agora

Privacy Protection

WHITE PAPER

agora.io

Contents

1. Overview

The traditional means of communication have shifted as the world adopts and popularizes new technologies, including mobile Internet technology such as the acceleration of the 5G commercial operations. Communication across the globe no longer relies on laborious international phone calls or business videoconferencing, and low-latency live interactions no longer require professional arrangements. People have grown accustomed to sharing aspects of their lives through online communication platforms so as people become more and more public with their lives, they also start to pay attention to privacy matters.

Privacy is the ability to withhold information, space, or activities from others that one deems personal. Internet users are interested in privacy, especially when using voice and video services where private matters can easily transmit throughout the Internet. In recent years, privacy leakage incidents have led people to doubt the privacy protection ability of Internet service providers and users now consider privacy as an important factor to consider when choosing Internet services.

In order to protect users' privacy, privacy protection laws and regulations have been issued around the world. Agora has always attached great importance to privacy protection and has established an information security and privacy system based on personal data protection, considering its own business features and various privacy protection regulatory requirements.

2. Agora Privacy Protection Culture

2.1 Privacy Culture

Agora regards personal data, a special category of data, as one of the most highly protected data categories. Agora adheres to the concept of personal data protection through minimizing collections and using and implementing strict personal data protection measures supported by the data security system.

Agora pays close attention to the privacy requirements of each country and region and protects the privacy rights of Agora's clients and end users on the basis of compliance. Currently, Agora issues customers the *Agora Privacy Policy* based on the supervision and compliance requirements of each service area and its own business features, such as Agora's external privacy commitment.

In order to effectively protect the privacy of clients and end users, Agora adheres to the principle of Privacy by Design (PbD) in the construction projects of services and products in accordance with industry best practices. Agora prioritizes the integrity and confidentiality of personal data in the initial design of services and products and ensures that personal data is effectively protected throughout the life cycle of services and products. Agora's privacy protection design follows the PbD Principle:

- **Proactivity and Prevention:** Agora approaches the issues of privacy risks in a proactive manner, mitigating potential risks before they become apparent. Poor information security and privacy practices must be recognized and improved as early as possible.
- **Privacy as the Default:** Privacy is built into the product and system by default. The privacy of the user can be protected without performing any action on the product or service.
- **Privacy Embedded into the Design:** Privacy is embedded in both design and architecture of the product and system. Privacy is treated as a basic feature rather than an additional feature, which will not limit users' experience of the product and integrates privacy in a holistic and innovative way for a better user experience.
- **End-to-End Security—Full Lifecycle Protection:** Before data enters the system, Privacy by Design is embedded into the system, securely extending throughout the life cycle of the data involved. Data is secured, protected, securely stored, and then properly destroyed.
- **Visibility and Transparency:** Accountability, transparency, and compliance are necessary for an effective and secure system and they create trust for the security level that the system provides. In addition, the system has also improved by allowing users and other interested parties to see how information is passed through.

- Respect for User Privacy: System architects and designers protect users' interests by providing powerful measures such as privacy default settings, appropriate notifications, and enhanced user-friendly options.

2.2 Compliance Support

Compliance is the foundation of Agora's service operations. While providing services globally, Agora pays close attention to privacy compliance requirements of various countries and regions to create real-time voice and video services that are trusted by clients. Therefore, Agora is committed to building management systems and services in accordance with internationally recognized information security and privacy standards, as well as industry best practices. To further prove compliance capability, Agora will continue to obtain more professional certifications in the future to ensure its own compliance and provide compliance support to clients to help them comply with applicable regulations and supervisory requirements.

- **ISO/IEC 27018: 2019 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**

  ISO/IEC 27018 is a supplement to ISO/IEC 27002 (Information technology—Security techniques—Code of practice for information security controls), which strengthens personal data protection in public cloud services and provides a set of personal data protection guidelines applicable to public clouds.

  Agora has established a personal data protection system to protect personal data from the aspects of privacy rights and data life cycle. This certification demonstrates that Agora has implemented an effective cloud-based personal data protection system.

- **General Data Protection Regulation, GDPR**

  The EU General Data Protection Regulation is a comprehensive data protection law which aims to protect the basic privacy rights and personal data of data subjects in the EU through strong measures.

  Agora is committed to helping clients meet GDPR compliance requirements while providing services and products. Agora attaches great importance to the impact of GDPR on enterprises involved in personal data processing and has continuous in-depth analysis and understanding of GDPR. In addition to the PbD practice mentioned above, Agora also integrates the requirements of GDPR into product planning and business activities by creating a timely response mechanism for privacy rights to respond to data subjects demands, building privacy protection responsibility model for Agora's servers, conducting regular or on-demand data protection impact assessments (DPIA) and actively fulfilling the duties as data processers and controllers.

3. Privacy Protection Measures

Agora considers privacy protection a priority to fully protect the privacy rights of clients and end users and provide clients with compliant online voice and video services. Agora has implemented a series of privacy protection measures, including personal data protection specifications, management processes, product functions and service design requirements. To ensure that privacy protection measures can be effectively implemented and continuously improved, Agora has appointed professionals within the company as Data Protection Officers (DPOs) and assigned personal data protection responsibilities in different service areas. Agora currently implements the personal data protection strategies of the data lifecycle, underpinned by the data security system.

3.1 Range of Collection

Agora provides online voice and video transmission services. Except for specific storage or caching services, Agora does not store client voice, video or message data. However, in order to meet the system monitoring, operation, and maintenance requirements, as well as comply with the laws and regulations in specific areas, Agora will record the equipment information and system operation status. There are three main personal data categories that Agora currently collects or retains:

- System log covering both the clients' and end users' equipment and network information
- Online messages cached from the Real-time Messaging service and the recorded video cached from the Real-Time Recording service (see Section 4.2.3 for details)
- Client contact information for Agora's website service registration

3.2 Storage and Processing

Agora categorizes and classifies personal data collected and retained according to regulatory requirements and the sensitivity of personal data. Agora then takes appropriate data protection measures to prevent the loss, damage, leakage or tampering of personal data in the process of storage and processing. Agora fully assesses the use scenarios and requirements of personal data and processes and uses the personal data only when it is necessary for the business and subject to the scope that is directly or reasonably related to the purpose for which the personal data was collected. If business requirements request the use of personal data beyond consent, Agora will re-obtain the consent of the data subject. When storing sensitive personal data, Agora adopts encryption methods and configures different access control rules and technical means depending on the data sensitivity to restrict internal personnel's access to, and operation of, the data, to avoid unauthorized use or illegal processing of personal data.

To ensure comprehensive and effective protection, Agora regularly carries out a comprehensive review of the collection and use of personal data, including the categorization, resources, methods of storage and processing of the data. By examining the personal data processing and testing the corresponding treatment mechanism, Agora analyses the implementation of data protection strategy and the compliance situation with relevant laws, regulations and standards. Agora's data protection personnel and information security personnel are responsible for following up and responding to any violations or risks found.

3.3 Transmission and Sharing

When it comes to the transmission or sharing of personal data, Agora evaluates the situation of data transmission, following the principles of reasonableness, legitimacy and necessity, transmitting the necessary data externally only in the necessary scenarios, satisfying the requirements of reasonable, legitimate business purposes and minimizing transmission. Clients will be informed of the content of personal data transmission and the purpose of use and third-party data receiver in the form of service agreement or privacy policy.

Agora has established a data security transmission control policy and mechanism, which adopts a number of encryption technologies to ensure the confidentiality and integrity of data during transmission. Agora will conduct security assessments on the third-party institutions involved in data transmission, clarify the security responsibilities of both parties, identify the requirements of personal data protection measures, and establish a long-term follow-up audit mechanism to ensure that the third-party institutions always meet the security requirements of Agora. If Agora finds that a third party fails to handle personal data in accordance with the cooperation or authorization requirements, or fails to effectively fulfil its responsibility to protect personal data, Agora will immediately require the third party to cease such behavior and require effective remedial measures be taken to control or eliminate personal data risks.

If Agora's business requires personal data to transfer abroad, Agora's DPOs will identify and analyze the sensitivity and amount of personal data to be transferred. They will also uncover the legal and regulatory requirements of both the country where the data origins originates, and the country where the data will be stored. When the relevant compliance requirements are met and the secure transfer of personal data is guaranteed, Agora will explain the purpose, scope, the content of the cross-border transfer, data recipient and the country as well as the area where the data recipient locates, and conduct the cross-border transfer with the consent of the clients or end users.

Agora's DPOs will monitor and periodically review Agora's cross-border data transfer to confirm regulatory requirements of the geo-political regions are met.

3.4 Treatment

Agora has identified the location, form and period of retention of personal data according to the service commitment, minimum period to meet business requirements, and the compliance requirements of laws and regulations. The retention period of personal data of different categories or classifications has been clearly defined and communicated to clients or end users in the form of service agreement or privacy policy.

When the service expires or Agora discontinues certain services or products, Agora will strictly conform to the data retention period requirements and delete the personal data after the data retention period expires. For the personal data that cannot be deleted immediately due to business requirements, or because the deletion will affect the normal business operation of the company, Agora will adopt the method of anonymization to ensure that the anonymized data cannot be identified or associated with the data subjects. In addition, clients have the right to voluntarily opt out of the service or request Agora to delete the personal data transmitted or provided by the client. Agora will respond to clients' request within the response time defined in the privacy policy.

If a third party retains personal data, Agora will require that the third party stop using the relevant personal data and respond to the request of data deletion in a timely manner according to the service agreement. Agora will verify the results of data disposal by relevant third parties to ensure that personal data is effectively deleted or anonymized.

3.5 Right of Client

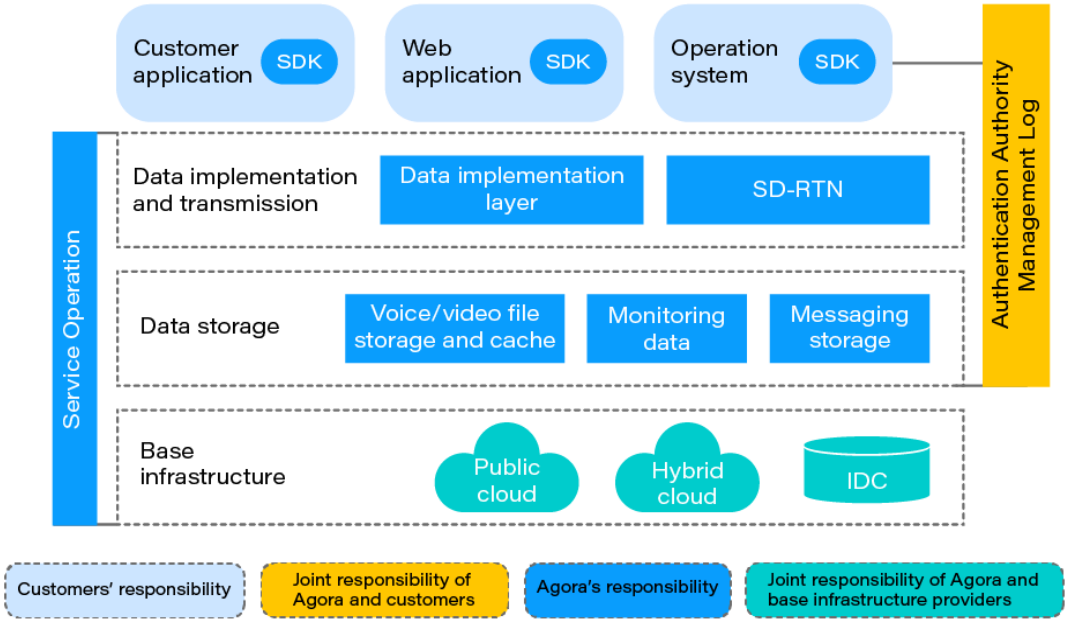
To ensure that clients exercise their privacy rights, Agora has coordinated across departments and established a standard privacy rights response process. Clients can contact privacy@agora.io on the Agora official website or submit a claim to the service support team. Agora will support clients to exercise the following rights:

- **Right to access:** Clients have the right to access all data uploaded by them or personal data of clients or end users collected by Agora
- **Right to rectification:** Clients have the right to correct or complete their personal data
- **Right to erase (right to be forgotten):** Clients have the right to request that Agora delete their personal data under some circumstances
- **Right to restriction of processing:** Customers have the right to be free from decisions based solely on automated processing, such as user profiling and differentiated recommendations based on data analysis
- **Right to be informed:** If the purpose and method of using personal data changes, Agora will inform the clients in a timely manner

4. Privacy Protection Responsibility

As a professional voice and video transmission service provider, Agora and its clients provide voice and video services to their end users. Agora is solely responsible for the transmission of voice and video. The collection, processing, local storage and deletion of personal data of end-users are still the responsibility of the clients. Agora will work with its clients to protect end-users' privacy.

The following figure shows the privacy protection responsibility model based on the cloud service SPI responsibility division.



Privacy protection responsibility model of Agora's service

4.1 Responsibility of Agora

Agora, as a voice and video service provider, is responsible for protecting personal data collected and generated during the service in accordance with the requirements of the service agreement and privacy policy, and protecting the information systems involved in the voice and video transmission service:

- **Restriction of data use:** Agora uses personal data strictly in accordance with the purpose of the service or client's requirements. Agora will timely inform clients of any changes in the service content and use of personal data.

- **Infrastructure security ability:** Agora protects the infrastructure that supports the voice and video transmission services, such as hardware device, network, server operating system, database and application system, etc., from unauthorized access and damage
- **Personal data protection:** Agora provides a variety of personal data protection technologies based on the regulatory requirements and best industry practices, including but not limited to authentication and access control, data encryption, data disposal, and audit log.

4.2 Responsibility of Client

As the direct collector of personal data, Agora's clients have the right of control over personal data. When providing services to end users, clients should fully consider the compliance requirements of each country and region to protect the privacy rights of end users.

When using Agora's online voice and video transmission service, clients should ensure the legitimate source of personal data. Prior to the collection of personal data, clients should obtain the consent of end users through a privacy policy, a service agreement, information collection tips and through other means.

Clients should truthfully inform end users of the scope and related purposes of personal data collected or processed by the clients and Agora during the use of the voice and video services, the processing and storage of personal data, and the responsibility boundaries when sharing personal data.

Clients shall establish personal data protection strategies for end users and implement appropriate management and technical measures to fulfill the privacy protection commitment for end users or meet the compliance requirements that may be involved, and to prevent personal data from unauthorized access, disclosure and tampering. For the management and technical measures that need to be implemented with the cooperation of Agora, clients should identify such measures and inform Agora. Agora will cooperate to realize the corresponding strategies.

Clients should also respect and protect the rights of end users as data subjects, make timely response to the requests of data subjects, and establish compliant management and end user escalation management systems. If an end user's privacy claim involves Agora's services, or if clients need to change the way the personal data is used due to business adjustments, clients should inform Agora in a timely manner and Agora will respond within the specified time.

5. Statement

5.1 Copyright Statement

This document is copyrighted solely by Agora. Without Agora's prior written permission, no subject may copy, modify, copy, or disseminate the content of this document in whole, in part, or in any form.

5.2 Restriction of Use

This document is written based on the current status of Agora's services and businesses and is intended only as a reference guide for clients using Agora's services and products. Agora does its best to provide appropriate introductions and implementation recommendations, but Agora does not guarantee in any way the accuracy or completeness of the descriptions in this document.

The services or products purchased or used by clients are subject to Agora's commercial contracts or service agreements, and clients shall not place service requirements on Agora based on the description in this document.