OPPO 移动终端

隐私保护白皮书

文档版本 V1.0

发布日期 2023-02-16

目录

1 前言

截至 2022 年，OPPO ColorOS 全球月活跃用户数已超过 5 亿。目前 ColorOS 已应用于 OPPO 生态内包括手机、手表、平板等移动终端设备中。根据相关统计，全球用户人均拥有 3 至 4 台智能设备，预计至 2032 年，人均将拥有 12 台智能设备。随着设备规模和服务规模的快速增长，移动终端设备作为用户数据交互的其中一个重要端口，其隐私保护相关问题已受到了社会的广泛关注。

2018 年，欧盟《通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）率先发布，引领全球个人信息保护监管趋势。2021 年，中国相继颁布并实施了《数据安全法》与《个人信息保护法》，结合已施行的《网络安全法》，我国已逐步建立起数据安全和个人信息保护的顶层监管框架。在此框架内，中国于 2022 年颁布并实施了《数据出境安全评估办法》、《移动互联网应用程序信息服务管理规定》等要求，进一步对数据安全和个人信息保护作出了细致要求。同时，网信办和工信部针对违反上述法律法规的行为开展专项整治行动并予以处罚，进一步表明了国家对数据安全、个人信息保护工作的重视。日趋严格的隐私保护监管要求，一方面反映了消费者与社会各界的关注，另一方面也激发了移动终端行业保护个人信息的自觉意识，进而促进了移动终端个人信息保护技术的发展。

用户在享受更加便利、智慧服务的同时，也期望个人的信息能得到保护。为达到用户期望，在最新发布的智慧跨端系统——潘塔纳尔中，OPPO 将隐私保护作为系统核心能力进行打造，依托 OPPO 的安全研发体系和创新机制，持续为用户提供安全可信赖的感知。潘塔纳尔在隐私保护方面，以精准共享、动态授权、全域安全、透明合规为原则，为用户提供贯穿数据、服务全链路的安全防护。

目前，OPPO 在隐私保护方面已取得阶段性成效，获得了全球首家 CC MDFPP(v3.2)安全认证和国内首家 2407-2021 版移动智能终端安全技术五级能力认证，以及 ePrivacy、TrustArc、ISO 等多项第三方机构认证，并积极参与建设行业标准体系，为用户提供安全可信赖的产品和服务。

2 隐私保护体系

2.1 隐私保护原则

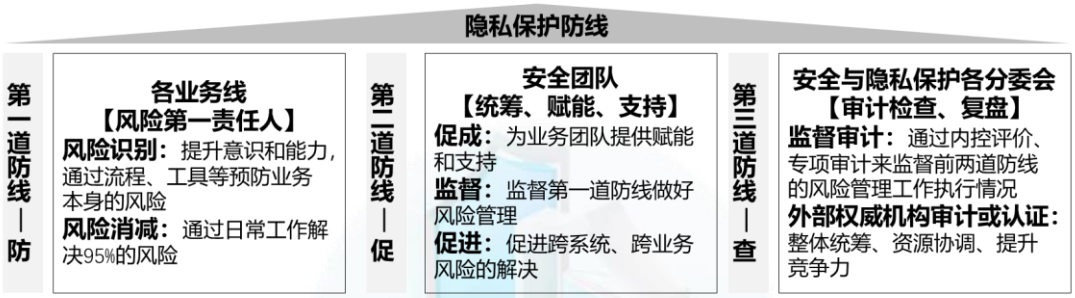
OPPO 参考欧盟隐私保护法规 GDPR 所提出的七项隐私保护原则（合法性、公平性和透明性；目的限制；数据最小化；准确性；存储期限限制；完整性和保密性；可归责），融入移动终端行业在隐私保护的优秀实践，形成了 OPPO 的隐私保护管理体系，并已经通过 ISO/IEC 27701 认证。同时，我们深度解析重点国家隐私保护的相关法律法规，定制适配重点国家的隐私合规基线，并融入产品、业务，实现全球范围的隐私保护合规。

2.2 隐私保护组织

为促进公司产品与服务的安全合规管理，有效识别和主动管理、防范、处置安全合规风险，提高全体员工安全合规意识，公司成立安全合规委员会，作为公司安全合规管理领域最

高级别的领导决策机构。安全合规委员会主任由公司 COO 担任，委员及分委会主任由各业务系统高管及公司首席合规官担任。

安全合规委员会下设 9 大分委会，覆盖欧加所有公司产品与服务的安全合规管理。各分委会负责各领域的业务合规落地，搭建隐私合规管理体系，明确合规路线规划，制定和解读合规标准，并对标准落地进行监督和审计。安全与合规委员会通过安全与隐私管理的三道防线，协同推进安全隐私工作的落地。



2.3 隐私保护流程

通过深度解读重点国家的法律法规和执法案例，OPPO 将安全与隐私保护的要求和活动融入项目集成产品开发（Integrated Product Development，IPD）流程的各个环节，包括需求、设计、研发、测试、发布和运营，并通过不断的优化和改进确保其有效实施，保障最终交付产品和服务的质量。

2.4 隐私保护制度与技术

2.4.1 隐私保护制度

OPPO 积极响应各个国家/地区的法律法规要求，包括欧盟 GDPR，美国《加利福尼亚州消费者隐私法》(CCPA)和《加州隐私权法》(CPRA)，中国《个人信息保护法》、《数据安全法》和

《网络安全法》等，并针对中国《信息安全技术 个人信息安全规范》、《移动智能终端安全能力技术要求》等重点标准做了细化解读，导入产品研发合规库实现“外规内化”，制定了包括《OPPO 数据保护制度》、《OPPO 数据隐私合规原则通用评估标准指引》、《终端业务隐私合规技术要求及评审规则》、《个人信息与敏感个人信息分类关键指引》、《移动终端安全事件应急响应流程》等内部制度规范。

2.4.2 隐私保护技术

OPPO 从数据生命周期角度出发，并根据个人身份可识别程度和影响程度将移动终端数据分为 4 个级别，分级越高数据对应的敏感程度越高，实施的保护措施也更为严格。对于 1 级数据，沿用系统原生安全机制（基于文件的加密），不施加额外保护措施（BP）。对于 2 级数据，在沿用系统原生安全机制的基础上，提供常规内容加密（CP）。对于 3 级数据，在 CP 基础上，额外增加与锁屏状态相关的只读保护（RP）。对于 4 级数据，在 RP 基础上，额外禁止锁屏状态下创建文件的操作（FP）。另外，针对需要用户即时验证身份才能访问的数据，提供了认证保护（AP）的可选能力。

OPPO 已在手机端侧系统和部分应用中使用本地化差分隐私技术，在数据中添加随机噪声，仅保留数据整体统计特征，确保用户数据不出终端设备即可实现相关功能，从而更好地保护用户隐私安全。同时，OPPO 也在推进联邦学习、安全多方计算、同态加密等前沿隐私保护技术的研究，为进一步增强隐私保护不断积累技术能力。

3 隐私保护实践

3.1 隐私保护影响评估

3.1.1 隐私影响评价（PIA）

为识别、减少需求分析和设计过程中终端系统和应用中相关业务方案的隐私合规风险，OPPO 建立了规范的业务方案隐私影响评估（Privacy Impact Assessment，以下简称“PIA”）流程，以确保在进入软件项目开发阶段前，业务方案的隐私合规性得到保证，最大限度地预防和减少隐私保护不合规行为发生的可能性。

PIA 流程将隐私保护关注点整合到系统和软件生命周期的研发实践中，基于隐私合规要求及评估准则进行隐私评审活动，旨在从设计阶段开始识别、削减隐私合规风险，以满足公司安全及隐私合规要求。

为实现 PIA 流程的有效执行，我们设立了单独的隐私合规评审岗位和专业人员，包括数据与隐私合规工作组和隐私合规专员，负责公司 PIA 流程的相关工作。数据与隐私合规工作组负责制定并维护 PIA 流程及实施方案，受理业务方隐私合规评审需求，输出评审意见及合规整改方案等工作。隐私合规专员对接本部门各业务的数据安全与隐私合规工作，并组织开展业务方案的隐私合规评审会议，对合规方案及遗留事项进行跟进并落地。

3.1.2 个人信息保护影响评估（DPIA）

个人信息保护影响评估（简称为“DPIA”）是实现隐私保护嵌入产品设计（Privacy by Design，Privacy by Default）的重要手段，目的是在 PIA 等常规流程之外，针对重大、新兴的技术开发、产品设计或运营活动策划初期引入个人信息处理风险评估流程，以衡量个人信

息处理的必要性和相称性，识别处理活动对自然人的权益和自由可能产生的风险，并采取相应风险管理措施。

中国《个人信息保护法》、欧盟 GDPR 等全球不同国家/地区数据保护法律对 DPIA 做出了相关规定。OPPO 实施 DPIA 不仅是为了遵从法律要求，也是发自内心地践行用户隐私保护的理念。

实施 DPIA 有助于有效管理隐私合规风险，根据中国《个人信息保护法》，有下列情形之一的，企业应当在事前进行 DPIA:

1)处理敏感个人信息；

2)利用个人信息进行自动化决策；

3)委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

4)向境外提供个人信息；

5)其他对个人权益有重大影响的个人信息处理活动。

根据 GDPR，当数据处理活动“可能对自然人的权益和自由造成高风险”时，实施 DPIA 是强制性要求。该要求与中国《个人信息保护法》中“对个人权益有重大影响”要求的情形类似。

在国内，当公司开展的任何个人信息处理活动，无论是针对内部人员、商业合作伙伴、用户及其他数据主体，只要满足中国《个人信息保护法》要求的启动标准时，就应当实施 DPIA。其中，针对构成重大影响的评估可进一步参考欧盟 GDPR 相关要求中所述的 9 个标准。需要注意的是，如果依照上述判断标准无法确定是否需要实施 DPIA，从充分满足合规要求的角度，仍应当实施 DPIA。

3.2 隐私检测能力

OPPO 采用人工检测和自动化工具检测结合的方式，将隐私检测内嵌到业务开发和测试流程中，对隐私合规要求进行覆盖。在数据全生命周期方面，检测覆盖了包括收集、存储、使用、加工、传输、提供、公开、删除阶段的合规要求。在检测对象方面，覆盖了 OPPO 自研应用（含引入的自研 SDK 和第三方 SDK）、终端预置的第三方应用（含引入的 SDK）、日志文件、二进制文件等。

OPPO 已研发结合静态检测和动态检测技术的自动化工具，开发人员可以在应用发布前，使用该工具识别 SDK 中存在的隐私合规风险。其中静态检测技术包括静态污点分析、二进制文件分析、源代码分析等，动态检测技术包括系统插桩、动态污点分析、UI 自动化测试框架等。

3.3 隐私保护表现

ColorOS 以用户数据安全和隐私保护为核心，建立了完善的控制体系和权限管理流程，提供用户数据存储加密、传输加密、应用行为记录、隐私替身等安全技术措施和功能，全方位保护用户的数据与隐私安全。ColorOS 在设计时即考虑构筑全面的终端安全架构，进行了大量安全和体验性的功能创新，为用户提供端到端的安全保护，旨在为用户提供最高的安全和透明体验。

ColorOS 系统提供如下功能践行用户隐私保护（部分举例）：

“应用行为记录”功能：ColorOS 允许用户对已安装的应用程序所申请的权限进行细粒度的控制，并可查看已安装的 App 最近 30 天权限使用的详细记录。

“敏感权限提醒”功能 ：当应用在调用摄像头、麦克风、定位信息等敏感权限时，状态栏右侧会立即出现对应权限的调用状态图标，对用户进行提示，增强用户感知并提醒用户对相关应用进行权限管理。

“应用锁”功能：为了防止用户将手机借出时，他人未经允许访问涉及隐私的应用，ColorOS 提供了“应用锁”机制。用户可以为应用软件设置访问密码、指纹、人脸验证保护，设置后用户必须通过验证才能访问被“应用锁”保护的应用，从而可以有效保护用户的隐私。

“私密保险箱”功能：ColorOS 私密保险箱提供基于用户密码加密的保护空间。用户可以将一些敏感或重要的个人文件（照片、音频、视频、文档等）添加到私密保险箱中进行加密保护，从而降低用户私密数据泄露的风险。

“系统分身”功能：为了满足用户隐私保护的高要求，ColorOS 提供工作生活双系统的系统分身功能，用户既可以提升工作效率，又能在工作结束后快速切换到生活状态。系统分身实际是独立于主系统空间的另一个私密空间，可直接克隆主系统应用，无需重复下载，可满足用户将工作、生活 、娱乐应用隔离使用，无痕隐藏私密数据，快速在双系统间切换的需求。

“隐私替身”功能：用户在使用不同应用时，会担忧自己的个人信息被超目的、超范围收集、使用，针对某些应用必须获取权限才可使用的情况（如读取通话记录、联系人、账号信息、日程信息等敏感权限），ColorOS 为用户应用提供隐私替身功能以保护用户的隐私信息。

“自动打码”功能：为用户提供自动打码聊天截屏中双方头像、昵称等隐私信息的功能，从而避免用户隐私信息泄露。该功能目前主要面向指定应用（如微信、QQ、钉钉等沟通软件）的聊天界面。

4 生态建设

4.1 对外合作

4.1.1 行业交流

OPPO 每年定期举办技术交流会或参与安全领域各类峰会及论坛，向外界开放共享最新研究成果及安全技术实践，持续推动行业安全、隐私保护的交流合作。

2022 年 8 月，OPPO 与 CCF 共同举办“泛在信赖、连接未来”的安全技术研讨会，围绕系统安全、应用安全、AI 安全等领域中的问题和最前沿的进展进行集中分析和研讨，共同探讨如何持续为用户提供安全可信赖的产品。

2022 年 11 月，OPPO 与 XDef 共同举办“XDef-OPPO”安全技术沙龙。沙龙集中研讨系统立体防御、数据存储中的 DOS 攻击、蓝牙协议中的内存漏洞挖掘、跨设备信息流构建和污点分析、Android 混合开发模式下攻防等问题和前沿进展，并邀请业内多位知名学者共同探讨面向未来终端安全环境，OPPO 的产品和服务应具备和储备哪些相关技术能力来应对技术挑战与机遇。

4.1.2 生态联盟

2020 年，为提升移动终端产业的竞争力，促进技术进步，推动新技术、新生态的快速发展，OPPO 作为创始成员单位，联合生态软硬件企业发起成立移动智能终端生态联盟。在金标联盟中，OPPO 作为应用安全组组长角色，牵头制定了《联盟应用安全测试技术要求》等联盟标准，携手推进联盟生态建设，旨在构建一个开放共享、安全合规的产业生态。

4.1.3 隐私保护标准制定

OPPO 深度参与国家、行业、团体标准的编制工作，牵头起草了《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第 3 部分：图片信息》等一系列保护用户隐私权益的标准，并参与 100 余项国家、行业、团体等标准的起草制定。针对《信息安全技术 移动互联网应用程序 APP 生命周期安全管理指南》、《信息安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南》、《信息安全技术 移动智能终端应用市场移动互联网应用程序（App）个人信息处理活动管理指南》等国家标准，OPPO 积极参与应用试点工作，为行业的标准化建设贡献力量。如下是 OPPO 近三年牵头、参加编制的国家、行业、团体标准的示例：

序号	标准号	标准名称
1	GB/T 41387-2022	《信息安全技术 智能家居通用安全规范》
2	GB/T 39720-2020	《信息安全技术 移动智能终端安全技术要求及测试评价方法》
3	YD/T 2407-2021	移动智能终端安全能力技术要求
4	YD/T 4177.3-2022	《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第 3 部分：图片信息》
5	T/TAF 077.1—2022	APP 收集使用个人信息最小必要评估规范 第 1 部分：总则
6	T/TAF 109-2022	移动应用分发平台系列规范：APP 开发者信用评价体系
7	T/TAF 081.3-2022	移动应用软件调用行为记录能力要求 第 3 部分：API 接口
8	T/TAF 081.2-2021	移动应用软件调用行为记录能力要求 第 2 部分：保存和展示

9	T/TAF 081.1-2021	《移动智能终端应用软件调用行为记录能力要求 总则》
10	T/TAF 051-2021	《移动智能终端及应用软件用户个人信息保护实施指南 第 5 分：终端权限管理》

4.2 权威认证

通过持续审视提升内部合规体系成熟度，OPPO 有布局、有节奏地取得了一系列国内外安全隐私认证。通过有公信力的认证检验，建立与政府相关监管部门、合作伙伴、消费者间的信任，夯实企业自证合规基础。

纵观行业内，考虑重点国家/区域、专业认证领域、认证机构背景等维度，OPPO 当前认证侧重点明显，覆盖度全面且重复度低，数量和专业性上整体处于行业领先地位。

2018年7月

- **TRUSTe**

TrustArc是美国隐私认证机构的领先者，是行业内具有公信力的认证机构。获得该机构的认证，意味着OPPO隐私管理体系、重点产品及服务的实践符合认证机构制定的关于个人信息使用的相关规范与要求，更好地保护你的隐私。

2018年8月

- **ePrivacyseal**

ePrivacy是一家欧洲权威隐私认证机构，为数据产品和厂商提供独立的认证、GDPR审计，隐私图章，并以极高的技术和法律专业水平著称。获得ePrivacy的认证，是OPPO数据隐私合规工作的重要里程碑。OPPO会持续丰富ePrivacy认证的产品体系，为你的隐私保驾护航。

2019年6月

- **ISO/IEC 27001**

ISO/IEC 27001是国际标准化组织发布的，在信息安全领域极其知名的标准。获得认证意味着OPPO互联网业务在产品的设计、研发、测试和运营各环节充分考虑安全风险，建立了科学有效的管理体系，能够全面、系统、持续提供互联网服务并保护你的信息安全。

- **ISO/IEC 27018**

ISO/IEC 27018是一个由国际标准化组织(ISO)于2014年颁布的国际标准，是专注于云中个人信息保护的国际行为准则。OPPO获得该认证，标志着OPPO云服务的安全能力足够满足国内外高标准的个人信息保护的行业和法律法规要求，能够为OPPO云服务用户的信息提供坚实的保障。

- **CSA STAR**

CSA STAR认证是云安全联盟对云服务安全性的独立评估，它以信息管理系统标准为基础，结合了CSA云控制矩阵16个控制域的要求，全面评估云服务安全性。获得认证，意味着OPPO云服务安全性符合国际高要求的云安全标准要求，能够为你提供持续、稳定和安全高效的云服务。

2019年9月

- **ISO/IEC 27701**

ISO/IEC 27701是国际标准化组织发布的全球权威隐私体系标准。获得认证意味着OPPO互联网业务在设计、开发、运营、下线等全产品生命周期中，构建了以用户隐私保护为核心的隐私信息管理体系，能够持续全面保护你的个人信息。

2020年4月

- **移动智能终端安全认证**

移动智能终端安全认证是由泰尔认证中心有限公司依据《YD/T 2407-2021 移动智能终端安全能力技术要求》的五级要求（该标准最高等级）进行测评，由电信终端产业协会（TAF）批准认证。获得本认证，意味着ColorOS 12.1版本可为你提供该标准最高等级的软件安全和隐私保障。

2021年10月

- **PCI DSS**

PCI-DSS认证是全球范围权威的金融数据安全认证之一，由VISA和Master Card联合多家机构成立的支付卡行业数据安全标准委员会制定和推行，以认证标准严格著称。OPPO在钱包、支付、信贷等业务通过了PCI-DSS认证。获此认证意味着OPPO以严格的要求保护持卡人数据，守护你的每一笔交易。

2021年10月

- **CC MDFPP**

CC(Common Criteria)认证基于信息技术安全评估通用标准对IT产品的安全功能和安全保障能力进行全方位评估，涉及产品设计开发、安全功能、交付管理等方面。MDFPP是基于CC标准为移动设备定义的全面安全评估框架，通过该认证意味着OPPO终端产品得到全方位评估和验证。

2022年4月

- **ioXt**

ioXt通过制定物联网安全的全球标准提高连接设备的安全性。该计划可衡量产品的"升级、安全补丁、漏洞管理、版本校验、安全算法、默认安全、认证安全和安全接口"的级别。 获得该标准高等级测评，意味着OPPO终端产品为你提供该标准高等级的安全和隐私保障。

4.3 文化建设

为了保证公司从管理层到普通员工有足够的隐私保护意识及能力，以践行 OPPO 对用户数据保护的承诺及具体要求，公司安全隐私专业团队定期面向全公司组织专业培训和意识宣导。

在关键合规岗位上，培养和组建了具有专业背景和资深从业经历的安全合规队伍，主 要负责产品安全隐私策略的具体落地和应用、自查自纠。连续多年在全公司范围内举办安全与隐私宣传活动，通过线上传播及线下活动，探讨年度数据保护热点话题，让员工在互动中增长安全与隐私合规知识、提高安全与隐私技能。常规安全隐私培训覆盖 95%以上主要业务人员，并将培训通过情况纳入考核指标。同时，OPPO 内部推出了针对安全合规专员的终端安全隐私能力认证，认证课程由移动终端安全与隐私保护各分委会制定，从意识及实践方面整体赋能。

5 展望

建立移动终端数据全生命周期的安全防护，构建可信赖的用户体验是 OPPO 一直以来坚持的信念。OPPO 将会继续深耕安全领域，坚持以用户安全和隐私保护为核心，为打造一个绿色生态、合作共赢、守护用户安全和隐私的立体防护体系而不断努力。OPPO 将持续强化在移动终端隐私保护方面的投入和能力构建，持续优化提升数字化可信工程建设，将安全、隐私、合规打造成 OPPO 的核心竞争力，并与行业共筑安全可信生态。