Honor Device Co., Ltd.

Privacy Protection White Paper

January 2024

HONOR

CEO's Messages

Your privacy, our priority - A Letter from the CEO to All Employees:

To fulfill our commitment to users, we have established an all-around privacy security protection system in terms of organizational structure, managerial requirements, process integration, and corporate culture. We have integrated the requirements for privacy protection into all of our business processes to ensure the effective implementation of these requirements through continual optimization and improvement. With continuous innovation in privacy protection technologies, we are committed to protecting the privacy of users on an all-around basis and creating a trustworthy tech brand while bringing users better products and experience. Your privacy is our priority. We will always make our best efforts to excel in everything we do.

— Zhao Ming, CEO of Honor Device Co., Ltd.

Table of Contents

Preamble 01

01 Our Understanding of Privacy Protection 02
1.1 Privacy Protection Concept 02
1.2 Principles for Personal Data Processing 02

02 We Build a Sophisticated Privacy Protection and Management System 04
2.1 Organizational Structure 05
2.2 Management Requirements 08
2.3 Process Integration 09
2.4 Corporate Culture 10
2.5 Tools Platform 11

03 We Protect Personal Data Through the Entire Life Cycle 12
3.1 Notification to Data Subjects 13
3.2 Options and Consent from Data Subjects 13
3.3 Collection 13
3.4 Use, Retention, and Disposal 13
3.5 Disclosure to a Third Party 14
3.6 Cross-border Transfer of Data 14
3.7 Rights of Data Subjects 15

04 We Integrate Privacy Protection into the Product Development Process 16
4.1 Proactive Prevention in the Product Research and Development Process 16
4.2 Rigorous Review Before Product Launch 16
4.3 Full Protection of Product O&M Processes 17
4.4 Systematic Management of Product After-Sales Service 17

05 We Provide Users with All-around Privacy Protection Experience 18
5.1 Protect Important Information from Being Abused 19
5.2 Protect Routine Use from Being Harassed 20
5.3 Protect Personal Data from Being Leaked 21
5.4 Prevent User Behavior from Being Tracked 22
5.5 Protect Personal Information from Being Viewed 23

06 We Build a Privacy Security Ecosystem With Partners 24
6.1 Privacy Security of the Hardware Ecosystem 24
6.2 Privacy Security of the Software Ecosystem 26
6.3 Partner Management 29
6.4 Collaborative Innovation 29

07 We Do More to Protect Privacy 30
7.1 Protect Children's Privacy and Escort Them in the Way to the Digital World 30
7.2 Care for the Elderly by Keeping Them Safe from Internet Fraud 31
7.3 More Secure AI Services Based on End User Computing 31
7.4 HONOR Health with Independent Control of Users' Personal Data 32
7.5 HONOR AI Space Protects the Privacy Security of Families 33

08 We Are Always Communicative and Transparent 34
8.1 Cooperation with Regulators 34
8.2 Consumer Communication 35
8.3 Privacy Security Certification 36
8.4 Cooperation with Industry Associations 37

Conclusions 38

Preamble

As technologies are developing and advancing, smart devices and mobile Internet are greatly changing people's lives. New technologies like 5G, cloud computing, and artificial intelligence (AI) are changing with each passing day. While greatly facilitating people's lives, intelligent services also bring great challenges to the protection of users' privacy.

In order to cope with this challenge, major economies around the world have formulated and improved laws and regulations on personal data protection, such as the General Data Protection Regulation (GDPR) fully implemented in the European Union in 2018, and the Personal Information Protection Law of the People's Republic of China (Personal Information Protection Law) and supporting regulations and standards that were enacted and implemented in China in 2021. Law enforcement agencies of various countries are also formulating detailed regulatory measures under the existing legal framework and stepping up the enforcement.

As the world's leading provider of smart devices, HONOR is committed to becoming a globally iconic tech brand that covers all scenarios, channels, and user groups and provides users with "innovative, premium, free, and trustworthy" products. Particularly, trustworthy products include not only products and services of high quality, but also the protection of users' privacy and data security. By applying continuous innovation in privacy protection technologies, HONOR will protect the privacy of users on an all-around basis and create a trustworthy tech brand while bringing users better products and experience.

This White Paper will systematically expound on HONOR's methodologies and practices in privacy and personal data protection.

01 Our Understanding of Privacy Protection

Privacy is closely related to everybody and everyone's privacy shall be respected and protected. HONOR takes users' privacy seriously. Privacy is a fundamental right of users. We regard the protection of user privacy as the most important prerequisite for supplying products and services. To implement the requirements for privacy protection, HONOR has put forward a privacy protection concept and formulated the seven principles for personal data processing.

1.1 Privacy Protection Concept

HONOR has been adhering to the principle of “Your privacy, our priority” since our inception and implement it throughout the business. With innovation, quality and service as the three strategic control points, HONOR keeps investing in R&D and forward-looking technology. We bring global consumers ever-innovative intelligent devices and create an intelligent new world for everyone. Meanwhile, HONOR always believes that technologies should be based on people and used for people. When it comes to personal privacy, we take privacy as the fundamental right of users and regard the protection of user privacy as the prerequisite for supplying products and services.

1.2 Principles for Personal Data Processing

HONOR has established principles for personal data processing based on laws, regulations, and industry practices. We comply with the following seven principles when processing personal data globally:

Principle 1: Legality, legitimacy, and transparency

Personal data shall be processed in a legal, legitimate and transparent manner. Personal data shall be processed in a way that complies with legal regulations and has a basis of legitimacy. Personal data shall be processed for legitimate purposes and in a justified manner. A privacy statement shall be provided to users before the processing of personal data to succinctly and objectively describe the type of personal data to be processed, the purpose of processing, the retention period, the rights of personal data subjects, and other key information. Also, the consent from users shall be obtained or other basis of legitimacy shall be established according to law.

Principle 2: Purpose restriction

Personal data shall only be processed for clear and legitimate purposes. The purposes for which personal data are processed shall be directly related to the services provided and it is prohibited to misuse personal data beyond the stated purposes. HONOR will seek permission of the individual concerned to process personal data for new purpose (where required) or otherwise ensure that it has a solid legal basis to do so.

Principle 3: Data minimization

Personal data shall be processed to the relevant, necessary, and minimal extent based on the purpose. Personal data shall only be processed on a minimal and essential basis and shall not be collected beyond the scope of the business purpose. Personal data shall be anonymized or pseudonymized as much as possible to mitigate the impact on personal data subjects without affecting services and experience.

Principle 4: Information accuracy

Based on the purpose of processing personal data, reasonable measures shall be taken to ensure that inaccurate personal data are deleted or corrected in a timely manner, so as to avoid adverse effects on personal rights and interests due to inaccurate and incomplete personal data.

Principle 5: Minimum storage period

Personal data shall not be stored for a period longer than what is necessary to achieve the purposes for which they are processed. Instead, they shall be kept only for the shortest period necessary to achieve the purposes, and erased or anonymized completely and timely when the retention period expires.

Principle 6: Integrity and confidentiality

Appropriate technological or managerial measures shall be taken during the processing of personal data to ensure data security. Those measures shall include secure channels for transmission, encrypted storage of personal data, and the control of access to personal data. The purpose is to avoid accidental or unlawful destruction, loss, alteration, unauthorized access to, and disclosure of personal data.

Principle 7: Accountability

By constructing a personal data protection system, we can establish a personal data protection organization, appoint personal data protection owners, formulate requirements for personal data protection and management, carry out routine assessments on the protection of personal data, and record personal data processing activities. In this way, we make every process traceable and accountable.

02 We Build a Sophisticated Privacy Protection and Management System

HONOR has built a comprehensive privacy protection system in terms of organizational structure, management requirements, process integration, corporate culture, and tool platform. Our privacy protection system is shown as follows:

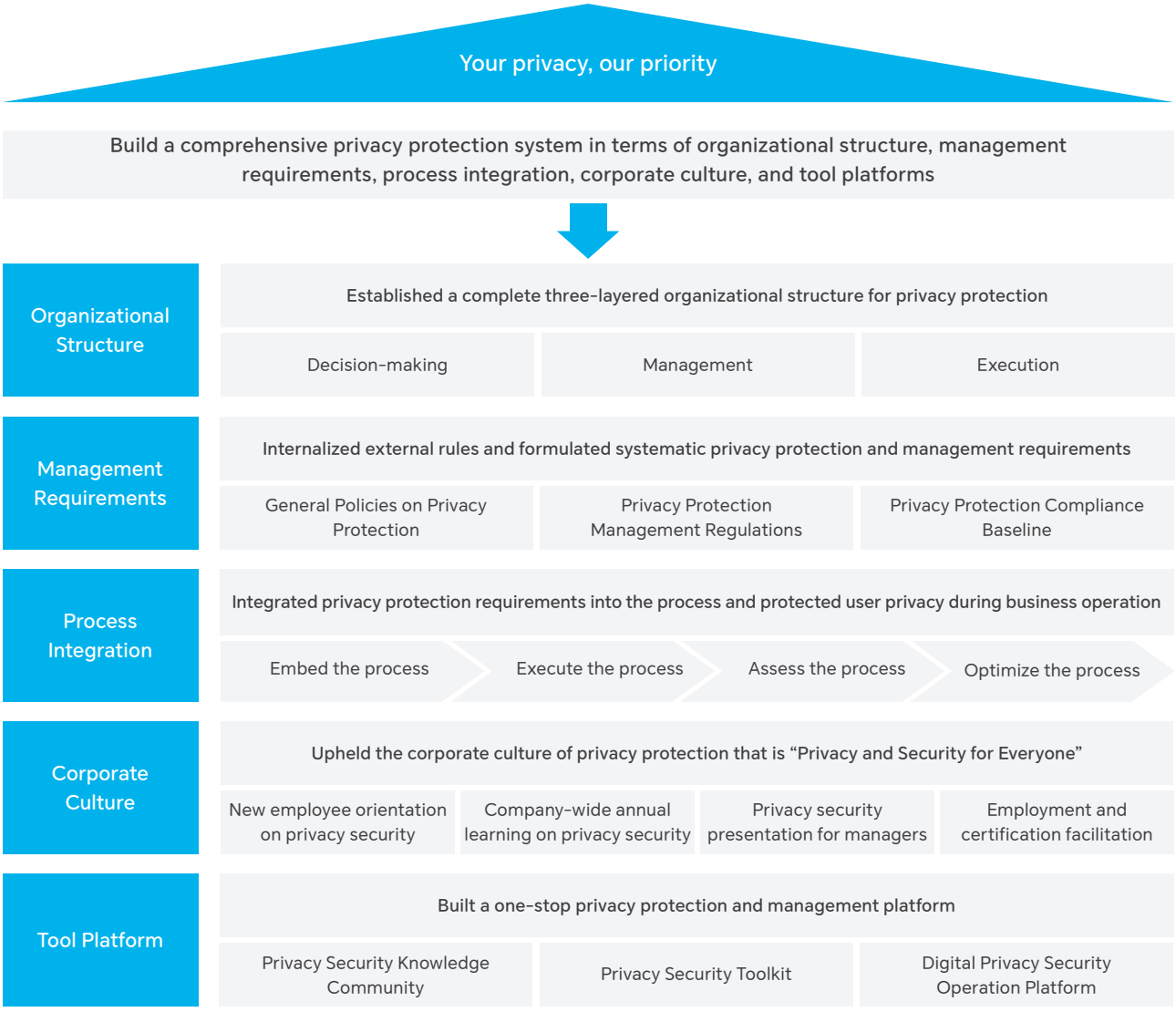


Figure 2-1: HONOR’s privacy protection system

2.1 Organizational Structure

HONOR has established a complete organizational structure for privacy protection. Its composition is shown in the figure below:

HONOR has established a complete three-layered organizational structure for privacy protection. The Global Cyber Security and Privacy Protection Committee (GSPC), as a decision maker, is the supreme governing body for the cyber security and privacy protection of the company. GSPC is chaired by the Global Cyber Security and Privacy Officer (GSPO) and reports to the CEO. The Privacy Protection Joint Conference (PPJC) as a business manager, governs routine privacy protection and management of the company. It is operated by the Privacy Protection & Compliance Department and reports to GSPC. Each business organization and regional organization has its own privacy engineers in place who, as executive managers, are responsible for implementing the privacy protection measures of their organizations. The organizational structure of HONOR's privacy protection function is shown in the figure below:

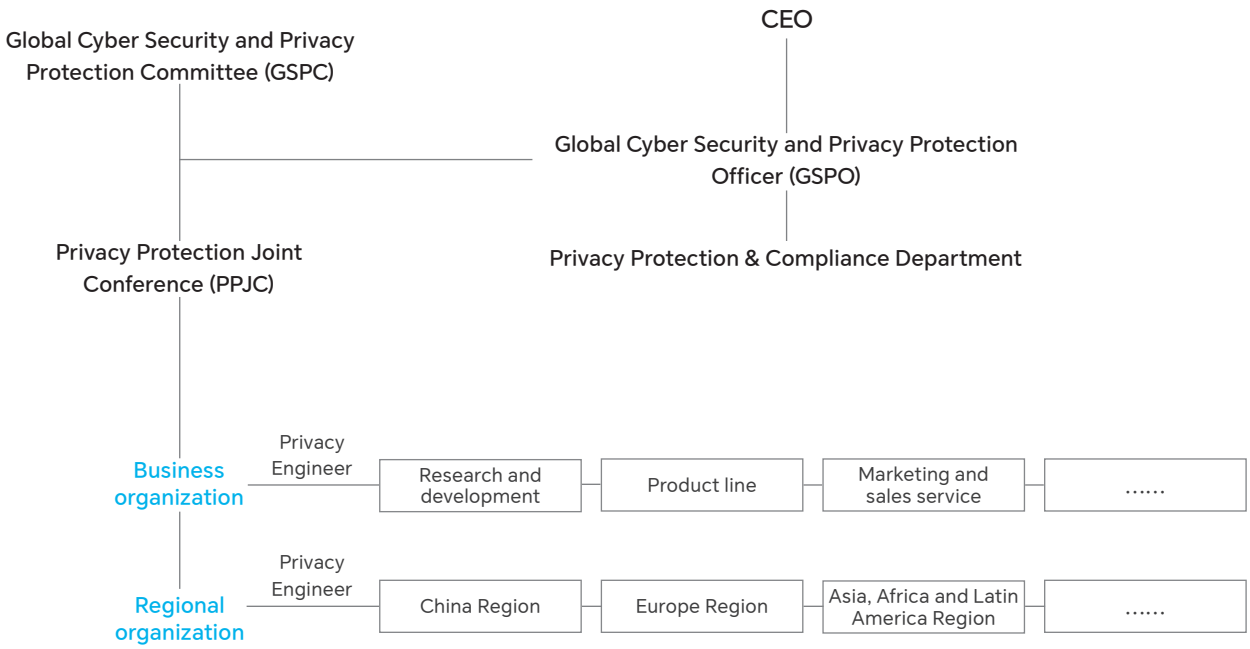


Figure 2-2: HONOR's organizational structure of privacy protection

2.1.1 Global Cyber Security and Privacy Protection Committee

The Global Cyber Security and Privacy Protection Committee (GSPC) is the highest governing body of HONOR for cybersecurity and privacy protection whose members are appointed by the CEO. Main duties of the GSPC include: directing HONOR's cybersecurity and privacy protection strategy and investment decisions; reviewing HONOR's cybersecurity and privacy protection technology planning; reviewing HONOR's annual work plans for cybersecurity and privacy protection in each business sector; investigating major privacy security incidents, applying administrative improvement measures, and identifying accountabilities.

2.1.2 Global Cyber Security and Privacy Officer

The Global Cyber Security and Privacy Officer (GSPO) is HONOR's head of cybersecurity and privacy protection, who is appointed by and reports to the CEO. Main duties of the GSPO include: formulating HONOR's directions and objectives of cybersecurity and privacy protection; steering the implementation of cybersecurity and privacy protection measures; overseeing the implementation of cybersecurity and privacy protection plans; resolving major issues in a timely manner; building up a managerial team of cybersecurity and privacy protection; selecting and training cybersecurity and privacy protection professionals.

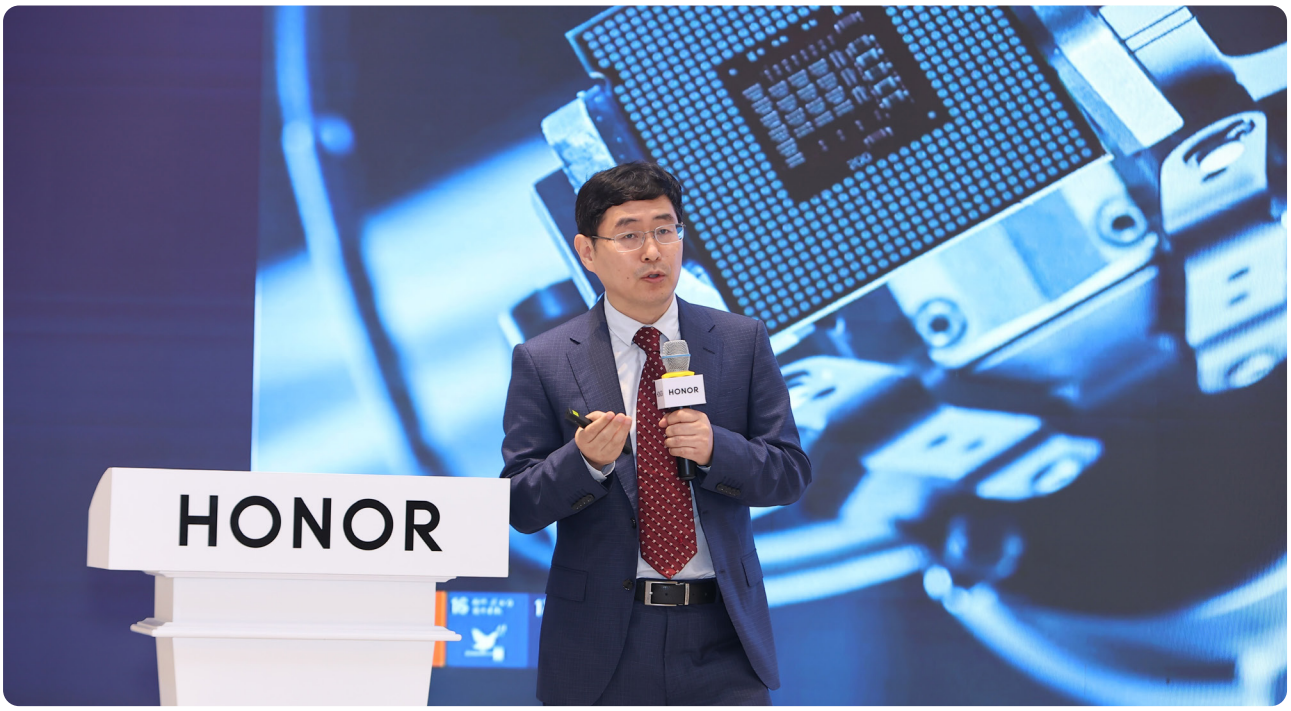


Figure 2-3: HONOR's GSPO Ma Bing was expounding on HONOR's privacy practices at the Launching Ceremony of the Environmental, Social and Responsible Governance Report on April 21, 2023

2.1.3 Privacy Protection Joint Conference

The Privacy Protection Joint Conference (PPJC) is responsible for the routine privacy protection management duties of HONOR. Its members, who are appointed by GSPC, include privacy experts from various business sectors. Main duties of the PPJC include: interpreting privacy laws and regulations and summarizing excellent practices in the industry; formulating HONOR's technical standards, specifications and baselines for privacy protection; assessing the compliance of privacy protection programs of various business sectors and guaranteeing the compliance of business launch.

2.1.4 Privacy Protection & Compliance Department

The Privacy Protection & Compliance Department is an entity of HONOR for privacy protection management. Its main duties include: building HONOR's privacy protection system; constructing the privacy protection organization, process and tool platform; running the GSPC and the PPJC; managing HONOR's privacy compliance risks; carrying out routine privacy compliance inspections; tracking the implementation of risk management measures; developing a team of privacy experts; enhancing the capacities of privacy protection practitioners; holding routine privacy training sessions and awareness promotion activities.

2.1.5 Privacy Engineer

Appointed by the GSPO, a privacy engineer is a person in charge of privacy protection in a business sector. HONOR has appointed privacy engineers for each business sector and region. Main duties of a privacy engineer include: designing the privacy protection compliance program in the current area; handling the requests of personal data subjects in the current area; taking charge of privacy protection risk management in the current area; steering the creation of a privacy protection culture in the current area.

2.2 Management Requirements

Framed by the Generally Accepted Privacy Principles (GAPP) of the industry and based on GDPR and Personal Information Protection Law of the People's Republic of China, HONOR has adapted itself to different statutory and regulatory requirements of countries and regions, and has formulated and released the General Policies on Privacy Protection, the Privacy Protection Management Regulations, the Privacy Protection Compliance Baseline, and other administrative regulations, so as to make sure that HONOR always meets those requirements when operating business in those countries and regions around the world.

The General Policies on Privacy Protection is the outline of privacy protection. It specifies HONOR's general policies for privacy protection, expounds on our basic principles and general requirements for the processing of users' personal data, stipulates the organizational responsibilities and duties of different departments of HONOR in protecting personal data, authorizes the Internal Audit Department to independently audit the privacy protection performance of each department, and proposes principles and requirements for investigating the violation of privacy protection policies.

Designed to implement the requirements of the General Policies on Privacy Protection, the Privacy Protection Management Regulations stipulates specific requirements for the processing of personal data in all business sectors, including conducting the Privacy Impact Assessment (PIA) and observing the Privacy Protection Compliance Baseline. It also clarifies administrative requirements regarding the implementation of personal data subject requests, the formulation of emergency response plans, the conduct of drills, and the grading and accountability investment for privacy protection violations.

The Privacy Protection Compliance Baseline breaks down the requirements set forth in the Privacy Protection Management Regulations into scenario-based check items and implementation guidance, clarifies the specific requirements for each stage of personal data processing, and proposes different requirements for different regions, business scenarios and populations.

HONOR holds routine sessions to interpret external laws, regulations, regulatory requirements, and law enforcement cases to gain insights into industrial practices. We also incorporate the latest external requirements and excellent practices into our own regulation system to secure the integrity of administrative requirements for privacy protection.

2.3 Process Integration

By embedding privacy protection requirements into the execution, evaluation, and optimization processes, HONOR can ensure the effective implementation of those requirements in business.

At present, HONOR has embedded privacy protection requirements into business processes that involve personal data processing, including R&D, supply chain, procurement, sales services, administrative services, financial management, and human resource management. For example, activities such as PIA, cybersecurity design, open-source and third-party software cybersecurity assessment, and privacy compliance review before the service launch have been embedded into the R&D process; requirements for incoming material security, manufacturing security, anti-tampering in the transportation process, and personal data erasure for returned materials have been embedded into the supply process; requirements for due diligence on privacy protection by suppliers/ partners and signing of data processing agreements have been embedded into the procurement process; requirements for conducting PIA in marketing campaigns and enabling the maintenance mode when repairing products have been embedded into the sales service process.

HONOR adopts a mature quality management system to supervise consistently the execution of business processes, evaluate the compliance performance of privacy protection activities, identify promptly possible deviations and risks in execution, analyze the root causes of identified risks, formulate improvement measures, and optimize processes.

2.4 Corporate Culture

HONOR upholds the corporate culture of privacy protection that is “Privacy and Security for Everyone”. To make sure every employee has an accurate understanding of our user privacy protection and strictly implements our privacy protection regulations and processes at work, HONOR has established a complete privacy protection training system for all employees (including new ones), privacy protection specialists and managers.

HONOR values the engagement of all employees in privacy protection and has developed a privacy protection training curriculum for all employees. Every year, HONOR holds learning sessions and exams for all employees to improve their privacy protection awareness.

HONOR attaches great importance to the development of expertise for privacy protection specialists. In this regard, we require privacy engineers and privacy COEs to learn the professional knowledge and pass exams before they can take up their posts; regularly organize professional privacy protection skill training to enhance the capabilities of privacy protection specialists; and require them to acquire professional certifications regarding privacy protection.

HONOR also requires managers to stay updated with new knowledge, learn and master privacy protection requirements on a regular basis, and be able to make proper decisions and communications in daily activities.

On January 28 of each year (Data Privacy Day), HONOR launches the Privacy Protection Week where various privacy protection campaigns are held, including annual speeches on privacy protection delivered by the chairman or CEO, introduction to global privacy protection legislation and privacy protection tips, promotion of privacy protection cases, and online communication in the privacy community. By doing so, HONOR keeps improving the privacy protection awareness for all employees and practicing the corporate culture of privacy protection.

2.5 Tools Platform

HONOR has systematically built a one-stop privacy protection and management platform, which covers the Privacy Security Knowledge Community, the Privacy Security Toolkit, and the Digital Privacy Security Operation Platform to support the efficient management and operation of the privacy protection business.

The Privacy Security Knowledge Community covers laws and regulations, managerial requirements, implementation guidelines, business practices, insights and consultations, training and empowerment, AI governance, and Q&A. Meanwhile, technologies such as intelligent search and large model Q&A were introduced to improve the experience of knowledge retrieval and interaction. HONOR provides routine maintenance and supplements to privacy protection knowledge, allowing employees to rapidly find, access, and exchange relevant knowledge on privacy protection via the Community.

The Privacy Security Toolkit includes PIA tools, protocol management tools, and Key Management Service (KMS), which are used to efficiently support the implementation of privacy security requirements and guarantee privacy security throughout the process ranging from product development, release, and operation & maintenance to after-sale services.

The Digital Privacy Security Operation Platform encompasses Online Business Review, Data Subject Request (DSR), Vulnerability Management, and many other systems and dashboards, facilitating privacy security operators to manage and supervise the implementation of privacy security measures.

03 We Protect Personal Data Through the Entire Life Cycle

HONOR has established a long-term mechanism for personal data protection based on GAPP, which covers all aspects of personal data processing, including notification to data subjects, options and consent from data subjects, data collection, use, retention and disposal, disclosure to a third party, cross-border transfer of data, and the rights of data subjects. The purpose is to ensure that users are given full-lifecycle protection.

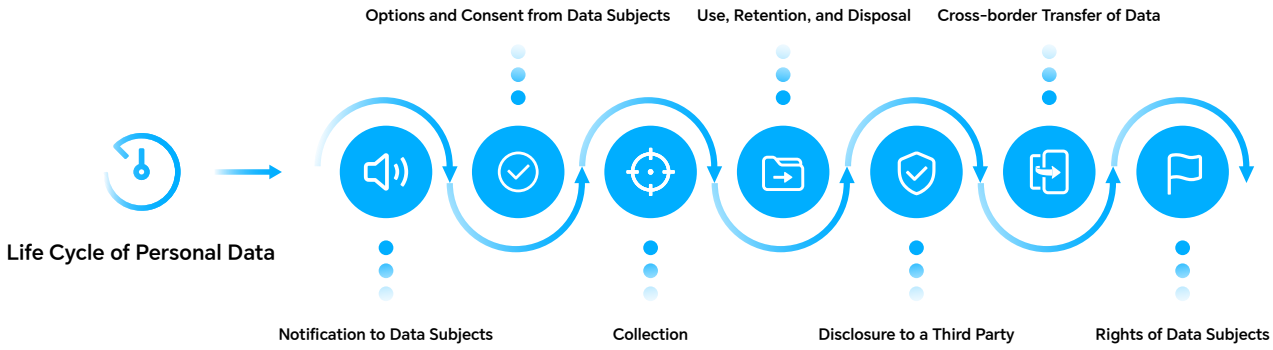


Figure 3-1: Life cycle of personal data

3.1 Notification to Data Subjects

Before collecting personal data from users, HONOR provides a clear and concise privacy statement that truthfully and accurately informs users of personal data processing details such as processing purpose, processing methods, personal data type, and retention period, so as to make sure users are fully informed. At the same time, users may review the privacy statement at any time. In the event of changes in the processing of personal data, HONOR will promptly update the privacy statement.

3.2 Options and Consent from Data Subjects

After users are fully informed, HONOR will provide them with the right to choose and decide before processing their personal data, and HONOR will collect users' personal data only after obtaining their consent (or according to other lawful bases). HONOR will obtain express consent from users before processing sensitive personal data. Meanwhile, HONOR allows users to withdraw the permission for personal data processing in a convenient way at any time where provided for by local laws.

3.3 Collection

HONOR collects personal data in accordance with its privacy statement and the data minimization principle. Meanwhile, HONOR takes into account specific business scenarios and adopts privacy-enhancing technologies for personal data such as pseudonymization, anonymization, and differential privacy to make sure users' privacy is protected.

3.4 Use, Retention, and Disposal

HONOR follows the principle of purpose restriction in the use of personal data. With the privacy compliance review before the service launch, we ensure that personal data are used in strict accordance with the privacy statement and in the scope specified in the agreement, and well-developed security technologies and measures are used to ensure that personal data are not leaked. In the event of changes in the purpose for which personal data is used, HONOR will ensure that it obtains permission from the individual concerned or otherwise has a valid legal basis to do so.

HONOR strictly classifies and manages personal data of users and has formulated and released the Personal Data Categorization, Grading and Protection

Specification that classifies personal data into four privacy levels, namely, "very high", "high", "medium", and "low", based on the content, attributes, uses, and application scenarios of personal data. HONOR also develops corresponding security policies and control measures for different privacy levels. For screen-lock passwords, fingerprints and face information, HONOR encrypts and protects that information by using local, independent secure storage chips on the phone to ensure security. Models used to provide AI-based automated decision-making services are deployed and run locally on the phone. It is required that the data used for training and learning must be stored locally on the phone and algorithms must be fair and unbiased.

HONOR only stores personal data necessary for the provision of services. Except as otherwise provided by laws and regulations, HONOR will delete or anonymize personal data at the end of services, or when personal data subjects exercise the right to deletion, or in other circumstances.

3.5 Disclosure to a Third Party

HONOR shares personal data necessary for the services with third parties based on the principle of data minimization. Before sharing personal data with a third party, HONOR will conduct a PIA beforehand, including performing due diligence on the third party, to ensure that the third party is capable enough for privacy security. HONOR will also sign a privacy security agreement with the third party, requiring it to use personal data in strict accordance with the agreement, take security measures to protect personal data, and strictly prohibit the use of personal data for other purposes. Also, HONOR will provide users with a privacy statement to fully indicate the type of personal data shared, the purpose of use, and other information.

3.6 Cross-border Transfer of Data

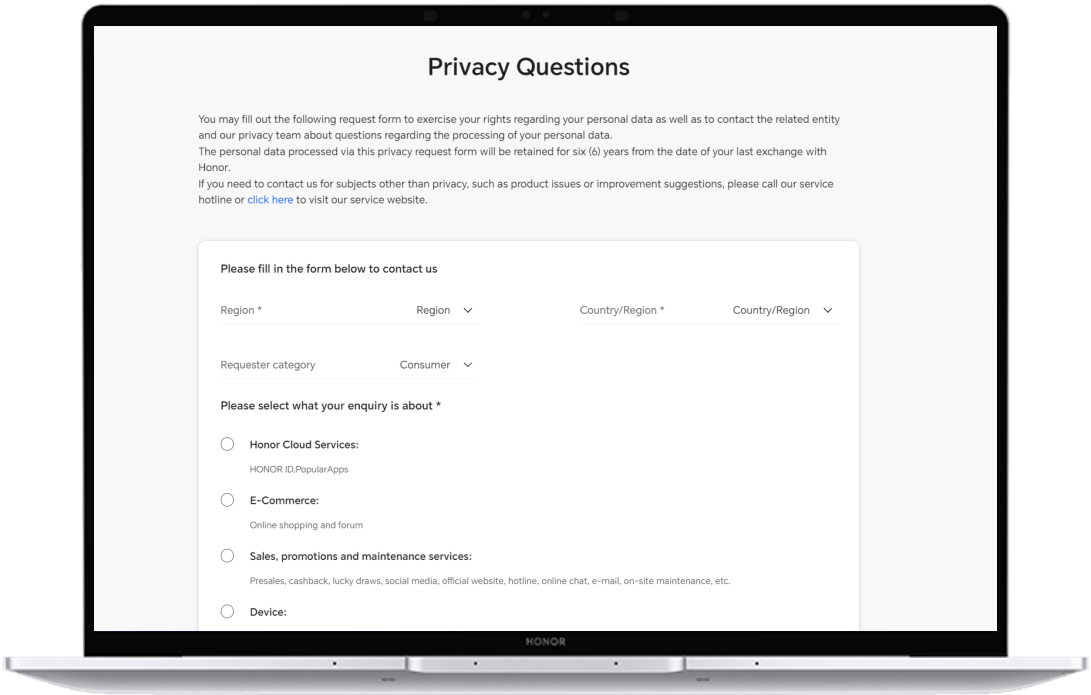
HONOR strictly complies with the legal and regulatory requirements for cross-border transfer of personal data in the countries or regions where the business is located. In principle, HONOR applies localized deployment, operation, and O&M to reduce unnecessary cross-border transfer of personal data. Currently, HONOR has established multiple local data centers around the world to meet the requirement for data localization. If the cross-border transfer of personal data is unavoidable, HONOR develops a compliant cross-border transfer program in strict accordance with the legal and regulatory requirements of the country or region in which the sender of personal data is located. We also conduct regular PIAs on the cross-border transfer of personal data to make sure it satisfies the legal and regulatory requirements of the relevant country or region.

3.7 Rights of Data Subjects

In order to make sure that users are able to exercise the rights granted to them by laws and regulations, HONOR provides an array of ways for personal data subjects to exercise their rights, which are shown as follows:

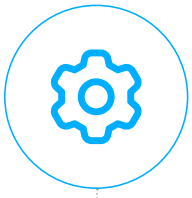
Users can obtain a copy of their personal data in bulk by visiting "HONOR ID\Privacy centre\Get a copy of your data" on their terminal devices.

When users' needs cannot be addressed in the way mentioned above, users can also submit a personal data subject request by visiting the HONOR Privacy Issues page on the HONOR Portal (https://www.honor.com/global/privacy/feedback/) to exercise the right of access, correction, deletion, and portability. HONOR has designated a dedicated person to handle users' requests as personal data subjects. After receiving users' requests, HONOR will handle them in a timely manner in accordance with the requirements of relevant laws and regulations.



04 We Integrate Privacy Protection into the Product Development Process

Protecting user privacy is the most basic prerequisite for HONOR to provide products and services. From the initial product design to the final service provision, HONOR finds ways in every stage to better protect user privacy and give users independent control over their personal data.



4.1 Proactive Prevention in the Product Research and Development Process

Privacy protection is an indispensable part of product design. In this regard, HONOR lives out the Privacy by Design (PbD) concept. In product design, we follow the principles of pre-event prevention, and protection of user privacy by default and so on. The PIA must be completed for all products in the development stage, including identifying PIA requirements, sorting out personal data lists and information streams, providing a privacy statement, identifying privacy-related risks, and designing a privacy protection program. The purpose of PIA activities is to ensure that products meet the requirements of users for privacy protection.

4.2 Rigorous Review Before Product Launch

In order to ensure that the products delivered strictly meet the privacy protection laws and regulations of countries or regions, HONOR has issued the Management Regulations on Privacy Compliance Review for Business Rollout. All products must receive and pass the rigid PPJC review before being launched. In order to guarantee the professionalism and objectivity of the privacy compliance review, the PPJC consists of privacy experts from different business sectors and is responsible for the results of the privacy compliance review.

4.3 Full Protection of Product O&M Processes

First of all, HONOR has formulated a series of O&M management specifications to define the privacy protection requirements of products in the O&M stage. Furthermore, HONOR has established a perfect operation and maintenance support platform to strictly control the permissions of operation and maintenance personnel in the principles of work relevance and minimum permission. Measures include the strict control and management of personal data addition, deletion, modification, inquiry, export and other operations. Meanwhile, HONOR fully records and routinely reviews the operation logs of all O&M personnel to make sure their behaviors are compliant and traceable. In addition, HONOR has constructed a privacy management platform to anonymize and obscure the personal data carried in the business system and make sure that the operation and maintenance personnel cannot have direct access to users' personal data, thus putting the personal data under protection. In order to meet the requirements of countries or regions for cross-border data transfer, HONOR has also established a local O&M team to respond to users' privacy and security issues in a timely manner and protect their rights and interests.

4.4 Systematic Management of Product After-Sales Service

HONOR conducts systematic privacy protection training and induction exams for after-sales service engineers, and requires them to perform repairs by using HONOR-designated tools to avoid data loss or leakage during the repair process.

In the process of providing users with after-sales services, the After-sales Service Center provides users with clear after-sales service guidance and privacy protection tips to protect data on users' devices. Those guidance and tips include reminding users to keep a data backup before having it repaired and enabling the maintenance mode during the repair.

Data are erased by HONOR from the products returned by users according to the corresponding management requirements. Parts and complete machines to be scrapped are destroyed irreversibly to make sure personal data in products are completely destroyed and will not be leaked.

05 We Provide Users with All-around Privacy Protection Experience

HONOR protects user privacy in every aspect when they are using HONOR products, allowing them to feel HONOR's respect and care for their privacy and rights. Around the use scenarios of users, HONOR has developed privacy protection features in five dimensions and is continuously improving them for products. With innovative privacy solutions and technologies, HONOR is committed to providing users with all-around privacy protection services.

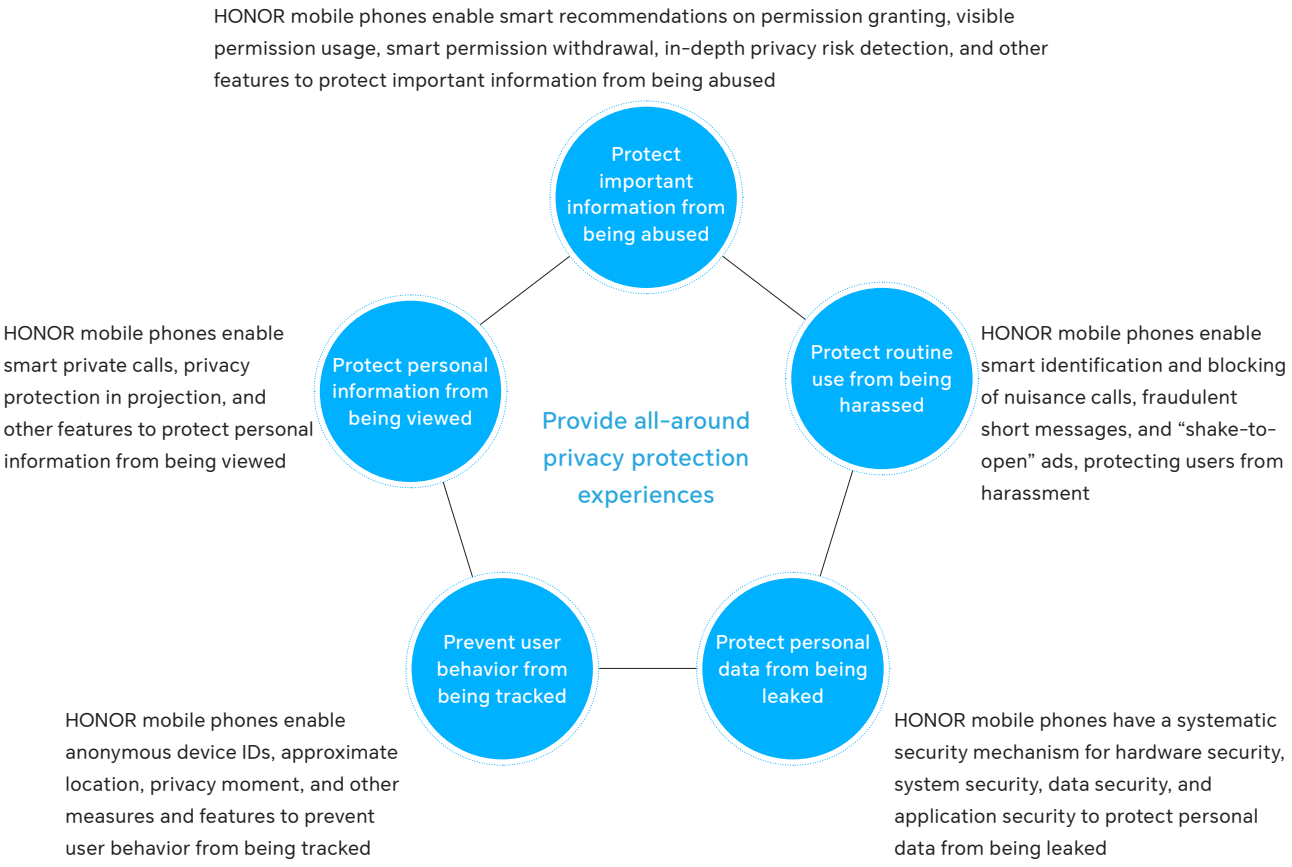
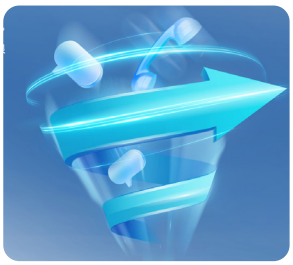


Figure 5-1: Five dimensions of HONOR Privacy Protection

5.1 Protect Important Information from Being Abused

Personal data may be misused in the following ways including excessive requests for permission by apps, function block by apps without permissions, and malicious reading of personal data and clipboard information obtained by apps in background. HONOR mobile phones provide the users with the function of deep privacy risk detection based on minimum permissions, visible permission adoption, and smart permission withdrawal, allowing users to have a real-time understanding of their mobile phones' privacy security status and prevent personal data from being abused in a systematic manner.

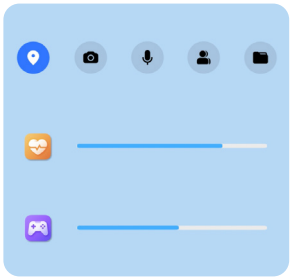
5.1.1 “App Permission Minimization Recommendation” Ensures Minimal App Permission



“App Permission Minimization Recommendation” is an intelligent tool to suggest the minimal permissions required for users. By analyzing the basic functions and use scenarios of apps and in combination with relevant standards and specifications, HONOR has launched the “App Permission Minimization Recommendation” feature to recommend permission for users when they launch the app, so users will have a way to give minimal permissions quickly and have their rights of choice better protected.

5.1.2 “Privacy Assistant” Provides In-depth Detection for Privacy Security

"Privacy Assistant" is a privacy security detection service provided by HONOR for its phone users, which allows them to know the privacy security status of their phones anytime anywhere. "Privacy Assistant" runs in-depth detection in terms of system environment, payment environment, and application behaviors, and provides one-tap optimization. It will provide a privacy security detection report and inform users of blocked app harassment and unauthorized access at the beginning of each month.



5.1.3 “Privacy Access Records” Makes Logs Viewable Anytime

“Privacy Access Records” allows HONOR mobile phone users to check app permission access Records. With this feature, users can see the permission access records of all apps in the past 7 days, facilitating users to check app permissions for reasonability and cancel unreasonable permission access at any time. This can avoid excessive permissions by apps or over-frequent acquisition of personal data.

5.1.4 Automatic Erasure of Clipboard to Avoid Malicious Reading

When we are using mobile phones every day, important information is inevitably stored on the clipboard, such as the recipient's information, telephone, email, and even passwords. To avoid user information from being leaked, HONOR’s phones will automatically clear the clipboard 15 minutes after it is updated. In addition, the system will notify users by displaying a message when the app reads the clipboard.

5.2 Protect Routine Use from Being Harassed

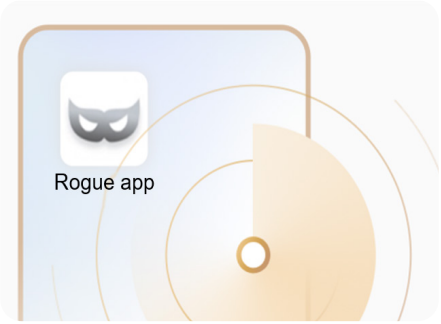
Users may be harassed in daily use scenarios of mobile phones. Common harassment concerns include marketing SMS, marketing calls, fraudulent calls, and app notifications. HONOR mobile phones can effectively intercept or block this kind of harassment.

5.2.1 “Intelligent Identification” Prevents Telecom Fraud

HONOR mobile phones can effectively identify fraudulent calls, short messages, and apps to keep users away from fraudulences. When a user receives a fraudulent phone call, the system will carry out targeted interception and warning. When a user receives a fraudulent short message, the system will intercept it too. Even if the message is covert and escapes system detection, the system will send an alarm when the user is replying to the fraudulent short message. When a user is installing and using a fraudulent app, the system will detect the risk and send an alarm.

5.2.2 “Intelligent Authorization” Reduces Pop-up Windows

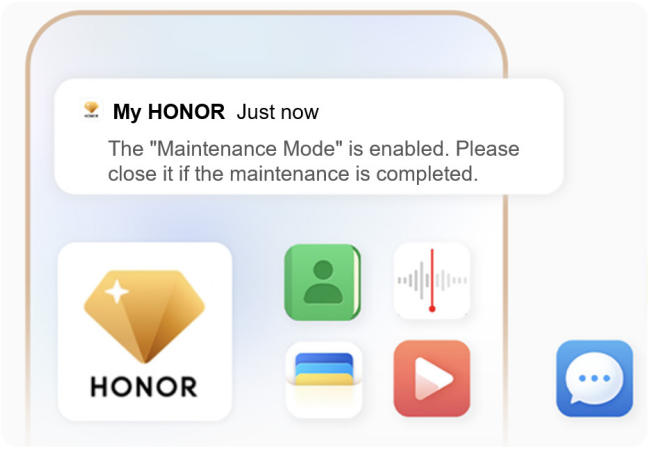
HONOR mobile phones can effectively reduce the frequency of pop-up windows to avoid disturbing users. When a user rejects the permission of an app twice, the system will smartly identify the permission and automatically block the permission request of that app. If the user needs to use the permission in later days, he/she can grant the authorization by visiting the system permission management interface.



5.3 Protect Personal Data from Being Leaked

Leakage of personal data can lead to serious consequences, and personal data can be leaked in many ways. HONOR mobile phones have a systematic security mechanism to protect users' personal data security, covering hardware security, system security, data security, and application security. For screen-lock passwords, fingerprints and face information of phones, HONOR encrypts and protects that information by using local, independent secure storage chips on the phone to prevent them from being maliciously obtained by apps. In addition, HONOR also systematically considers the protection of personal data in scenarios such as the use, maintenance, borrowing and loss of mobile phones to avoid personal data leakage.

5.3.1 “Maintenance Mode” Protects Privacy in After-sales Services



The “Maintenance Mode” is a system setting to protect users’ personal data from being unwillingly disclosed in after-sales scenarios. The Maintenance Mode encrypts users’ personal data with the best-of-class encryption algorithm to make sure personal data are protected. When the Maintenance Mode is enabled, the repairer will not have access to any personal data on the phone, which avoids the leakage of the user’s privacy. Once the repair is complete, the user can disable the Maintenance Mode by entering the screen-lock password and the phone will be back to normal.

5.3.2 Photo Sharing Enables One-tap Removal of Personal Data

HONOR mobile phones allow users to protect their privacy when sharing photos by erasing sensitive personal data such as locations and shooting data. When a user is sharing a picture, he/she can choose to enable the privacy protection function to erase the location where the photo was taken and other shooting data.

5.4 Prevent User Behavior from Being Tracked

The tracking of behavior is one of the greatest concerns of users. Common circumstances of behavior tracking include the tracking of location and activities, acquisition of the user behavior, and the tracking of device identifiers and Wi-Fi MAC addresses. By technological means such as anonymizing device identifiers and approximating location, HONOR mobile phones can prevent user behavior from being tracked on an ongoing basis.

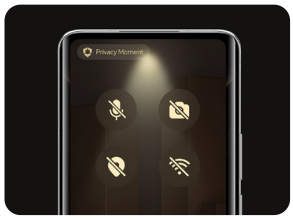
5.4.1 “Approximate Location” Prevents Apps from Locating or Tracking Users

HONOR mobile phones have a feature called “Approximate Location”, which can provide an approximate location to apps that don't need a precise location to prevent users from being located or tracked. When this feature is enabled, the system will provide an approximate location within a deviation of 1 square kilometer. This feature is ideal for apps that do not require precise locations such as weather forecasts or friending.

5.4.2 “Unknown Bluetooth Tag” Detects Malware Tracking

HONOR mobile phones provide users with the “Unknown Bluetooth Tag” feature to detect unknown Bluetooth connections and prevent users’ activity from being tracked. When a HONOR mobile phone detects a Bluetooth tag tracking the phone, it will remind the user so that the user can follow the sound to locate this unfamiliar Bluetooth tag and stop the malware tracking in time.

5.4.3 “Privacy Moment” Provides Ultimate Privacy Experience



The “Privacy Moment” feature in HONOR mobile phones allows users to focus on private conversations. When “Privacy Moment” is enabled, the Camera, Microphone, Location, Bluetooth and Internet functions will all be disabled. Only Phone, Contacts and Messages can be used and only calls from known contacts can be received to extensively protect users’ privacy.

5.5 Protect Personal Information from Being Viewed

In everyday scenarios of using mobile phones, the screen may be viewed by others, the album may be viewed by those who borrowed the phone, and phone calls may be heard in the crowded subway or elevator, leading to unnecessary embarrassment and trouble. In this regard, HONOR has developed systematic solutions for its mobile phones to address issues in mobile phone projectors, Sound leakage, mobile phone repair, and mobile phone borrowing.

5.5.1 Privacy Protection in Projection

HONOR mobile phones can protect users' privacy in device projection. When users are projecting their mobile phones onto a PC, a smart screen, or other large screens, the screen will not show WeChat messages, short messages, or other instant messages by default, nor will it display the screen of inputting the password, so as to prevent messages and passwords from being viewed.

5.5.2 "AI Privacy Call" Minimize Sound Leakage

Relying on innovative audio technologies and unique audio channel design, the "AI Privacy Call" supported by HONOR mobile phones can greatly mitigate sound leakage of phone calls. Users never have to worry about the leakage of calls, especially in an elevator, vehicle, or meeting, so as to keep their calls private and secure.

*The privacy protection features described in this chapter may vary depending on product models and system versions. Please refer to the actual situation of specific products.

06 We Build a Privacy Security Ecosystem With Partners

HONOR is committed to becoming an all-scenario, all-channel globally iconic tech brand for all. We choose to work with outstanding partners to create new things and build a security ecosystem, delivering users ultimate all-scenario smart life experience.

6.1 Privacy Security of the Hardware Ecosystem

HONOR never stops crafting a “human-oriented” smart life solution across applications and devices and delivering users seamless all-scenario experience. Those full-scenario solutions involve collaborative communication among multiple types of devices and the connection with third-party ecosystem products. HONOR has introduced control measures with MagicRing and ecosystem products to manage the privacy security of the hardware ecosystem.

6.1.1 MagicRing Supports Secure Collaboration Across Devices

HONOR devices support MagicRing, which is a ring of trust, and the identity-based authentication system. Different HONOR devices under the same account can automatically identify, network, and connect themselves in the low power mode. With the environment perception capability of devices and the platform-oriented AI capability of the smart engine Magic Live, HONOR enables free turnover and sharing of services. Functions such as Keyboard and Mouse Sharing, Notification Sharing, Call Sharing, and App Connectivity are now available across devices in an efficient and secure manner.

6.1.2 Privacy Security for Ecosystem Products Connection

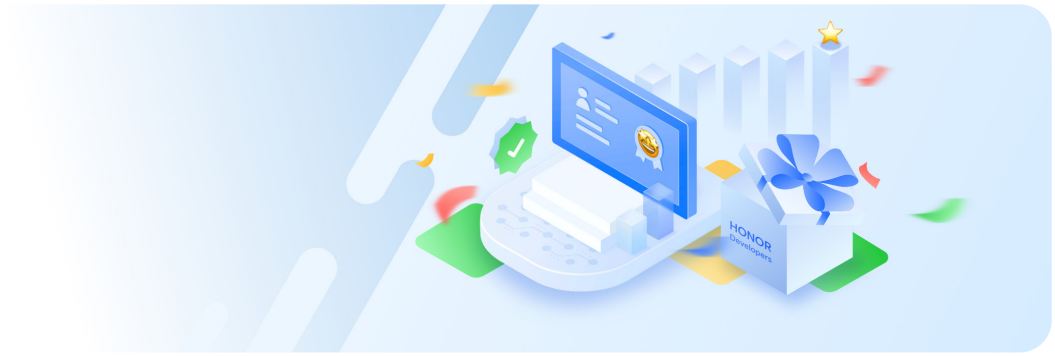
In order to effectively control the privacy security risks brought about by ecosystem products, HONOR has released the Administrative Regulations on Privacy Protection in all-scenario Integration of Ecosystem Products, which sets forth clear requirements for the privacy security of ecosystem products. HONOR will conduct due diligence on ecosystem product vendors that collect and store personal data to make sure they are capable of protecting users' privacy. Also, HONOR has also put forward clear privacy security requirements for ecosystem products. For example, ecosystem products shall be categorized and managed according to the types of products involved and the degree of data sensitivity; ecosystem products need to provide a privacy statement when processing personal data; ecosystem products need to pass the privacy security test before being admitted and the privacy security review before being launched.

6.2 Privacy Security of the Software Ecosystem

HONOR manages the privacy security of the software ecosystem by leveraging open capability privacy security control and HONOR App Market privacy security control.

6.2.1 Privacy Security for Open Capabilities

HONOR provides powerful open capabilities, with which developers can quickly and efficiently develop personalized features. HONOR manages the privacy security of the software ecosystem by means of open capability Kit delivery and developer integration of open capabilities.



All open capabilities of software available to developers need to undergo privacy security requirement analysis, privacy security design, and privacy security testing, and pass the privacy compliance review before they are released. When personal data are processed, HONOR will provide SDK compliant use instructions and SDK privacy statement in the Open Capability Kit to be released, thus allowing developers and users to understand how HONOR handles users' personal data.

HONOR imposes strict privacy security requirements for developers integrating open capabilities. HONOR reviews the qualification of developers and sign relevant agreements with them. HONOR requires developers to provide information about application signatures when developers create an app. HONOR requires developers to submit the due diligence report and verify the review result when their apps apply for data exchange. Developers must satisfy HONOR's integration requirements when their apps integrate open capabilities, such as citing HONOR's SDK privacy statement in the privacy statement of developers' apps. When an app is being used and applying for data exchange, a pop-up window needs to show up to gain the consent of the user. After the consent is granted, HONOR's open capabilities will verify the signature of the app and will only exchange data when the verification succeeds.

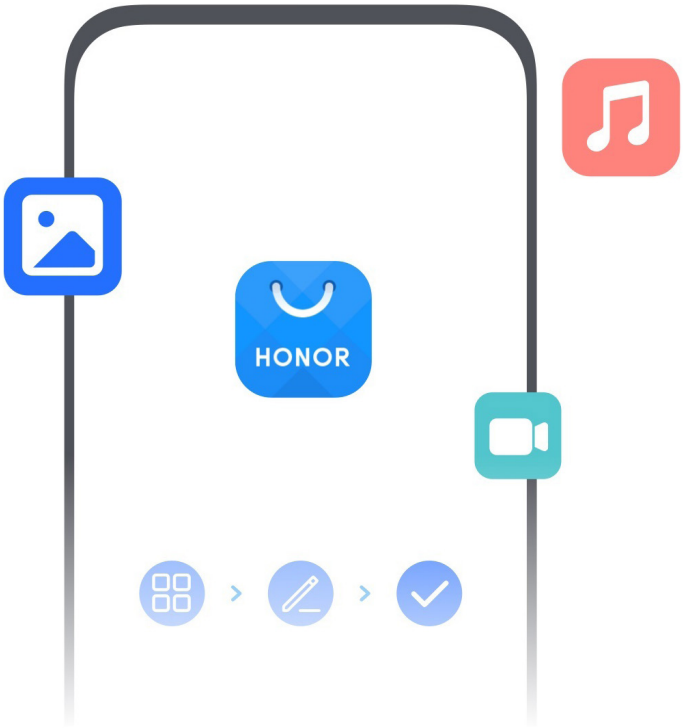
6.2.2 Privacy Security for HONOR App Market

The App Market is committed to building a safe and reliable app ecosystem for users. By reviewing apps before publishing apps, checking apps in the market, managing app levels, and other measures, HONOR provides users with rich experience in the privacy security of apps.

HONOR has set strict standards for reviewing apps before publishing them. When an application is filed for publishing an app, the App Market will accurately register and verify the information of the app and its developer and operator, and audit and technically test every app to be published. In this way, HONOR can control the privacy security of apps from the source.

HONOR routinely checks apps in the market. HONOR will pick out a proportion of apps for inspection based on the number of downloads, update time, and historical violation records, so as to make sure the disclosed information is consistent with reality.

The App Market allows developers to display privacy statements and permission details, facilitating users to fully understand how third-party apps process their personal data and what permissions are required to run the apps before installing apps. The App Market also supports app level management. After an app level is set, underage users can only install apps that are lower than or equal to the set level, so that the privacy security and physical health of the minor can be protected. In addition, the App Market also provides the “App Report” function. Users can report apps with privacy security violations and HONOR will verify and handle those reports received.



6.3 Partner Management

HONOR collaborates with partners in the hardware ecosystem construction, software ecosystem construction, marketing activities, and after-sales services. In order to ensure that the services provided by our partners can fully protect user privacy, HONOR has put forward demanding privacy protection requirements for our partners in access certification, daily management, and termination of cooperation.

In access certification, privacy security is one of the factors for admitting partners. When certifying a partner, HONOR will conduct due diligence on privacy protection, probe into the partner's capability of privacy security, review whether it meets privacy security requirements, and require the partner to sign a privacy security agreement and take necessary technological and administrative measures to protect personal data and prevent leakage, damage or loss of personal data.

In daily management, HONOR has set a routine mechanism to train or educate partners in privacy protection requirements, run self-inspections or audits on privacy protection for partners, identify risks timely and correct violations, and reduce business-related privacy security risks. Meanwhile, HONOR regularly evaluates the privacy security performance of partners, and requires the partners who fail the evaluation to make corrections within the time limit or ceases cooperation with them.

When ceasing the cooperation with a partner, HONOR will require it to stop processing personal data as agreed in the agreement, and require it to delete the data completely or return the data to HONOR.

6.4 Collaborative Innovation

As a company driven by product innovation and user experience, HONOR greatly values scientific research and innovation. We have incorporated patent management into the process of research, development, production, and operation while taking patent technologies as our core competitiveness. In the past few years, HONOR has constantly beefed up investments in privacy security and established a presence of patents with increased quantity and improved quality in terms of trusted execution environment, privacy computing engine, anti-telecom fraud, anti-harassment radar, and data security. HONOR has also established a line of joint privacy security innovation labs to keep providing users with comprehensive privacy protection experience through innovative privacy protection technologies.

*The privacy protection features described in this chapter may vary depending on product models and system versions. Please refer to the actual situation of specific products.

07 We Do More to Protect Privacy

While excelling in basic privacy protection, HONOR also values the privacy security experience of children and elder groups. Also, HONOR continues to improve privacy security experience in AI, payment, health, and smart life scenarios.

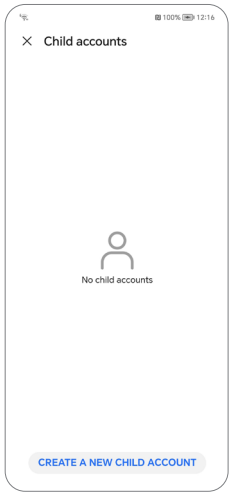
7.1 Protect Children's Privacy and Escort Them in the Way to the Digital World

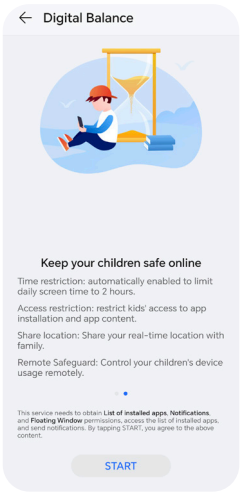
In the complicated Internet environment today, protecting the rights and interests of children has become a public concern. HONOR products value the protection of children's privacy and escort them along the way in the digital world with Child accounts - Parent Agreement, Digital Balance - the Children mode, the AI Space - Family, and other exclusive services.

Child identification is a prerequisite for protecting children's privacy. HONOR identifies children by child accounts. When child accounts are created, HONOR clearly informs parents or other guardians, through Parent Agreement, of the personal data that is necessary for HONOR to provide services for children, so that parents or other guardians understand HONOR's personal data processing activities and are given intuitive and complete control power.When children log into their accounts, the system will automatically match children identities, and provide parental authorization, default privacy protection, content control, remote management, and other features to protect children's privacy.

HONOR products are provided with the Healthy Mobile Life for Children mode in the operating system which, when enabled, will adopt content restriction, anti-ad tracking, and other restrictive measures to protect children's privacy.

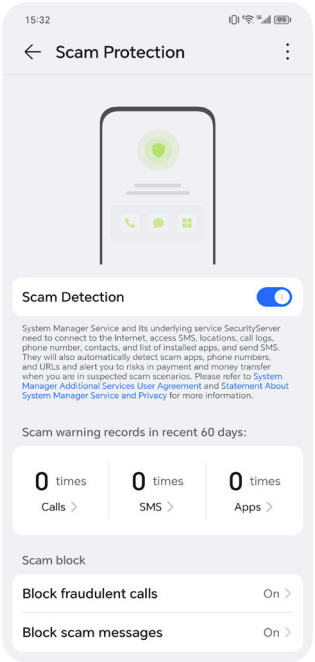
HONOR has also provided a children's privacy protection function based on the "AI Space - Family Space". Parents or other guardians can connect themselves to children's devices with this function to enable remote protection, remote positioning, setting of geo-fences, anti-fraud reminders, and many other functions that can better protect children's privacy.





7.2 Care for the Elderly by Keeping Them Safe from Internet Fraud

Due to economic and social advancement and the accelerated population aging, some criminals commit telecom fraud activities against the elderly by utilizing widely applied financial and information communication technologies. Those activities seriously jeopardize the property safety and physical & mental health of the elderly. HONOR has been focusing on the security of the elderly in the use of mobile phones, and is committed to keeping them away from Internet fraud by providing anti-fraud features and publicizing anti-fraud knowledge.

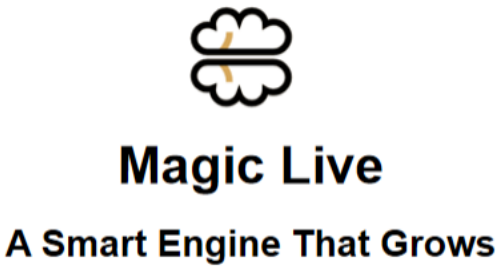


With an array of features such as virus detection, harassment blocking, malicious URL detection, fraud detection, WLAN security detection, protection against fake base stations, and reminders of external apps, HONOR mobile phones can keep the elderly from fraudulent short messages, fraudulent calls, and malicious apps, thus greatly reducing their chances of suffering Internet fraud.

The HONOR Club provides a “Security and Privacy Protection” section (https://club.honor.com/cn/forum-4530-1.html) where knowledge about privacy security and fraud prevention is released and senior users can learn how to prevent fraud.

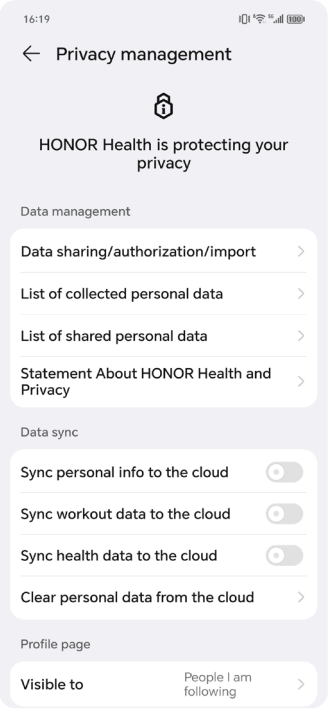
7.3 More Secure AI Services Based on End User Computing

The AI-enabled Magic Live smart engine allows end products to understand you better and function better. While facilitating people's lives, artificial intelligence also poses great challenges in the protection of user privacy.



HONOR always designs AI services based on privacy security and user experience, and builds “Trustworthy and Responsible” AI services systematically around the data, model and service. We use identifiers generated at the end instead of unique identifiers of devices to prevent misuse of user identity information. We support end-side AI models that only process required data in end devices, and carry out encrypted protection to the models at the hardware level by using the “Two Locks and One Chipset” technology, which is operated within the independent space of the device so as to avoid the tampering and replacement of the models effectively. We keep developing more transparent and easy-to-understand operation interfaces and explanations, so that every user can enjoy the convenience of smart services while gaining a full picture of the principles of smart services and managing them at any time.

7.4 HONOR Health with Independent Control of Users' Personal Data



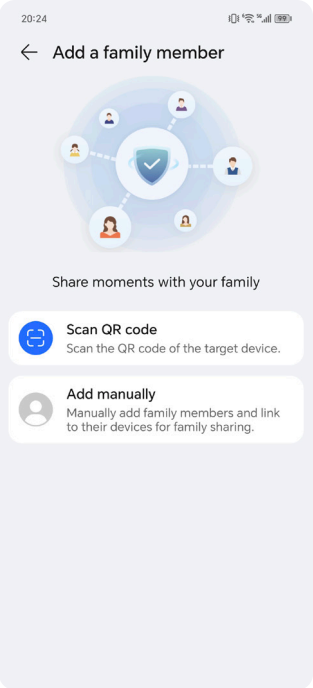
HONOR Health allows users to record and analyze fitness and health data. Since it involves sensitive personal data of users about fitness and health, privacy risks may occur against users once the data are shared or leaked illegally. HONOR protects the privacy and data of users by means of protection of user privacy by default, user-controlled data uploading to the Cloud, user-controlled data sharing, secure transmission, and encrypted storage.

By default, HONOR Health does not collect users' personal data, and will only do that after gaining consent from users. When performing statistical analysis of users' data and improving user experience, we adopt the differential privacy technology and add random noise to users' data to prevent the real data from being obtained by the cloud and therefore protect the privacy of users.

HONOR Health saves exercise and health data locally on the phone by default. Users can decide on their own whether to back up the data to the cloud as needed so that data can be accessed from different devices. Users can also clear the data in the cloud at any time. Also, users can choose to share exercise and health data with other apps or users, or stop the sharing at any time, which is fully controllable.

HONOR Health also provides users with all-around protection of data security by means of end-to-end transmission channels. All the data uploaded by users to the cloud are encrypted with a secure encryption algorithm before being stored.

7.5 HONOR AI Space Protects the Privacy Security of Families



HONOR AI Space is a unified management platform that can identify, connect, and manage HONOR all-scenario smart devices and HONOR Connect eco-intelligent products. It enables the interconnection of smart devices and the creation of an exclusive and colorful intelligent space. HONOR AI Space is connected to various third-party smart home devices. Once a third-party smart home device is hacked or controlled, it will lead to the exposure of users' private space and privacy. Therefore, HONOR protects the privacy of users and their families by applying well-developed security technologies, privacy security control for ecosystem products, and the Family Space Protection feature.

HONOR applies multiple security measures to secure the access authentication, transmission, and storage from IoT devices to mobile phones and from mobile phones to HONOR AI Space servers. Other measures include the authentication of identity on the client side, support for end-to-end secure transmission channels, encryption of transmission channels, and encryption of stored sensitive data.

HONOR will conduct due diligence on ecosystem product vendors that collect and store personal data to make sure they are capable of protecting users' privacy. Meanwhile, HONOR has also put forward clear privacy security requirements for ecosystem products. For example, ecosystem products shall be categorized and managed according to the types of products involved and the degree of data sensitivity; ecosystem products need to provide a privacy statement when processing personal data; ecosystem products need to pass the privacy security test before being admitted and the privacy security review before being launched. HONOR AI Space is equipped with the Family Space protection feature, with which parents or other guardians can connect themselves to family members' devices to enable remote protection, remote positioning, setting of geo-fences, anti-fraud reminders, and many other functions that can better protect the privacy of family members.

*The privacy protection features described in this chapter may vary depending on product models and system versions. Please refer to the actual situation of specific products.

08 We Are Always Communicative and Transparent

HONOR always complies with applicable privacy protection laws and regulations, and continuously strengthens the construction of privacy protection systems and capacities. In addition, HONOR communicates and cooperates with global regulators, consumers, certification bodies and industry associations in a transparent and open manner.

8.1 Cooperation with Regulators

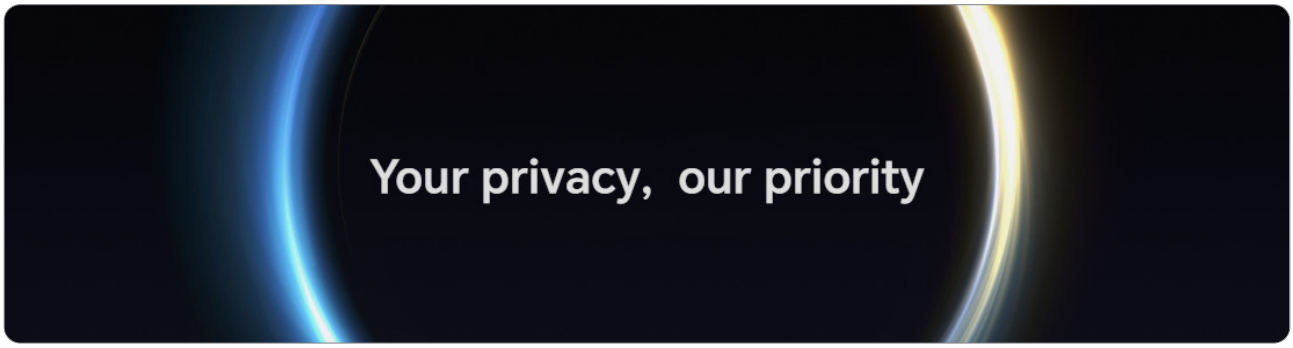
HONOR has always maintained a close eye on regulatory requirements and dynamics and actively communicated with the regulatory bodies where the business is located. We comply with regulatory requirements and respond to their requests in a timely manner. In Europe, HONOR has appointed a Data Protection Officer (DPO) who is responsible for HONOR's personal data protection and compliance in Europe. In countries or regions where businesses is conducted, HONOR has appointed privacy engineers to implement regulatory requirements in collaboration with local lawyers.

HONOR has established a standards team, joined multiple standardization organizations, and actively participated in the research and compilation of privacy security standards. Put forward constructive opinions based on our technical management practices and for the protection of users' rights; discuss with industry partners how to jointly promote standardization. By the end of 2023, HONOR had led or participated in the research and development of more than 60 standards related to data security and privacy protection.

8.2 Consumer Communication

HONOR communicates with consumers via a variety of channels to enhance their awareness of privacy protection, communicate HONOR's privacy protection features, and protect users' rights.

HONOR provides an official website for privacy protection (https://www.honor.com/global/privacy/) to facilitate consumers to understand HONOR's privacy protection concept, policies, and features.



The HONOR Club provides a "Security and Privacy Protection" section (https://club.honor.com/cn/forum-4530-1.html) where privacy security knowledge is published on a regular basis and consumers can have a better way to learn and exchange privacy security skills and opinions. They can also post questions about privacy protection features or submit improvement suggestions. The HONOR Club will have designated personnel answer those questions.

HONOR also has a web page titled HONOR Privacy Issues on the official website (https://www.honor.com/global/privacy/feedback/), where consumers can submit personal data subject requests to exercise their right of access, correction, deletion, and portability. HONOR has designated a dedicated person to handle users' requests as personal data subjects. After receiving users' requests, HONOR will handle them in a timely manner in accordance with the requirements of relevant laws and regulations.

8.3 Privacy Security Certification

In order to provide users with trusted products and continuously improve our capabilities and transparency of privacy security, HONOR has passed a series of authoritative privacy security certifications including ISO/IEC 27701, ISO/IEC 27001, ePrivacyseal, PCI DSS, TEE, FIDO, UPDSS, and the Dual List.

Figure 8-1: Privacy Information Management-ISO/IEC 27701 Certificate Awarding Ceremony

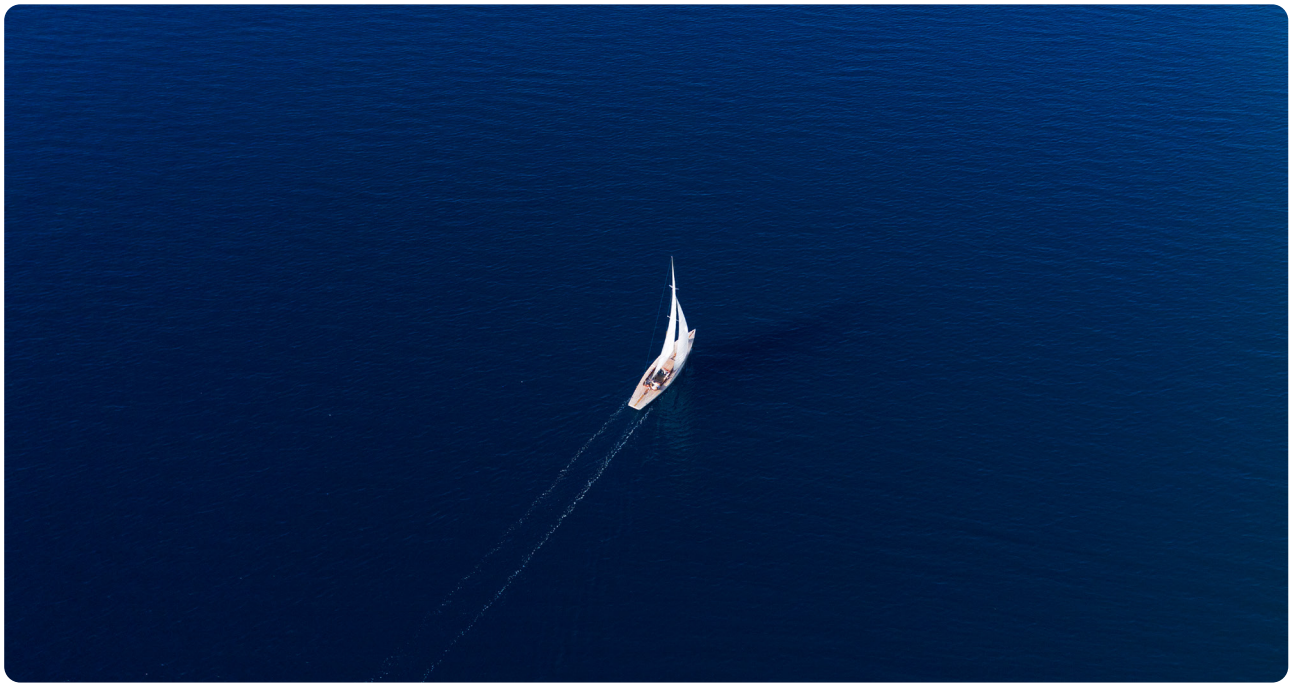
8.4 Cooperation with Industry Associations

HONOR attaches great importance to working with privacy protection associations and has joined the International Association of Privacy Professionals (IAPP) as a Platinum member. Now, HONOR has nearly 100 corporate members of IAPP in the company.

Conclusions

At present, HONOR has established a comprehensive privacy protection system. The concept “Your privacy, our priority” is deeply rooted among employees. The privacy protection organization is operating smoothly. Privacy requirements are effectively executed in business flows. HONOR also provides users with comprehensive privacy protection experience through innovative privacy protection technologies, allowing users to feel HONOR's respect and care for their privacy and rights.

In the future, HONOR will work with all partners along the industrial chain to build a healthy ecosystem of privacy security by relying on an open and transparent mindset, innovation-driven technologies, user-trusted products, intelligent protection features, and a win-win ecosystem.



Trademark Statement

Disclaimer

The information in this brochure does not constitute any offer or promise, and HONOR will not be liable for any decisions you make based on this brochure. The contents of this brochure are subject to revision without notice over the course of HONOR's development.