Honor Privacy Protection White Paper

Document Version: V1.0

Published: August, 2021

HONOR

Contents

1 Preface

Honor Device Co., Ltd. (hereinafter referred to as "we") is a leading international provider of smart devices. We are committed to providing innovative, high-end, free, and trustworthy products, our user-centric DNA is embodied by the longstanding heritage of innovation, quality, and service. We understood that winning the market meant building a brand that users can trust. For us, trustworthiness not only comes from the quality and safety of our products, but also from the special attention we give to the protection of user privacy.

Privacy is a fundamental right of our users, and we've made privacy protection a prerequisite for all the products and services we provide. From initial design to final delivery, we put privacy considerations into every step and give users autonomous control over their personal information. In addition, to fulfill our commitment, we have built a comprehensive privacy and security system that encompasses our management systems, organizational structure, process integration, and cultural development.

2 Privacy protection responsibility system

We understand the importance of user privacy and strictly comply with applicable privacy and personal data laws and regulations in all countries in which we operate. To effectively manage our efforts, we have established a comprehensive management system to develop and implement our privacy strategies and frameworks.

In addition to putting in place a tiered privacy management system, we’ve also established the Global Cyber Security and Privacy Protection Committee (GSPC). As the highest management body, the GSPC is responsible for approving and implementing our overall cybersecurity and privacy protection strategies. We've appointed a Global Cyber Security and Privacy Officer (GSPO) responsible for developing and enforcing end-to-end privacy policies. We have established the Privacy Protection Joint Conference (PPJC) to conduct professional assessments on all privacy-related matters. Privacy engineers were also appointed in all departments to ensure that privacy requirements and design capabilities are actuated.

Key organizations/roles and their responsibilities in the privacy management system.

Organization / Role	Responsibilities
Cyber Security and Privacy Protection Committee (GSPC)	Approve corporate cybersecurity and privacy protection strategies and provide resources to ensure their implementation.
Cyber Security and Privacy	Develop and enforce end-to-end privacy policies, set out departmental responsibilities, drive and audit implementation.

Officer (GSPO)	
Privacy Protection Joint Conference (PPJC)	Develop corporate privacy policies, standards, specifications, baselines, and white papers. Formulate business plan, review emergency handling processes, and carry out pre-launch major risk evaluations.
Privacy Protection Engineer	End-to-end privacy compliance management, requirement implementation and compliance, Data subject request handling, partner privacy compliance supervision, capability building, and staff awareness enhancement.

3 Privacy protection framework and data processing principles

3.1 Building a systematic privacy protection management system

We have developed a global privacy management system based on the Generally Accepted Principles and Practices (GAPP) and the General Data Protection Regulation (GDPR, the most stringent privacy protection law in the world). In addition, we have formed a comprehensive, ISO/IEC 27701 certified (by the British Standards Institution, BSI) global privacy management system. While adapting to the GAPP, we've included the seven aspects of the data lifecycle (notification to data subjects, choice and consent, collection, use, retention and disposal, disclosure to third parties, cross-border transfer of data, and data subject requests) and the four governance modules (management, security, quality, and implementation and monitoring) into consideration.

We've tailored our practices to comply with the laws and regulations of each country and conducted in-depth studies on external requirements to form privacy compliance baselines and integrated them into various areas to achieve strict privacy compliance worldwide.

3.2 Complying with the data processing principles set out in the GDPR

- **Lawfulness, fairness, and transparency:** Personal data should be processed in a manner that is lawful, legitimate, and transparent to the data subject.
- **Purpose limitation:** Personal data should be collected based on a specific, explicit, and legitimate purpose and should not be further processed in a manner inconsistent with that purpose.
- **Data minimisation:** Personal data collection should follow the principles of relevancy, appropriateness, and necessity. Anonymization or pseudonymization should be practiced wherever possible to minimize related risk to the data subject.
- **Accuracy:** Personal data should be accurate and updated timely when necessary. Reasonable measures should be taken to ensure that inaccurate personal data is deleted or corrected in a timely manner.
- **Storage limitation:** Data should be kept only for as long as necessary to achieve the purpose.
- **Integrity and Confidentiality:** Take appropriate technical or organizational measures (after taking available technical capabilities, implementation costs, and

the severity of privacy risks into account) to ensure that personal data is adequately protected from accidental or unlawful destruction, loss, alteration, unauthorized access, and disclosure.

- **Accountability:** The data controller is responsible for and able to demonstrate compliance with the above principles to the public.

4 Privacy Protection Best Practices

We've concluded the following best practices from years of compliance management experience:

4.1 Integrating privacy requirements into our processes

We reference each country's laws, regulations, and cases when forming compliance baselines and integrate these requirements into our daily operations. Doing so ensures that user privacy is considered in all aspects of R&D, supply chain, marketing, sales, service, and procurement. These requirements are also incorporated into our business processes to ensures effective implementation through continuous optimization and improvement.

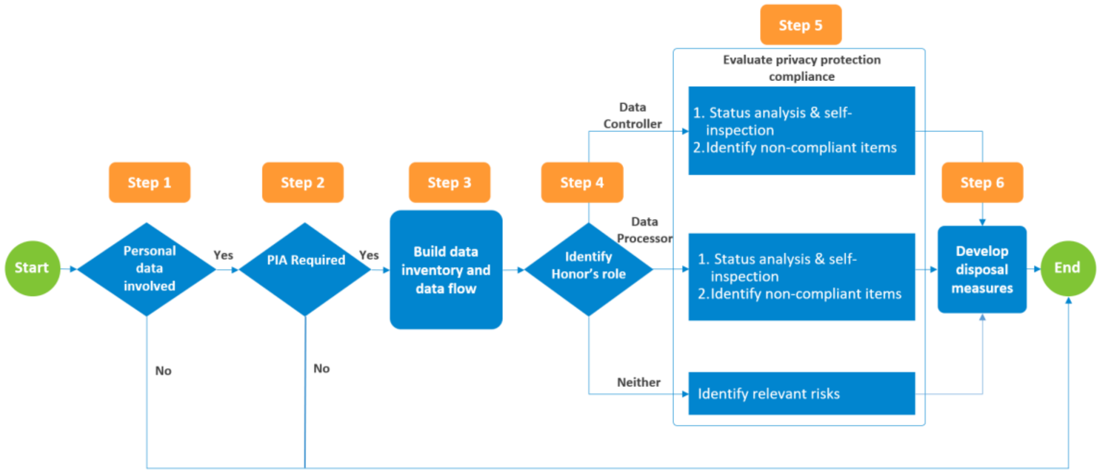
4.1.1 Data Inventory (DI) output requirements

We use data Inventory (DI) as the basis for identifying privacy risks. Our departments and subsidiaries are individually responsible for the identification of their data inventories. This encompasses the entire life cycle of the personal data involved (or likely to be involved) in various scenarios, including their flows and mandatory information. By referencing the legal requirements of each region/country and industry best practices, we have summarized and created the DI standard template.

4.1.2 Conducting Data Protection Impact Assessments (PIA/DPIA)

To help us systematically analyze, identify, and minimize data protection risks in our projects, we have developed the PIA (Privacy Impact Assessment) and DPIA (Data Protection Impact Assessment) methodologies.

- **PIA:** People in charge of business processes must identify personal data processing scenarios, implement PIA requirements, and perform privacy protection evaluations (including but not limited to developing specifications, systems and proposing detailed implementation requirements). the PIA process is required for products involving personal data processing, and assessment reports from standard PIA templates must be created.


Step 5
Evaluate privacy protection compliance
Data Controller
1. Status analysis & self-inspection
2.Identify non-compliant items
Step 1
Step 2
Step 3
Step 4
Step 6
Start
Personal data involved
Yes
PIA Required
Yes
Build data inventory and data flow
Identify Honor's role
Data Processor
1. Status analysis & self-inspection
2.Identify non-compliant items
Develop disposal measures
End
No
No
Neither
Identify relevant risks

- **DPIA:** DPIA is required for high-risk business scenarios meeting two or more of the following criteria. The assessment criteria for DPIA are more stringent while the involved business unit is responsible for its implementation.

a) Assessments and measurements (e.g., profiling and predicting)

b) Automated decisions that would have legal or similarly significant outcomes

c) Systematic monitoring

d) Highly sensitive personal data (e.g., special personal data types defined in Article 9 of the GDPR)

e) Large-scale data processing

f) Comprehensive matching of data sets

g) Data subjects belonging to vulnerable groups

h) Data uses that are innovative or involve new technologies

i) Scenarios in which the data subjects are not allowed to exercise their data subject rights, use a service, or execute a contract

Note: To assess privacy risks as comprehensively as possible, we have referred to a number of industry standards, frameworks, and best practices in developing our PIA and DPIA methodologies. These include but not limited to: the Privacy Impact Assessment Framework (EU), the DPIA Guide (EU Article 29 Working Party), the PIA Manual 1/2/3 (CNIL, France), Conducting Privacy Impact Assessment Code of Practice (ICO, UK), Directive on Privacy Impact Assessment (Canada), Guide to Privacy Impact Assessment (OAIC, Australia), and the DoD PIA Guide (US).

4.2 Privacy requirements integrated into product design

4.2.1 The five principles of privacy protection

The Privacy by Design (PbD) principle proposed in the GDPR is a recognized industry standard that clearly states that data controllers should consider security issues in the design and operation of products and protect users' personal information throughout the products' lifecycle. Drawing on industry best practices and our business situation, we have developed and implemented the following five privacy protection principles regarding the design and operation of our products.

- **Data minimization:** Minimal personal data collection and only when necessary. Data is kept only for as long as necessary to achieve the intended purpose.
- **Transparency and controllability:** Provide clear and unambiguous notices when collecting personal information to ensure that users know how it is being used and have the right to opt-out at any time.
- **On-device data processing:** Process and analyze data on-device whenever possible.
- **User Identity anonymization:** Use privacy-enhancing technologies to protect user identity and prevent tracking.
- **Security:** Use data protection technologies that are secure and reliable to safeguard user information.

4.2.2 Application of the five principles

We've put in place five safeguards for scenarios involving sensitive user data (such as camera, location, microphone, photo, and clipboard access) to prevent the occurrence of data misuse, disclosure, tracking, snooping, and user harassment. With comprehensive privacy protection, users will also be able to grant permissions before, be notified of risks during, and access exception records after using services.

For example, we’ve provided the following features in some products to enhance user privacy:

- Minimal permission recommendations: Provide scenario-based recommendations on granting the least number of permissions that match app functions.
- Repair mode: Users sending their devices in for repairs can enable repair mode so that their photos, videos, text messages, messenger apps, contacts, audio recordings, payment apps, and mobile banking data remain hidden from the technicians handling their devices.
- Permission notification reduction: No more permission request notifications will be shown when a permission request is denied twice in a row to avoid disturbing the user.
- Position fuzzification: Enable Fuzzy location in apps that don't need high location accuracy to avoid tracking.
- Projection privacy protection: When projecting your phone screen to other devices, the login screens of apps will not be shown on the projected device by default. Also, WeChat messages, SMS, and other information will not be shown when projecting to HONOR Vision TVs.

By further upholding the five privacy principles, we will continue to perfect the five safeguards and bring a full range of privacy protection services to our users.

5 Building a compliance culture surrounding privacy

We have established a privacy learning zone and developed a series of training courses to raise employee awareness and integrate privacy concepts into our organizational culture. In addition, we provide tailored privacy awareness promotion and empowerment for different crowds. Records are also kept to ensure that things can be verified and traced.

- For new employees, training on the basics of privacy protection is required before starting work.

- Personnel in privacy management positions must complete a series of compliance courses before starting work and be licensed after passing an examination.
- All employees must pass an annual privacy awareness test.
- Keep enhancing the capabilities and skills of privacy workers and require them to obtain external professional certifications such as CIPT/CIPM/CIPP.

6 Conclusion

Apart from maintaining compliance with the applicable local privacy/personal data protection laws and regulations, we will also strengthen our capabilities and system-building efforts while being open and transparent to regulatory bodies and our customers. Furthermore, with innovative technologies and comprehensive privacy protection, we will distinguish ourselves as a brand that users can trust.

If you would like more information about our privacy practices, please email us at privacy@hihonor.com