荣耀隐私保护白皮书

文档版本：V1.0

发布日期：2021 年 8 月

HONOR

目录

1 前言

荣耀终端有限公司（以下简称为 “我们”）是全球领先的智能终端提供商。我们致力于为用户提供“创新，高级，自由，可信赖”的产品，坚持以用户为中心，把创新、品质和服务融入到公司的基因当中，用创新和技术赢得市场，构筑用户可信赖的品牌。对用户而言，可信赖不仅仅是产品质量和安全，更是对用户隐私的保护。

隐私是用户的基本权利，保护用户的隐私是我们提供产品和服务最基本的前提条件。从最初的产品设计到最终的服务提供，每一环节我们都会考虑如何更好地保护用户的隐私，如何让用户对个人数据拥有自主控制。为了践行对用户的承诺，我们从管理体系、组织架构、流程融入、文化建设等方面构筑全方位的隐私安全保障体系。

2 隐私保护责任体系

我们深知保护用户隐私的重要性，在所有运营的国家都严格遵从适用的隐私保护和个人数据保护法律法规。为了有效管理隐私保护工作，我们成立了完善的隐私保护管理组织，负责制定公司的隐私保护策略、框架以及落地执行等工作。

我们建立了分层分级的隐私管理组织架构，成立了全球网络安全与隐私保护委员会（Global cyber Security and Privacy protection Committee，简称 GSPC），作为最高网络安全和隐私保护管理机构，负责决策和批准公司总体网络安全和隐私保护战略并确保其有效执行；我们任命了全球网络安全与隐私保护官（Global cyber Security and Privacy officer，简称 GSPO），负责端到端隐私保护政策的制定及推行与落地；我们成立了隐私保护联席会议（Privacy Protection Joint Conference，

简称 PPJC），对所有涉及隐私的业务进行专业评估；针对每个部门任命了隐私工程师，保障隐私保护的要求和设计能力落地到所有部门。

隐私保护管理组织中的重要组织/角色及具体职责：

组织/角色	职责
网络安全与隐私保护委员会(GSPC)	负责决策和批准公司网络安全与隐私保护战略，并提供必要的资源以保证战略得到执行。
网络安全与隐私保护官(GSPO)	负责端到端隐私保护政策的制定及推行与落地。明确相关部门的网络安全与隐私保护职责及角色，推动相关部门把网络安全与隐私保护的要求落实，稽核并推动改进。
隐私保护联席会议(PPJC)	负责制定公司隐私保护的隐私政策、标准、规范、基线和隐私白皮书，制定隐私保护 BP，隐私安全应急事件处理过程审视，业务上线重大隐私安全风险审视。
隐私保护工程师	负责对本业务领域的隐私合规端到端管理。负责隐私保护要求的落地、业务运营的隐私合规、处理数据主体请求、监督合作伙伴的隐私合规管理、负责本业务隐私能力构建、提升全员隐私意识和能力。

3 隐私保护框架及数据处理原则

3.1 构建系统的隐私保护管理体系

我们基于最佳的隐私保护方法（Generally Accepted Principles and Practices，简称 GAPP）和全球最严格的隐私保护法律法规（General Data Protection Regulation，简称 GDPR），融入了业界隐私管理的优秀实践，形成了自身完备的全球隐私保护管理体系，并已经通过了英国标准协会（ British Standards Institution，简称 BSI）的 ISO/IEC 27701 认证。我们结合业务特点对 GAPP 进行了适配，具体包含了业务运作中数据

生命周期的七个环节（通知数据主体、选择和同意、收集、使用、留存和处置、向第三方披露、数据跨境转移、数据主体请求），以及治理层面的四个模块（管理、安全、质量、实施与监控）。

同时我们适配各国法律法规，将外部要求经过深度解读形成我们自己的隐私合规基线，并融入到各个领域，做到全球范围内严格的隐私合规。

3.2 遵循 GDPR 规定的数据处理原则

- **合法、正当、透明**：个人数据应当以合法、正当、对数据主体透明的方式被处理。
- **目的限制**：个人数据应当基于具体、明确、合法的目的收集，不应以与此目的不相符的方式作进一步处理。
- **数据最小化**：个人数据应与数据处理目的相关，且是适当、必要的。尽可能对个人数据进行匿名或假名化，降低对数据主体的风险。
- **准确性**：个人数据应当是准确的，并在必要的情况下及时更新。根据数据处理的目的，采取合理的措施确保及时删除或修正不准确的个人数据。
- **存储期限最小化**：存储个人数据不超过实现数据处理目的所必要的期限。
- **完整性与保密性**：根据现有技术能力、实施成本、隐私风险程度和概率采取适度的技术或组织措施确保个人数据的适度安全，包括防止个人数据被意外或非法毁损、丢失、篡改、未授权访问和披露。
- **可归责**：数据控制者须负责且能够对外展示遵从上述原则。

4 隐私保护优秀实践

在我们多年的隐私合规管理实践过程中，通过不断的摸索，总结出如下优秀实践：

4.1 隐私要求融入流程

我们以各国家的法律法规、执法案例作为主要输入，形成隐私保护合规基线，并将基线的要求融入到日常业务活动中，让研发、供应链、市场与销售、服务和采购等所有环节都考虑到用户隐私，并将隐私保护要求嵌入到各个业务流程中，通过不断的优化和改进确保其有效实施。例如：

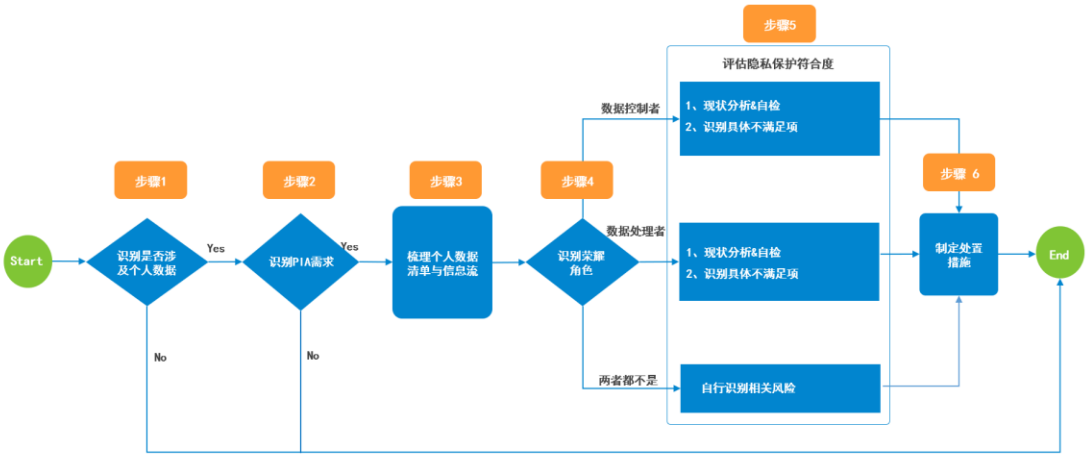
4.1.1 数据清单(DI)输出要求

数据清单（Data Inventory，简称 DI）是识别隐私风险的基础。机关各领域及子公司各业务部门是数据清单识别的责任人，负责识别业务场景中所涉及或可能涉及的个人数据及其整个生命周期的数据流向和必须信息。我们参考了各地区/国家法律要求、业界最佳实践，总结输出了 DI 标准模板。

4.1.2 开展隐私影响评估要求（PIA/DPIA）

为了帮助我们能够系统地分析、识别和最小化项目的数据保护风险的过程，我们制定了 PIA（Privacy Impact Assessment ，简称 PIA）和 DPIA(Data Protection Impact Assessment，简称 DPIA)方法论。

- **PIA:** 各业务流程责任人需识别个人数据处理场景，将 PIA 要求融入流程或对流程进行隐私保护打点（包括但不限于制定规范、制度，提出明确的动作执行要求）。涉及个人数据处理的产品都需要开展 PIA 活动并按标准的 PIA 模板输出评估报告。



- **DPIA:** 在业务场景满足下列标准中的两条或以上时，即属于高风险场景，应当执行 DPIA。DPIA 采用更加严格的评估标准，业务部门是执行 DPIA 的责任人。

a) 评估和度量（例如画像和预测）

b) 会产生法律或类似重大结果的自动决策

c) 系统性监控

d) 高度敏感个人数据（例如 GDPR 第 9 条中所定义的特殊类型个人数据）

e) 大规模数据处理

f) 数据集的综合匹配

g) 数据主体属于弱势群体

h) 创新使用或使用新技术

i) 该场景不允许数据主体实施数据主体权利、使用某种服务或执行某个合同

说明：为了尽可能全面的评估隐私风险，我们在制定 PIA 和 DPIA 方法论时参考了大量业界标准、框架和最佳实践，包括但不限于：EU PIAF（Privacy Impact Assessment Framework）、欧盟 29 条工作组发布的 DPIA Guide、法国 CNIL 发布的 PIA Manual 1/2/3、英国 ICO 发布的 Conducting Privacy Impact Assessment Code of Practice、加拿大发布的 Directive on Privacy Impact Assessment、澳大利亚 OAIC 发布的

Guide to Undertaking Privacy Impact Assessment、美国发布的 DoD PIA Guide。

4.2 隐私要求融入产品设计

4.2.1 隐私保护 5 大原则

GDPR 条款中提出的隐私保护设计（Privacy by Design，简称 PbD）原则是业界公认的标准，其明确指出：数据控制者在产品的设计和运行过程中应考虑安全保障问题，并在产品的整个生命周期里保护用户个人信息。我们在参考业界优秀实践的基础上结合自身的业务情况，制定了产品设计的隐私保护 5 大原则，并在产品设计及运行过程中贯彻如下原则用以确保在产品设计之初就将用户隐私安全作为重要的考虑因素纳入产品设计：

- **最小化：**只收集最少且必要的个人数据；仅在达成目的所需的期限内保存你的数据
- **透明可控：**采集个人数据时，我们会提供清晰、明确的通知，确保你知道数据被如何使用；同时你有权随时退出
- **端侧处理：**尽可能地在你的设备上处理和分析你的数据
- **身份匿名：**采用隐私增强技术保护用户身份，防止你的身份被定位、追踪
- **安全保护：**采用安全可靠的数据保护技术，用心守护你的数据安全

4.2.2 基于 5 大原则的应用

基于隐私保护 5 大原则，我们围绕着用户敏感个人数据使用场景（如：摄像头、位置、麦克风、照片、通讯录、剪切板等）构建 5 道隐私保护防线，帮助用户解决隐私痛点问题，实现保护用户的信息不被滥用、保护用户的数据不被泄露、保护用户的行为不被追踪、保护用户的隐私不被窥视、保护用户的使用不被打扰；同时在产品使用过程中，为用户提供事前

的授权选择、事中的风险提示、事后的异常统计披露，全方位的隐私保护服务。

例如，我们在部分产品中提供了如下功能帮助用户保护隐私（部分举例）：

- “APP 权限最小化推荐”功能：通过 APP 提供的基本功能和使用场景，为用户提供匹配 APP 功能的最小化权限授予建议，用以保护用户的信息不被滥用；
- “维修模式”功能：当用户手机出现故障送修时，只需要在手机上开启维修模式，维修人员将无法看到手机中的照片、视频、短信、即时聊天工具、通讯录、录音，支付应用和手机银行等数据，用以保护用户的数据不被泄露；
- “防弹窗频繁打扰” 功能：APP 申请权限时，当用户连续两次拒绝授权后，APP 后续就不会再通过弹窗消息进行询问，用以保护用户使用设备时不被骚扰；
- “模糊位置”功能：用户可以开启模糊位置功能给不需要精确位置的 APP，用以保护用户的使用行为不被追踪；
- “设备投屏隐私保护”功能：当用户使用手机跨设备投屏时，默认不在投射屏幕上显示 APP 的登录操作界面；投屏到智慧屏设备时，不会在投屏上显示你的微信、短信等相关信息，用以保护用户的隐私不被窥视。

我们将围绕隐私保护 5 大原则和以用户为中心构筑的 5 道保护防线，持续为用户带来全方位的隐私保护体验和服务。

5 隐私合规文化建设

我们建立了隐私保护学习专区，开发了一系列的隐私保护培训课程，提升全员的隐私保护意识，并将隐私保护的理念融入整个组织文化之中。针对不同人群，我们提供定制化的隐私保护意识宣传及赋能，并做好相关记录，保证可检查、可回溯。

- 针对新员工，入职上岗前需要接受隐私保护基础知识培训；

- 针对隐私管理岗位人员，上岗前要通过专业的隐私合规系列课程培训，通过考试后持证上岗；
- 针对全员，每年开展一次覆盖全员的隐私保护意识考试。

同时，我们会持续提升隐私保护从业人员能力和技能，要求隐私保护从业人员通过CIPT/CIPM/CIPP等外部专业认证。

6 结束语

我们始终遵守业务所在地适用的隐私保护/个人数据保护法律法规，并将在现有的隐私保护管理的基础上，持续加强隐私保护体系建设和能力建设，以开放的态度向相关的监管机构、客户和消费者保持透明。科技有道，隐私至上，我们将持续通过创新的隐私保护技术，给用户带来更好的产品和体验的同时，也给用户带来全方位的隐私保护，打造用户可信赖的科技品牌。

若您希望了解更多关于我们隐私保护的信息，请联系privacy@hihonor.com。