商米GDPR白皮书

上海商米科技集团股份有限公司

地址：上海市杨浦区淞沪路388号6层

网址：https://www.sunmi.com/zh-CN/

目 录

1. 概述

1.1. 适用范围

本文档信息适用于商米向位于欧洲经济区、英国或瑞士的用户或客户提供的产品或服务。

1.2. 发布目的

本文档旨在帮助商米客户或用户了解：

- GDPR 下数据合规的基本要求；
- 商米在不同业务模式下的数据处理角色与义务；
- 商米已针对 GDPR 采取了哪些合规措施。

1.3. 基本定义

- 个人数据是指与已识别或可识别的自然人（**“数据主体”**）相关的任何信息；可识别的自然人是指可以直接或间接识别的自然人，特别是通过参考诸如姓名、身份证号码、位置数据、在线标识符等标识符或与身体、生理、心理特定关联的一个或多个因素来识别的自然人。
- 处理是指对个人数据或个人数据集执行的任何操作或一组操作，无论是否通过自动方式，例如收集、记录、组织、结构化、存储、改编或更改、检索、咨询、使用、通过传输、传播或以其他方式提供的披露、排列或组合、限制、删除或销毁；
- 控制者是指单独或与他人共同确定个人数据处理的目的和方式的自然人或法人、公共当局、机构或其他团体；
- 处理者是指代表控制者处理个人数据的自然人或法人、公共机构、代理机构或其他机构。

2. GDPR 数据保护要求概述

2.1. GDPR 简介

《通用数据保护条例》(GENERAL DATA PROTECTION REGULATION (GDPR))是世界上最严格的隐私和数据保护法律之一，要求处理欧盟境内任何人的个人数

据的组织（无论其位于何处）均应遵循。2018 年 5 月 25 日正式实施的 GDPR 对全球范围内的数据保护造成了深远影响。

2.2. GDPR 基本原则&核心要求

(1) 基本保护原则

- 合法、公平和透明——应以合法、公平和透明的方式处理数据主体的数据；
- 目的限制——必须出于收集数据时向数据主体明确的合法目的来处理数据；
- 数据最小化——仅处理实现处理目的所必须的数据；
- 准确性—— 必须保持所处理的个人数据准确且及时更新；
- 存储限制——仅可在实现特定目的所需的时间内存储个人数据；
- 完整性和保密性——以适当安全的方式处理个人数据，包括使用技术或组织措施防止未经授权或非法处理以及数据的意外丢失、破坏或损坏；
- 应采取适当的措施保存合规记录，作为遵守数据处理义务的证明；

(2) 数据安全

通过实施“适当的技术和组织措施”来安全地处理数据，其中技术措施包括权限管理、数据加密等；组织措施包括：设置完善的组织架构、定期员工培训等。

(3) 遵循 Privacy by Design（PbD）的原则

PbD 旨在通过从产品、服务、业务实践和物理基础设施开发之初就纳入隐私设计来确保对个人隐私的保护。

(4) GDPR 对于同意做出了严格限定，例如

- 同意必须是“自由给出的、具体的、知情的和明确的”；
- 同意请求必须“与其他事项清楚地区分开来”，并以“清晰、简单的语言”提出；
- 数据主体可以随时撤回先前给予的同意，并且必须尊重他们的决定；
- 13 岁以下的儿童只有在获得父母许可的情况下才能表示同意；
- 需要保留同意的书面证据。

(5) 数据保护官（DPO）

并非每个数据控制者或处理者都需要任命数据保护官 (DPO)。在三种情况下，应任命 DPO：

- 公共机构；
- 核心活动要求大规模、系统地、定期地监控人员（例如 Google）；
- 核心活动是大规模处理 GDPR 第 9 条中列出的特殊类别数据或与第 10 条中提到的刑事定罪和犯罪相关的数据（例如医疗机构）；

即使没有达到上述条件，也可以选择指定 DPO。

(6) 保护数据主体权利

《通用数据保护条例》(GDPR) 的目标之一是赋予个人权力并让他们控制自己的个人数据。GDPR 下关于数据主体的权利，包括访问权、纠正权、删除权、限制处理权、数据可移植权、反对权和权利不受仅基于自动化处理的决定的影响。

3. 不同合作模式下，商米的数据处理角色

在商米与商米客户的不同合作模式下，商米的数据处理角色不同，所需履行的数据保护义务也有所差异，大致可分为以下三种模式[1]：

(1) 当商米仅为设备提供商，商米客户采用私有云部署方式，即数据均存储于商米客户的服务器中，商米不处理任何客户或相应的终端用户数据，也无需承担 GDPR 项下的数据合规义务；

(2) 当商米接受客户委托，为客户提供定制设备，并且受商米客户委托，协助其向终端用户提供相应的设备产品及服务，商米为数据处理者协助商米客户处理终端用户数据，商米需承担 GDPR 项下的数据处理者的义务；

(3) 当商米直接向商米终端用户提供产品或服务时，商米作为数据控制者处理终端用户的邮箱等信息，商米需承担 GDPR 项下的数据控制者的义务。

4. 基于 GDPR，商米采取了哪些合规措施

[1] 具体情形可能较为复杂多变，为便于理解，此处仅简化为三种情形。

目前商米采取了一系列措施与准备工作，以期满足 GDPR 的合规要求，具体体现在如下几个方面：

4.1. 坚持数据保护基本原则

商米始终坚持 GDPR 中数据保护的基本原则，例如：

- **坚持透明度原则：**商米坚持透明度原则，通过隐私政策告知用户在用户使用商米提供的相关产品或服务时，商米如何处理用户数据，相关内容详见商米《法律文件》页面；此外，如商米修改更新隐私政策，会通过弹窗提示用户阅读最新版本隐私政策。
- **目的限制原则：**商米致力于基于收集数据时所声明的目的，或在法律规定的情形下处理用户数据。
- **数据最小化原则：**商米尽最大努力在产品研发全流程中坚持数据最小化原则，例如：数据采集最小化：收集阶段评估具体字段收集必要性；数据存储时间最小化：仅在履行特定目的所需的最短时间内存储数据。

4.2. 技术及组织安全措施

商米已采取的采取了一系列技术及组织安全措施确保数据安全，具体包括：

(1) 技术措施

- 通过 ISO/IEC 27001 信息安全管理认证，并且采取了其中所涉的技术措施；
- 终端安全：商米对设备的安全管理扩展到了其整个生命周期，确保终端从生产组装（Manufacturing final assembly）、运输交付（Delivery）、维修（Repair）、退出使用（decommissioning）等各环节都得到安全控制并符合 PCI、银联、CC 等标准规范；
- 权限控制：在设备接入过程中，商米通过采取访问控制措施对接入设备进行身份验证，确保仅授权设备才能访问商米后台系统，从而防止了未经授权的访问风险；同时，商米在公司内部设置了权限管控制度与技术措施，以确保相关人员仅可访问其职责范围内所需访问的数据；
- 体系化的数据保护策略：具体措施包括根据业务和隐私保护的需求进行安全配置工作，例如操作系统配置、网络设置、安全防护、数据库加密

策略等，设置恰当的访问控制策略和密码策略。

(2) 组织措施

- **成立信息安全委员会：**商米成立了信息安全委员会，负责信息安全管理体系建设等一系列组织活动。
- **成立跨部门联动的数据合规小组：**商米法务部门、产品与研发中心、商务运营部门及数据合规顾问，共同成立了数据合规小组，以负责公司整体数据合规建设。
- **任命 DPO：**任命 DPO，以全盘了解企业的数据处理概况，并实施同步数据相关的新政策，跟进企业整体数据合规工作。
- **加强员工数据安全意识：**我们定期组织员工信息、数据安全相关的培训。此外，商米还进行应急演练，以增强全体员工在安全方面的应急处理能力。
- **建立适当的数据保护政策：**《个人信息安全管理制度》、《数据安全评估制度》、《数据安全管理规范》等内部管理制度。
- **建立数据安全应急响应制度：**制定《数据安全应急响应制度》以应对可能的数据泄露等安全事件。

4.3. 遵循 Privacy by Design（PbD）的原则

商米在产品研发和服务提供过程中，始终关注于在功能评审、服务器部署方案设计等环节，将可能的数据合规风险作为重要参考因素之一，最终综合形成设计方案。

4.4. 落实告知同意

商米尽力在各产品或服务中落实告知同意流程，例如：

- 用户在首次激活商米设备时，商米会向用户展示《商米设备隐私政策》并取得用户同意；
- 用户在注册商米帐户，商米会向用户展示《商米帐号隐私政策》并取得用户同意；
- 当用户在使用商米提供的具体服务时，商米还会根据该服务向用户展示相应

的隐私政策，并取得用户的同意。

4.5. 数据跨境流动

为减少数据跨境安全及合规风险，对于通过商米设备、商米网站等使用我们服务的用户，我们支持将用户的个人信息和数据留存于商米在当地部署或客户自行管理的服务器中。我们的本地化部署方案包括：对于位于欧洲经济区、英国或瑞士的用户，用户的个人信息将存储于欧盟范围内的服务器；对于私有化部署的客户，用户的个人信息将存储在客户指定的服务器之中。

4.6. 保护数据主体权利

商米致力于保障数据主体权利，例如：

(1) 在隐私政策中告知数据主体的享有哪些具体权利，可以何种方式行使自己的权利；

(2) 数据主体可直接通过商米提供的交互界面行使部分权利，例如访问与更改部分个人信息、注销账户等；

(3) 商米有专人维护与支持数据主体行权，并由数据合规小组会同相关业务部门提供法律及技术支持。

5. 结语

保护数据安全及用户隐私一直是商米产品设计的重中之重。商米会持续洞察法律更新情况，并不断优化内部数据合规流程、迭代产品设计，力图为用户提供更加安全合规的产品。

本白皮书仅供参考，不具备法律效力或构成法律建议。

6. 历史版本

日期	版本	版本描述
2024-02-01	1.0	