has passed the evaluation of third-party authorized evaluation institutions every year to provide customers with cloud services audited and certified by authoritative third-party certification institutions. Tencent Cloud not only strictly abides by applicable laws and regulations and industry supervisions in business operation areas, but also follows the best practices recognized by the industry, constantly improves the relevant management system, improves the security control level of Tencent Cloud, and better demonstrates Tencent Cloud's compliance ability to customers.

Up to now, Tencent Cloud has obtained more than 100 security compliance certifications or qualifications via independent third-party audits or evaluations, proving that the security management construction of Tencent Cloud meets the relevant certification standards or best industry practices. For more information about Tencent Cloud's compliance, please refer to Tencent Cloud compliance page.

**ISO27001 Certification**
Tencent Cloud's information security management system has been certified with ISO27001.

**ISO9001 Certification**
Tencent Cloud's quality management system has been certified with ISO9001.

**ISO27017 Certification**
ISO27017 offers cloud service providers with guidelines for cloud computing security controls and implementation.

**ISO27701 Certification**
Tencent Cloud is certified by a third-party authority and meets the requirements of the ISO 27701 Privacy Security Management System.

**ISO27018 Certification**
Tencent Cloud attained ISO 27018 certification: Code of practice for protection of PII in public clouds.

**German C5 Audit**
Tencent Cloud has passed the German C5:2020 basic and additional audit criteria.

**CSA STAR Cloud Security Certification**
Tencent Cloud was conferred the CSA Star cloud security certification with a gold rating.

**PCI DSS**
Tencent Cloud has attained the qualification of a PCI DSS Grade 1 service provider.

**SOC Audit**
Tencent Cloud follows the 2017 version of the trust services criteria issued by the American Institute of Certified Public Accountants (AICPA) .

**Korea KISMS Certification**
Tencent Cloud has achieved the Korean Information Security Protection Management System certification, becoming the first certified cloud provider in China.

**Singapore MTCS Certification**
Tencent Cloud has achieved the Singapore Multi-Tier Cloud Security Standard Level-3 certification.

**TISAX Audit**
Tencent Cloud passed the TISAX- German automotive industry 's highest level of information security access (AL3) review.

Selected Security Compliance Qualifications

● **Tencent Cloud privacy compliance certification**

Tencent Cloud attaches special importance to privacy compliance management, and plans, establishes, implements, maintains, and continually improves Tencent Cloud's privacy protection management system according to the following requirements for privacy compliance certification and qualification of multiple industry authorities, so as to ensure that Tencent Cloud's privacy protection level can reach the industry's recognized standards.

Currently Tencent Cloud has passed the privacy compliance certifications and qualifications as follows:



ISO/IEC 27701 is an extension of ISO/IEC 27001 and ISO/IEC 27002 in the field of privacy protection. It provides guidelines in the establishment, implementation, maintenance and continual improvement of privacy information management system (PIMS). ISO/IEC 27701 can be used for organizations of any type and any scale,

including public/private companies, government entities and non-profit organizations. It systematically outlines the concepts, requirements, and implementation guidelines of a privacy security management system for the first time in the world.



Released in 2014, ISO/IEC 27018 is the industry's first international code of conduct related to privacy in the field of cloud computing. By passing ISO/IEC 27018 certification, it can be proved that enterprises have reached high standards of best industry practices in protecting data, intellectual property rights, documents and cloud IT security.



BS10012 was released by the British Standards Institution (BSI) and came into force on March 31, 2017, replacing the version released in 2009. The 2017 edition of BS10012 has been updated and revised according to the European General Data Protection Regulation (GDPR) to make the requirements of BS10012 consistent with those of GDPR.



Based on ISO/IEC 27002 control practice rules and ISO related security standards and specifications, ISO/IEC 29151 provides a series of guidelines for information security and PII (personally identifiable information) protection control, and guides organizations to select control measures that match PII specific processing according to the results of

risk analysis, so as to develop a comprehensive control system and reduce the risk of privacy data leakage.

# 2. Overview of Tencent Cloud privacy management

## 2.1 Terms

- **Customer:** The purchaser of Tencent Cloud products or services, which may be an enterprise or an individual, forming a business partnership with Tencent Cloud in form and in fact.

- **"Personal data"** is information relating to natural persons who (a) can be identified or are identifiable directly from the information in question; or (b) who can be indirectly identified from that information in combination with other information. Examples of personal data include a name, date of birth, passport number, national identification number, open ID, IP address, location data, cookie identifier, email address etc.

- **'Data Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. Examples of processing include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Virtually any action with Personal Data is Data Processing.

- **Customer data:** Customer data includes two types of data. One is the data generated by customers' registration, inquiry, or interaction with Tencent Cloud in the process of using and purchasing Tencent Cloud services to carry out their own business, and Tencent Cloud is the controller of this type of data. The other one is the business data controlled by the customer, which refers to the content data stored on the side of Tencent Cloud for the customer's business, including but not limited to text, audio, video, or image, and Tencent Cloud is the processor of this type of data.

- **'Data Controller'** means a person which, alone or jointly with others, determines the purposes and means of the processing of personal data. Such person can be a natural or legal person, public authority, agency or other body.

- **'Data Processor'** means a person which processes personal data on behalf of the controller. Data Processors (as Data Controllers) can be natural or legal persons, public authorities, agencies or other bodies. The key difference from a Data Controller is that a Data Processor is unable to decide the purpose or means of Data Processing.

- **'Data Subject'** is a natural person who is identified or identifiable by his or her Personal Data.

## 2.2    Tencent Cloud privacy protection concept

Tencent Cloud documents (including the Tencent Cloud Service Agreement) set forth guarantees that Tencent Cloud processes data for the provision of Tencent Cloud services and otherwise in accordance with applicable laws and regulations. On this basis, Tencent Cloud takes personal data compliance as the primary factor in the process of service provision, and takes generally recognized personal data compliance principles (such as legality, fairness, transparency, purpose limitation, data minimization, integrity, accuracy, confidentiality, accountability, etc.) as the guiding concept of privacy compliance, which is integrated into all links of product design and development and the whole life cycle of personal data, making privacy compliance an inherent attribute of products. Moreover, Tencent Cloud strictly complies with privacy protection laws and regulations of applicable countries and regions in the world. Tencent Cloud's many years of security experience and accumulation ensures the security of the cloud platform infrastructure and provides a solid foundation for customers' business privacy compliance.

## 2.3    Tencent Cloud privacy protection culture

● **Cultural dissemination and training**

Tencent Cloud attaches great importance to the training and dissemination of employees' privacy compliance awareness and organizes various security awareness training from multiple dimensions and aspects to comprehensively improve employees' privacy security compliance awareness.

In addition to formulating various systems to implement privacy compliance requirements for employees to learn, Tencent Cloud has also taken action to promote security in key stages, specific scenarios and relevant positions, including but not limited to enrollment training for new employees, and professional guidance and courses for key positions, so as to help employees better understand privacy compliance requirements and practices in specific jobs and scenes.

Tencent Cloud also disseminates privacy compliance knowledge to employees through company privacy days, celebrity lectures, internal forums, its official account, etc., to draw all employees' attention to privacy compliance.

● **Academic research and expert team**

Tencent Cloud actively participates in the formulation of various cloud computing security standards, actively participates in various industry exchanges and academic discussion activities related to privacy compliance, continually follows up the latest changes in regulatory policies and law enforcement trends, and updates the relevant requirements for privacy compliance management in a timely way to ensure the timeliness of Tencent Cloud's privacy protection management system.

Tencent Cloud focuses on cloud security technology research and cloud network security innovation and has a professional security technology team to support Tencent Cloud security architecture design, security protection, operation, and maintenance.

Tencent Cloud has set up a security compliance team and a legal expert team, which are specifically responsible for coordinating privacy compliance work in jurisdictions where we operate, participating in the formulation of privacy compliance management policies and strategies and providing privacy compliance support depending on the business development stage and the specific situation of the country or region, so as to achieve the privacy compliance of Tencent Cloud products and businesses. These teams are empowered with decision-making power and escalation rights reflecting legal requirements in the jurisdictions in which Tencent Cloud's services are available.

## 2.4 Tencent Cloud privacy management system

Tencent Cloud operates in many jurisdictions (with often conflicting approach) and in the constantly evolving legal and technical environment. We strive to ensure compliance with key standards (e.g. ISO 27701, ISO 27018) and applicable laws, including the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), the PRC Personal Information Protection Law (PIPL), The Singapore Personal Data Protection Act (PDPA), and many others.

Tencent Cloud has established its own privacy protection compliance guidelines and policies in accordance with applicable laws, regulations, and standards, formulated corresponding management systems and methods, and kept relevant records related to personal data processing, so as to manage the full life cycle of personal data in a traceable way. Meanwhile, Tencent Cloud implements established privacy protection compliance guidelines and policies, as well as corresponding management systems and methods, to ensure the

effective implementation of the privacy protection management system in the practice of compliance and constantly improve it. Tencent Cloud also continues to strengthen the training and dissemination of privacy management system, ensures employees' understanding of and compliance with the relevant management requirements, improves its personal data protection capabilities, and strengthens the privacy compliance awareness of all staff.

## ● 2.4.1 Organization management

### Privacy compliance management organization

Tencent has established privacy compliance management organizations, including the data privacy protection center. Tencent Cloud's privacy compliance work is carried out strictly under the guidance of the organization, which is mainly responsible for privacy protection and compliance management and follows up on applicable laws, regulations, and standards, formulates personal data compliance management norms and process systems, reviews privacy compliance risks in business, produces compliance opinions, promotes privacy related certification, provides data privacy protection support depending on business development, increases the company's attention to privacy protection and compliance awareness, and reduces risks in business operations.

With its establishment, the organization unifies the command and deployment of the company's personal data compliance work and effectively guides and evaluates the work of the project implementation team. It ensures the implementation of regulatory requirements, implements the company's unified requirements and objectives, and arranges specific data compliance tasks accordingly; it, in accordance with the requirements of compliance, implements all types of important issues in the process, organizes discussions on the strategy, reaches consensuses, and pushes for a resolution.; and it conducts regular privacy compliance audits for businesses, guides and supervises the specific implementation and completion of privacy compliance corrections, and ensures that compliance requirements are met as soon as possible.

### Appointing a Data Protection Officer

Tencent has appointed a Data Protection Officer (DPO) to actively participate in the establishment of a privacy protection management system, participate in compliance audits, and on the basis of having ensured public trust and corporate responsibility, assist Tencent Cloud in using the data to promote innovation and to establish privacy protection compliance with customers and partners.

### ● 2.4.2 Process management

Tencent Cloud has adopted globally applicable privacy compliance laws and regulations as the baseline. Examples of applicable laws include: the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Information Protection Law (PIPL), The Singapore Personal Data Protection Act (PDPA), and many others. By integrating ISO 27701 and ISO 27018 and other international standards, it has established a complete set of management processes related to Tencent Cloud's personal data protection, including privacy protection management standards, personal data use procedures, privacy risk management procedures, etc. Tencent Cloud carries out compliance control over relevant data throughout its life cycle in accordance with established management processes related to personal data processing.

### Product privacy compliance review

Tencent Cloud strictly abides by applicable privacy laws and regulations and effectively implements compliance requirements in the cloud products and services it provides. In the actual business scenario, in order to reduce the privacy compliance risk of Tencent Cloud, Tencent Cloud requires each product to undergo a pre-release privacy assessment, to inform customer about how their data is processed by Tencent Cloud via the Privacy Policy (PP) and Data Processing and Security Agreement (DPSA)  on the official website and how Tencent Cloud implements privacy protection principles and obligations in business activities as a personal data controller and a personal data processor.

### ● 2.4.3 Technical management

In terms of privacy security, Tencent Cloud has always adhered to the concept of Privacy by Design & Default (PbD) to create a management system for Tencent Cloud and its products that runs through the whole data life cycle. Relying on research on network attack and defense and security operation experience of Tencent Cloud, we provide Tencent Cloud customers with constant security and stable compliance services. Furthermore, the technical team has been committed to studying various privacy protection technologies, such as confidential computing and homomorphic encryption, to accumulate privacy protection technical capabilities and provide a more solid technical base for customers' personal data compliance.

# 3. How Tencent Cloud practises privacy compliance when it is a data controller?

From the perspective of privacy compliance, Tencent Cloud can be roughly divided into two categories with regard to its data processing role:

- **Data controller:** Via the official website of Tencent Cloud, it collects information provided by customers when registering for Tencent Cloud services, as well as data generated from interaction with Tencent Cloud in this process. In this case, Tencent Cloud will fulfill the obligations of a data controller in accordance with the Tencent Cloud Privacy Policy (PP). Considering the nature of the service, Tencent Cloud also acts as a controller for certain data transferred to it when required.

- **Data processor:** Customers use Tencent Cloud products or services to process the data collected by customers based on their own business purposes. In such case, Tencent Cloud will not only be responsible for the function and security of products or services, but also fulfill the obligations of a data processor in accordance with the Tencent Cloud Data Processing and Security Agreement (DPSA).

## 3.1    Tencent Cloud as a data controller

From When Tencent Cloud is a data controller, it collects the relevant information generated by customers' use and purchase of Tencent Cloud services and their interactions with Tencent Cloud, which may include:

### ● Information offered by customers

When customers inquire about Tencent Cloud services, use Tencent Cloud services or contact Tencent Cloud by phone, email or other means, they may provide the relevant information to Tencent Cloud. Examples include information provided by customers when registering for Tencent Cloud services (or acting as the company's business representative to register for services for enterprise customers), such as the customer's name, email address, ID card with photo, phone number and other information that helps Tencent Cloud register customers to use the services.

### ● Information collected by Tencent Cloud when customers use services

When customers use services via the Tencent Cloud portal, Tencent Cloud will automatically collect some information from customers, including IP addresses, customer agents, and information related to the use of Tencent Cloud services, such as access logs, website access requests, uploads and downloads.

- **Information generated from customer's interactions with Tencent Cloud:**

Tencent Cloud also collects and stores information every time customers interact with Tencent Cloud (for example, when customers communicate with Tencent Cloud via email, activate new services, or fill out forms on Tencent Cloud's website). We also store information about the services our customers have purchased, such as activation codes, purchase dates, and information about any support issues.

## 3.2 Privacy management practice of Tencent Cloud as a data controller

- ## 3.2.1 Privacy protection principles

As a data controller, Tencent Cloud always handles customers' personal data according to the following seven principles:

### Product privacy compliance review

- **Legal, fair, and transparent:** When Tencent Cloud collects your data, it will inform you by a privacy statement, which lists the type of data and field information we must collect to provide you with services, and we will collect and process your relevant data only where there is legal basis, including consent.

- **Purpose limitation:** Tencent Cloud's privacy statement clearly introduces the purpose of various types of data collection and processing, and we will not process the relevant data in a manner which is incompatible with those purposes.

- **Minimum data:** Tencent Cloud will only collect the type of data and field information that must be collected to provide you with services but will not collect excess data.

- **Accuracy:** Tencent Cloud has ensured the accuracy of data transmitted to Tencent Cloud via access control, integrity authentication, and other means. Moreover, Tencent Cloud also provides customers with communication channels for customers to correct or delete the relevant inaccurate data by themselves.

- **Storage restrictions:** Tencent Cloud's privacy statement introduces the mechanisms used for the retention of each type of data, and Tencent Cloud will not retain data beyond the period which is necessary for the purposes or applicable law.

- **Integrity, accuracy, and confidentiality**: Tencent Cloud has adopted encryption, anonymization, access control, monitoring and management and other technical means to ensure that customer data will not be accessed or processed without authorization, so as to minimize the possibility of data tampering, loss, or damage.

- **Accountability:** Data impact analysis is needed for each cloud service / product of Tencent Cloud, and records of completed activities will be left for data processing activities.

- ## 3.2.2 Key areas of privacy compliance

Tencent Cloud complies with the requirements of laws and regulations to perform relevant obligations and complies with the data processing principles under the privacy compliance system to establish specific behavior mechanisms to ensure the security of personal data. In practice, Tencent Cloud mainly focuses on the full life cycle management of personal data, and introduces key compliance requirements such as Privacy by Design & Default (PbD), data subject right response, personal data disclosure, etc.

**Data Collection**

- **Minimize collection**

Tencent Cloud will clarify the purpose of data processing, data types, and personnel with access rights and third parties, and conduct compliance assessment to ensure that only data related to the purpose of data processing are collected.

- **Adequate notice before data collection**

Before collecting the relevant information generated from the customers' use and purchase of Tencent Cloud services and their interactions with Tencent Cloud, we will inform customers of the relevant information about data collection and processing with clear, definite and easy-to-understand privacy policies.

- **Confirm legal basis before data collection**

On the premise of the above notification to the data subject and other applicable legal basis, Tencent Cloud also obtains the explicit and voluntary consent of the data subject to data collection via the registration interface.

**Data Storage**

- **Data storage and encryption**

Tencent Cloud encrypts the sensitive information collected. As a data controller, we store the collected data in database with multiple security protections by default to ensure that the stored data can resist SQL injection, brute force cracking and other attacks.

● **De-identified storage**

Information provided by the customer when registering the Tencent Cloud account is used to create the account, Tencent Cloud will generate a unique identifier number (UIN) for account information. In most cases, Tencent Cloud only needs to identify a customer's UIN to provide the selected services to the customer without needing to authenticate the information of the registered account. Tencent Cloud uses this method to protect the personal data of registered accounts.

Customer are clearly informed of the purpose, scenario to use the data, and customer's registration information is processed in the privacy policy, such as in bill issuing and collection reminders. Tencent Cloud will mask some information with asterisks when it is displayed to protect the personal data of customers.

● **Storage period**

Tencent Cloud has set the retention period according to different types of data to ensure that the expired data can be deleted in time when the purpose of data processing has been met.

## Data Usage

● **Tencent Cloud Data processing conforms to the purpose of initial data collection**

Tencent Cloud requests all services and related businesses to use collected data only for the purpose, scope, and users that are informed to customers at the time of collection. For this reason, the relevant departments of Tencent Cloud will continually follow up on the actual purpose, scope, and users of data and whether these have changed since the data was collected. In case of any change, the data subject will be informed again, and the legal and effective consent of the data subject will be obtained before using the data where legally necessary.

● **Data processing shall be carried out according to the principle of minimum necessity**

Tencent Cloud will evaluate the relevance between its data processing and the purpose of data collection. Moreover, Tencent Cloud has deployed multi-factor authentication technology to implement accurate access control, so as to ensure that the data usage is consistent with the information provided at the time of collection.

● **Data subjects can restrict data processing**

Depending on the region where the customer is located, the customer may have certain rights to restrict data processing. For example, where the customer agrees that Tencent

Cloud will use its data for marketing or analysis, the customer can submit an application via email (cloudlegalnotices@tencent.com) to refuse to have its data processed in this particular case.

## Data Transfer/Shared

● **Transmission encryption**

In the process of personal data transmission, Tencent Cloud uses a secure and reliable transmission protocol to encrypt the channel, together with other security means, to ensure the security of data in the transmission process and avoid data leakage in the transmission process.

● **Data sharing**

As mentioned in the privacy policy, Tencent Cloud may share information with third parties within and outside the customer's country/region. The third party referred to herein usually includes the third-party services that Tencent Cloud uses to process payments, send SMS service notifications, or provide other services, support, or functions. In this process, Tencent Cloud will try to transmit de-identified information or desensitized information, and it has established a strict process to standardize the sharing transmission mechanism and implement monitoring and approval measures. In the process of introducing third parties, there are also strict introduction mechanisms and due diligence to control the compliance of third parties.

## Data Deletion

Tencent Cloud has set a reasonable data retention period according to the data type. If the customer is told that the purpose has been achieved or the retention period has expired, Tencent Cloud will delete the relevant customer data.

In addition, Tencent Cloud can, under reasonable circumstances, meet the needs of personal information subjects to delete the relevant information.

## The Other Compliance Points

● **Access control**

Access control is one of the main methods of protecting and maintaining network security. Its purpose is to ensure that information and resources are not used and accessed in an unauthorized manner.

To Privacy impact analysis also requires regular re-evaluation of products that have been released and evaluated by PIA, including but not limited to product functions, target customers, and whether there are changes in the collection and sharing of special types of personal data, so as to ensure the effectiveness of privacy impact analysis. According to the results of the privacy impact assessment, non-compliant data processing behavior is required to be corrected to reduce the risk of privacy compliance.

● **Personal data Record of Processing (ROP)**

The ROP includes product information and data security management. It aims to understand the types of data involved in the product and the control measures of data in the whole life cycle of collection, storage, use, transmission/sharing and deletion. The business party explains the legitimacy of relevant data collection by truthfully disclosing the scenarios of data collection. The reviewer will review the data processing method in the data life cycle in accordance with data processing principles and give orders to correct the non-compliance of products so that they become compliant before approving the product online release audit process. In addition, it ensures the accuracy and integrity of information disclosure, and the legal expert team will output the privacy policy on the basis of PIA and ROP and release it on the official website.

● **Data leakage**

In order to try to control the impact of data leakage events on data subjects and properly protect data assets in the event of major data security events, Tencent Cloud has established an event response process to ensure relevant parties can be notified in time after the occurrence of events and ensure the responsible team can take remedial measures quickly, orderly, and effectively, and formulate improvement measures to avoid recurrence of issues and minimize losses caused by the event to the businesses of the customers and the company.

In order to prevent the occurrence of network security events (including data leakage events), Tencent Cloud actively adopts a security monitoring system to classify and categorize security vulnerabilities to analyze, track, record, and correct events in a timely manner.

When an information security incident occurs, Tencent Cloud will follow a specific incident response process aiming to respond to the incident effectively and in accordance with and within the timeframes set forth in applicable law and its policies. Tencent Cloud will prioritize efficient and quick resolution of any incidents. Tencent Cloud has a detailed set of responsibilities and authorities for those dealing with security incidents and defines the categories and assigns levels of information security incidents based on its nature and

importance.

To prevent incidents, Tencent Cloud uses the security monitoring system and grades and classifies the security vulnerabilities aiming to analyze, follow up, record and redress them in time.

# 4. As a data processor, how can Tencent Cloud help customers practice privacy compliance?

## 4.1 Tencent Cloud as a data processor

As a cloud service provider, Tencent Cloud will be responsible for the operation and maintenance of the cloud platform. Most of the work of Tencent Cloud platform has been automated to avoid the risk of human error as much as possible. In most cases, the operation and maintenance personnel of Tencent Cloud platform do not need to access customer business data when providing technical support to customers. Unless the customer clearly states that it needs Tencent Cloud to provide operation and maintenance support, its help to handle some customer business data, or other requests of such nature, Tencent Cloud will obtain clear customer authorization, and data will be processed strictly in accordance with the principle of minimum necessity.

## 4.2 Tencent Cloud responsibility sharing model

For "customer business data", Tencent Cloud will always adhere to Tencent's business philosophy of "everything is based on user value" and is committed to empowering customers and helping customers achieve secure and compliant personal data on the cloud in accordance with the "Tencent Cloud Responsibility Sharing Model".

Tencent Cloud uses a unified infrastructure and resource sharing to provide customers with the network, storage, computing and other cloud resources they need. Customers can adopt three different resource forms of cloud computing services such as IaaS, PaaS and SaaS of Tencent Cloud according to their needs. Tencent Cloud has established the following responsibility sharing models for different service models. The light blue section shows the responsibilities of Tencent Cloud, the light purple section shows the responsibilities of the customer, and the light green section shows the responsibilities which are jointly undertaken by Tencent Cloud and the customer. For more information about the "Tencent Cloud Security Responsibility Sharing Model", please refer to the "Tencent Cloud Security White Paper".

| | IaaS | PaaS | SaaS | |
|---|---|---|---|---|
| **Customer Responsibilities** | Data Security | Data Security | Data Security | |
| | Terminal Security | Terminal Security | Terminal Security | **Shared Responsibilities** |
| | Access Control Management | Access Control Management | Access Control Management | |
| | Application Security | Application Security | Application Security | **Tencent Cloud Responsibilities** |
| | Host and Network Security | Host and Network Security | Host and Network Security | |
| | Physical and Infrastructure Security | Physical and Infrastructure Security | Physical and Infrastructure Security | |

Tencent Cloud Shared Security Responsibility Model

Regarding customer business data on the cloud, the customer, as the data controller, shall be responsible for identifying the laws and regulations applicable to its business and ensuring that collection and identification, classification and grading, authorization and encryption and other security controls can be carried out for its own cloud personal data in accordance with the requirements of the relevant laws and regulations. Meanwhile, Tencent Cloud, as a data processor, is responsible for ensuring the security of the underlying cloud platform. Based on Tencent's technology accumulation over many years, Tencent Cloud has been committed to studying solutions to help customers improve their data security capabilities. We expect that helping customers meet their security capabilities will also improve their compliance ability to manage personal data, so as to help customers build a perfect privacy compliance system.

## 4.3 How does Tencent Cloud help customers practice privacy compliance?

Nowadays, personal data compliance surveillance is becoming increasingly intensive. When customers conduct business on Tencent Cloud, they should identify applicable laws, regulations and regulatory requirements. Although the jurisdictional requirements and regulatory conditions of countries and regions are not the same and there are certain differences in the specific requirements of laws and regulations, the accumulated experience of Tencent Cloud's global operation summarizes some basic commonalities and principles from the perspective of personal data protection and compliance. In the follwing, we will

how customers should respond to these compliance requirements and how Tencent Cloud can help customers respond to these compliance requirements based on the full life cycle of personal data on the customer cloud and other key compliance requirements.

The following are not specific to the laws and regulations of one country or region but are general compliance considerations. When customers want to carry out relevant business in one country or region, each customer must assess the legal and regulatory requirements that apply to their activities, the processing of their data, and the engagement of any service providers. We have included a few helpful tips below, which our customers tell us they often consider as part of their compliance program. This is no substitute for, and is not intended to be any substitute for, legal advice. All customers must obtain advice from a legal professional to understand how their activities may be impacted by laws and regulations.

| Key area | Compliance requirements | Customer responsibilities | How Tencent Cloud helps customers |
|---|---|---|---|
| Data collection | The personal data of the data subject should be collected for specific, clear, and legal purposes.<br><br>Before collecting the personal data of the data subject, the data subject shall be informed in accordance with the requirements of applicable laws and regulations, including but not limited to the purpose of data collection and use.<br><br>The personal data collected shall meet the business purpose stated in the notice, and no personal data for purposes other than the specified one shall be collected. | As the data controller, the customer shall identify the collection purpose and processing scenario of personal data by itself and inform the data subject before collection in accordance with the applicable laws and regulations.<br><br>Meanwhile, the customer shall ensure that it will not collect excess personal data that are not required to meet the business purpose of the notice. | As the data processor, Tencent Cloud supports customers to integrate necessary privacy policies in their applications.<br><br>Tencent Cloud has products with relevant capabilities for customers to choose from. See 4.4 for details. |

| | | | |
|---|---|---|---|
| **Data storage** | The storage period of personal data shall be consistent with the content when informing the data subject.<br><br>The storage period of personal data should not be longer than the period required to achieve the business purposes.<br><br>The security of personal data in storage shall be ensured. | As the data controller, the customer shall identify the personal data that must be collected and stored, the storage period and the storage location for its business.<br><br>The customer shall ensure the security of personal data in storage, including but not limited to anonymization or encryption of personal data in storage. | As the data processor, Tencent Cloud supports customers to select regions and zones by themselves, and store customer business data in their selected regions.<br><br>For products with the function of storing data, Tencent Cloud supports customers to set the data storage period by themselves. When customers choose to delete the personal data they collect, Tencent Cloud will destroy the relevant data in an irreversible manner.<br><br>Tencent Cloud has products with relevant capabilities for customers to choose from. See 4.4 for details. |
| **Data use** | The use of personal data shall be consistent with the purpose which is told to the data subject. | As the data controller, the customer shall identify the purpose of using the personal data, how to use them, and who can access the relevant data. The above use shall be consistent with the content notified to the data subject. | As the data processor, Tencent Cloud can access customer business data necessary for locating issues only after obtaining the customer's authorization.<br><br>Tencent Cloud has products with relevant capabilities for customers to choose from. See 4.4 for details. |
| **Data transmission/sharing** | The data sharing shall be based on legal basis, including consent.<br><br>When personal data are transmitted to overseas countries, attention shall be paid to the laws and | As the data controller, the customer shall select the appropriate Tencent Cloud region as needed. Before transmitting (disclosing / sharing) personal data to other organizations, the data subject shall be informed of the purpose of transmission, data to be transmitted and the | As the data processor, Tencent Cloud will not transfer customer business data to areas other than its selected region.<br><br>Tencent Cloud will carry out HTTPS encryption for the communication of customers accessing Tencent Cloud |

| | | |
|---|---|---|
| regulations of the country where the data subject is located and the country where the data flows in, so as to ensure that the transmission meets the applicable compliance requirements.<br><br>The security of personal data in transmission shall be ensured. | name of other data processing institution, and there should be a legal basis for any relevant processing. When transmitting personal data outside the country where the data subject is located, appropriate laws and regulations should be identified to ensure that appropriate control measures are deployed and implemented in accordance with the requirements of the laws and regulations, such as signing a data transmission agreement with the receiver of a third country, clarifying the control requirements of data processing, clarifying the jurisdiction and other contents, as well as adequacy, derogation, appropriate safeguards, etc. depending on applicable law requirements.<br><br>The customer shall ensure the security of personal data in the transmission process, including but not limited to the use of secure transmission protocols, network encryption channels and other measures. | console via the Internet; similarly, communications between the customers and Tencent Cloud via cloud API also supports HTTPS data encryption transmission protocol to improve the security of data.<br><br>Tencent Cloud has products with relevant capabilities for customers to choose from. See 4.4 for details. |

| | | | |
|---|---|---|---|
| **Data deletion** | When the stated business purpose is achieved, the relevant data shall be deleted promptly.<br><br>When the data subject requests to delete its personal data, the relevant data shall be deleted promptly. | As the data controller, when the business purpose is achieved, the customer should delete the personal data of the relevant data subject promptly.<br><br>When the data subject requests to delete its personal data, the customer should cooperate to delete the relevant data. | When the cloud service agreement is terminated or the customer voluntarily deletes the data, as the data processor, Tencent Cloud will erase and overwrite the data on the storage medium according to the agreement reached with the customer, using an industry-recognized mechanism, to ensure that the data stored in the data disk are completely erased, and ensure that the deleted data are not recoverable. |
| **Responding to data subject rights** | The corresponding data subject rights shall be identified according to the requirements of applicable laws and regulations, including but not limited to access rights, correction rights, deletion rights, etc., and applicable subject rights shall be provided for the data subject. | As the data controller, the customer shall identify the corresponding data subject rights according to the requirements of applicable laws and regulations, including but not limited to access rights, correction rights, deletion rights, etc., and provide applicable subject rights for the data subject. | Customers can request necessary support from Tencent Cloud via email (cloudlegalnotices@tencent.com) |
| **Privacy by Design& Default (PbD)** | When designing new products/applications, personal data compliance and security measures shall be considered and integrated into the overall design. | As the data controller, the customer shall consider personal data compliance and security measures when designing new products/applications and integrate them into the overall design. | The privacy by design & default is considered for Tencent Cloud products. |

| | | | |
|---|---|---|---|
| **Privacy Impact Analysis (PIA)** | For high-risk scenarios such as new technologies, automated decision-making and large-scale processing of personal data, privacy impact analysis shall be carried out to determine whether the risk of processing is controllable for the data subject. | As the data controller, the customer shall conduct Privacy Impact Analysis for high-risk scenarios such as new technologies, automated decision-making, and large-scale processing of personal data to judge whether the risk of processing is controllable for the data subject. | Tencent Cloud conducts Privacy Impact Analysis for products. |
| **Personal data records of processing** | Personal data records of processing shall be retained. | As the data controller, the customer shall record personal data processing activities. | Tencent Cloud keeps records of personal data processing activities. |
| **Data leakage** | Where leakage of personal data occurs, the local regulators and data subjects shall be notified as needed in accordance with the laws and regulations of each country. | As the data controller, the customer should formulate an appropriate data leakage management process, which should effectively identify the requirements of laws and regulations for data leakage and the relevant regulatory agencies. | Tencent Cloud has developed a standardized and procedural emergency response mechanism for personal data leakage within the scope of Tencent Cloud's responsibility, so as to respond to the event in a timely manner, notify it to the customers, and provide support for the customers to handle the event. If the event occurs within the scope of the customer's responsibility, Tencent Cloud will also provide appropriate assistance to support the customer to deal with the relevant event upon request from the customer. |

For more information about Tencent Cloud data security, refer to "Tencent Cloud Data Security White Paper".

**4.4** **Tencent Cloud's products and solutions for compliance of customers**

In terms of customer business data, customers have full control over their data hosted in the cloud and are ultimately responsible for the security management of their own business data stored in the cloud. To help customers build a privacy-compliant cloud environment, Tencent Cloud provides customers with a full range of cloud products and services.

In the following table, some representative Tencent Cloud products and services are listed. These tools are intended to support our customers' compliance program, not replace it. Each customer must consider what technical and organizational measures they need to adopt to comply with the laws in the jurisdictions where they operate. In some cases the tools we have developed may help our customers meet certain of these requirements. For more information about Tencent Cloud products and services, refer to the product page of the Tencent Cloud official website.

| Data lifecycle | Product or service name | Product functions |
|---|---|---|
| Data collection | Data Security Center | Data Security Center is a data security operation platform integrating sensitive data discovery and classification and grading, data map, and abnormal data access analysis. It helps enterprises automatically sort out data assets, classify and grade enterprise cloud data, and assess security risks. It also works with Tencent Cloud security capabilities to form a closed data security protection network, helping enterprises maximize their security benefits.<br><br>The product can be used in both data storage and data use stages. |
| | Mobile Security | Mobile Security (MS) provides customers with a one-stop security solution for the whole life cycle of mobile applications (APPs). It covers application reinforcement, security evaluation, compatibility testing, piracy monitoring, crash monitoring, security components and other services. It has been constantly improved after its application in 1.2 billion terminals over many years, and has served many industries such as finance, Internet, Internet of vehicles, Internet of things, operators, and government affairs. It is stable, simple, and effective, so mobile security construction is no longer a burden.<br><br>The product can also be used in the data use stage. |

| Data storage | Key Management Service | Key Management Service (KMS) is a security management service that allows you to easily create and manage keys, protect the confidentiality, integrity, and availability of keys, meeting the key management needs of customers with multiple applications and services, as well as regulatory and compliance requirements. |
|---|---|---|
| | Secrets Manager | Secrets Manager (SSM) provides customers with full lifecycle management services such as the creation, retrieval, updating, and deletion of credentials, and easily realizes the unified management of sensitive credentials in combination with resource-level role authorization. For the leakage risk caused by sensitive configuration and sensitive credential hard coding, customers or applications can retrieve their credentials by calling the Secrets Manager API, effectively avoiding the business risk caused by sensitive information leakage and out-of-control permissions caused by program hard coding and plaintext configuration. |
| Data use | Cloud Access Management | Cloud Access Management (CAM) is a customer permission management system provided by Tencent Cloud to help customers securely and finely manage the access to Tencent Cloud products and resources. You can create customers or roles in access management, assign them separate security credentials (console login password, cloud API key, etc.) or request temporary security credentials for them to access Tencent Cloud resources. You can manage permissions to control what operations customers and roles can perform and what resources they can access. Moreover, if your enterprise or organization has an intranet account system, you do not need to create sub-customers or collaborators for enterprise customers in Tencent Cloud account. The identity provider will provide SSO (single sign-on) capability for enterprise customers, and external customers who pass IdP authentication can directly access your Tencent Cloud resources. |
| | Host Security | Based on the massive threat data accumulated by Tencent, Host Security uses machine learning to provide customers with security protection services such as hacker intrusion detection and vulnerability risk early warning, mainly including password cracking and interception, abnormal login reminder, Trojan file detection and killing, high-risk vulnerability detection and other security functions, so as to solve the major network security risks faced by the current server and help enterprises build a server security protection system. |

| | | |
|---|---|---|
| **Data use** | Security Operation Center | Security Operation Center (formerly known as situational awareness (public cloud)) is a cloud security operation platform based on customer cloud security data and Tencent security big data. Through multi-dimensional and continual intelligent analysis of massive data, it provides customers with vulnerability intelligence, threat discovery, event handling, baseline compliance, leakage monitoring, risk visualization and other capabilities, and takes corresponding security measures to ensure the security of information systems and help customers realize secure operation in the full life cycle. |
| | Cloud Audit | Cloud Audit is a service that supports the monitoring, compliance detection, operation audit and risk audit of your Tencent Cloud account. With Cloud Audit, you can record logs, continually monitor and retain account activities related to operations in the entire Tencent Cloud infrastructure. Cloud Audit provides event history of Tencent Cloud account activities, including operations performed via Tencent Cloud management console, API services, command line tools, and other Tencent Cloud services. This event history can simplify security analysis, resource change tracking and problem troubleshooting. Cloud Audit is a service that supports the monitoring, compliance detection, operation audit and risk audit of your Tencent Cloud account. With Cloud Audit, you can record logs and continually monitor and retain account activities related to operations in the entire Tencent Cloud infrastructure. Cloud Audit provides event history of Tencent Cloud account activities, including operations performed via Tencent Cloud management console, API services, command line tools, and other Tencent Cloud services. This event history can simplify security analysis, resource change tracking and problem troubleshooting. |
| **Data transmission/ sharing** | Virtual Private Cloud | Virtual Private Cloud (VPC) is a private cloud cyberspace built on Tencent Cloud, which provides network services for your resources on Tencent Cloud, and different private clouds are completely logically isolated. As your exclusive cyberspace on the cloud, you can manage your private network VPC by defining the network via software and realize the configuration management of IP address, subnet, routing table, network ACL, flow log and other functions. The Virtual Private Cloud also supports a variety of ways to connect the Internet, such as elastic IP, NAT gateway, etc., and provides a variety of billing methods and bandwidth packages to help you save costs. Furthermore, you can also connect Tencent Cloud and your local data center via VPN connection or Direct Connect access, and flexibly build a hybrid cloud. |

| | | |
|---|---|---|
| **Data transmission/ sharing** | Direct Connect | Direct Connect (DC) provides a convenient method to connect the enterprise data center and Tencent Cloud, so as to establish a private connection service completely isolated from the public network via Direct Connect. Compared with the public network, Direct Connect has the characteristics of higher security, higher stability, lower delay, wider bandwidth and so on. You only need a dedicated physical line of an operator to access Tencent Cloud at one point, and you can quickly create multiple dedicated channels to connect computing resources deployed in Tencent Cloud for flexible and reliable hybrid cloud deployment. In many cases, different billing options of dedicated channels can also save you the cost of using dedicated lines. |
| | VPN Connections | VPN Connections is a transmission service based on network tunneling technology to connect the local data center with Tencent Cloud resources. It can help you quickly build a secure and reliable encrypted channel on the Internet. VPN Connections has the characteristics of simple configurations, real-time effectiveness of cloud configurations and high reliability. Its gateway availability reaches 99.95%, ensuring stable and continual business connections and helping you easily realize complex business scenarios such as remote disaster recovery and hybrid cloud deployment. Tencent Cloud VPN Connections provides services under relevant national policies and regulations but does not provide access to the Internet. |
| | SSL Certificates | SSL Certificates, also known as server certificates, provide you with a one-stop service for secure socket layer (SSL) certificates, including certificate application, management, and deployment functions. It works with top-level digital certificate authority (CA) institutions and agents to provide HTTPS solutions for your website and mobile applications. |
| | Migration Service Platform | The Migration Service Platform (MSP) integrates various migration tools and provides unified monitoring. Customers can choose Tencent Cloud's official migration tools or an officially certified third-party migration tool for migration. The Migration Service Platform helps customers easily and quickly migrate the system to the cloud, and clearly understand the migration progress. The Migration Service Platform (MSP) does not charge any extra fees. You only need to pay for the migration tools and resources you use. |

| | | |
|---|---|---|
| **Data transmission/ sharing** | Web Application Firewall | Tencent Cloud Web Application Firewall (WAF) helps customers in and out Tencent Cloud deal with Web attack, intrusion, vulnerability exploitation, Web-Page Trojan Horse Clue, tampering, backdoor, crawlers, and other Website and Web business security protection issues. By deploying Tencent Cloud WAF, enterprise organizations transfer the threat pressure from Web attacks to Tencent Cloud WAF protection cluster nodes and obtain Tencent web business protection capabilities at the minute level to escort the secure operation of the organization's Website and Web services. |
| | Anti-DDoS Pro | Anti-DDoS Pro is a paid service for customers whose businesses are deployed on Tencent Cloud to improve their DDoS protection capabilities. It is directly effective for cloud products without changing IP. After purchase, it can be used only by binding the IP that needs protection. It has the characteristics of convenient access and zero change. |
| | Anti-DDoS Advanced IP | Anti-DDoS Advanced IP is a paid protection service released to target situations in which Internet services (including Tencent Cloud services and non-Tencent Cloud services) will suffer from high-volume DDoS attacks, resulting in the unavailability of customer services. |
| | Tencent Cloud EdgeOne | Tencent Cloud EdgeOne provides L4/L7 security protection and acceleration services for overseas markets based on Tencent's global edge nodes, protecting e-commerce and retail, financial services, content information and games, and improving customer experience. |

# Privacy Compliance Issues – FAQ

## 1. How does Tencent Cloud define "personal data" (or "personal information")?

Tencent Cloud has analyzed laws and regulations related to the protection of personal information in countries where it provides services and adopted the strictest definition of "personal data" (or "personal information"), that is, all types of information recorded electronically or in other ways that can identify the identity of a specific natural person or reflect the activities of a specific natural person, either alone or in combination with other information, including but not limited to the name, date of birth, certificate information (ID card number, passport number), email address, account password and location information, IP address, website browsing records, etc. of a natural person.

## 2. What customer related data do Tencent Cloud collect?

 When Tencent Cloud acts as a data controller, it collects the relevant information generated by customers' use and purchase of Tencent Cloud services and their interactions with Tencent Cloud. For details, refer to Chapter 3.1 of this white paper.

 When Tencent Cloud acts as a data processor, the content data are stored on the side of Tencent Cloud by customers for business purposes, including but not limited to text, audio, videos or images.

## 3. Who controls customer business data?

As a customer, you have full control of your data. Tencent Cloud only processes such data according to customers' instructions. You are fully responsible for the access rights of customers to your cloud data and to ensure that only specific personnel can perform specific operations for specific data. Tencent Cloud uses Tencent's years of compliance management practices to provide you with a full range of data security and privacy protection tools and technologies to help you better manage cloud customer data.

## 4. How does Tencent Cloud respond to government requests?

These operational guidelines are for any law enforcement authority or other governmental authority making a request to Tencent Cloud. Tencent Cloud will scrutinize all requests to make sure they comply with the applicable laws and regulations and will request court order, subpoena, search warrant, authorization document(s) and/or other valid legal process, as the

case may be. When there is any request for data (including customer data) to Tencent Cloud, Tencent Cloud will abide by applicable law and conduct a full assessment of the request, determine the legal basis of the request and decide whether it is allowed to disclose taking into account the request received, the applicable procedures and the guaranteed awarded to data by all applicable laws. Tencent Cloud responds to requests of an international nature made pursuant to a Mutual Legal Assistance Treaty and similar procedures (collectively, "MLAT"). These procedures are aimed at determining the procedures as to how countries can assist one another in legal matters such as criminal investigations or enforcement proceedings. In the absence of MLAT we are at times not allowed to disclose data requested internationally.

## 5. How does Tencent Cloud collect account information and information generated by customers using Tencent Cloud's official website?

In its privacy policy, Tencent Cloud introduces how it collects and uses account information and how customers use the information generated by Tencent Cloud's official website. We know that you are concerned about how your relevant information is used, and we process your information in accordance with the requirements of applicable laws and regulations. If you have any questions, comments and requirements, you can send an email to cloudlegalnotices@tencent.com to contact us.

## 6. Where are the customer data stored?

Up to now, the infrastructure of Tencent Cloud has covered 26 geographical regions around the world. Tencent Cloud supports customers to choose regions to store their customer data for products with geographical attributes. After receiving the customer's instructions for the storage location, Tencent Cloud is completely isolated between different regions to ensure the maximum stability and error tolerance between different regions. Without the authorization of the customer, the customer's data will not be transferred outside the Tencent Cloud region selected by the customer, unless otherwise required by law or a binding directive issued by a government department.

Tencent Cloud supports customer queries on the data center location of their stored data by submitting work orders.

## 7. How long is the retention period of customer data?

According to the agreement reached between Tencent Cloud and customers, the customer data will be retained for a reasonable period of time after the expiration or termination of the service, and customers must complete the migration of customer data before the expiration of the retention period. After the expiration of the retention period, Tencent Cloud service

system will automatically delete all customer data and account information of customers, and all deleted data cannot be recovered, unless otherwise required by laws and regulations.

## 8. What measures have Tencent Cloud taken to protect the security of customer data?

With years of security experience and accumulation of Tencent Group, Tencent Cloud has built a strong in-depth security defense system for the cloud platform, in which data security has always been a crucial link. For details, see "Tencent Cloud Security White Paper" and "Tencent Cloud Data Security White Paper".

Moreover, Tencent Cloud complies with the compliance requirements of different countries and industries, builds a perfect information security management system, and provides customers with cloud services that are audited and recognized by third-party authoritative certification institutions and are trustworthy to customers. For more details of Tencent Cloud compliance, refer to the "Tencent Cloud Compliance" page.

## 9. If customers have questions about data protection and privacy compliance, how can they contact Tencent Cloud?

If customers have questions about data protection and privacy compliance, they can send an email to cloudlegalnotices@tencent.com to contact us.

# Conclusion

Protecting the security and compliance of personal data is the common mission of Tencent Cloud and its customers. Tencent Cloud has created a comprehensive operation mechanism at the platform level to effectively ensure the security of the infrastructure and platform services. In order to better protect customers' data assets hosted in the cloud, Tencent Cloud will define its role clearly in data processing activities, provide one-stop solutions for the full life cycle of data for customers to choose from, provide data security solutions suitable for integration with personal data, cover enterprise data flows from the aspects of links, networks, and access requests, help customers protect sensitive information such as personal data in the flow of big data, and minimize the risks in process, technology and privacy compliance.

Tencent Cloud will uphold the open and shared characteristics of cloud computing services, continually improve its privacy compliance capabilities, and help customers achieve privacy compliance and security on the cloud.