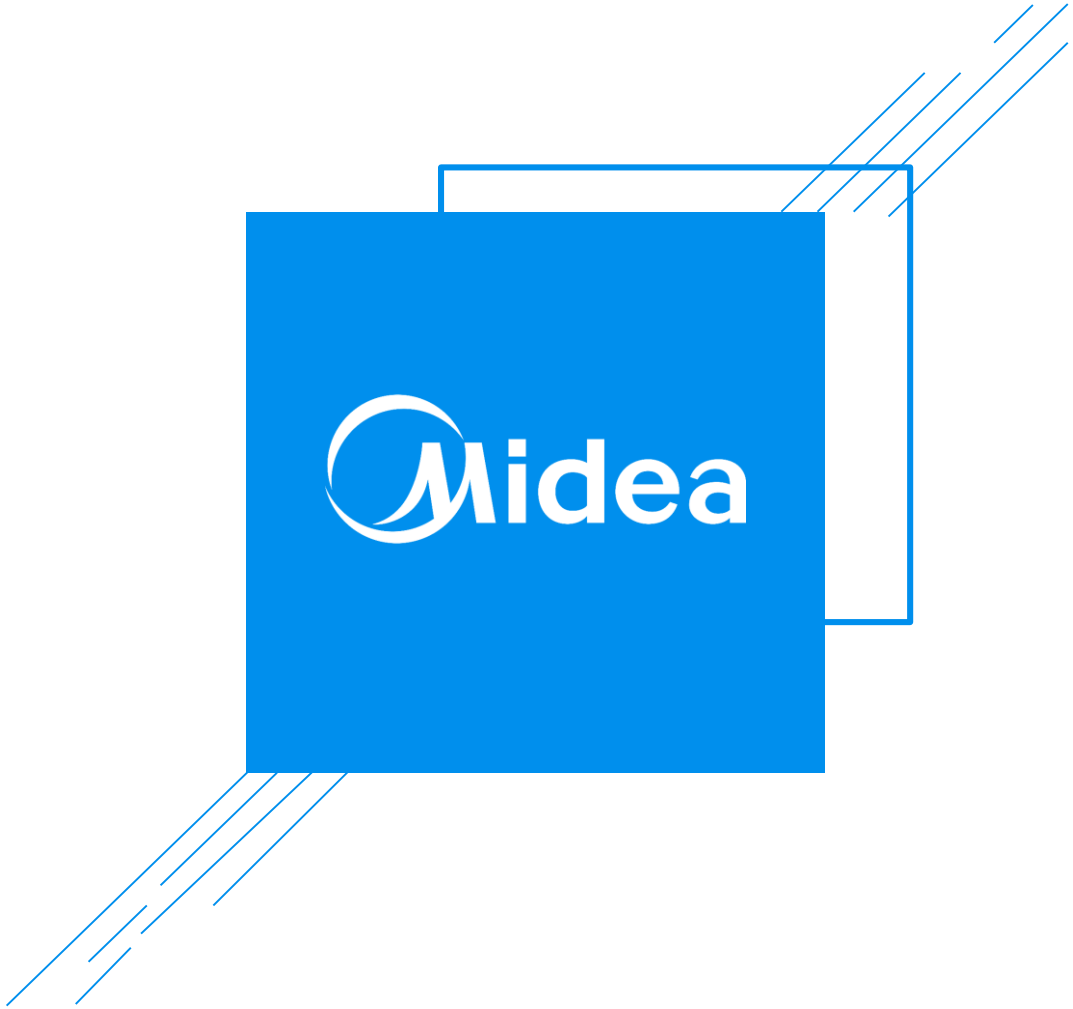
Midea
智慧生活可以更美的



美的智能家居隐私合规体系建设实践

美的集团

个人简介

Midea
智慧生活可以更美的

戚进业：美的IoT 应用安全与隐私专家

美的IoT 安全专家，8年的IoT安全攻防经验，专注于APP/云/智能家电的安全漏洞和隐私合规研究。

发展历程

Midea
智慧生活可以更美的

2019.07
安全与隐私保护成立

2019.10
美的美居获取ePrivacyApp 认证

2020.04
美居云平台通过PCI DSS 认证

2020.05
获取TRUST企业体系隐私认证

2020.06
美的多品类家电获取CCRC智能家居产品认证

2020.10
通过ISO 27701隐私体系认证

2020.12
美的多品类家电获取ETSI 303645欧洲隐私认证

2021.01
美的美居获取CCRC APP安全认证

2021.04
美的获取等保2.0三级备案证明

2021.05
美的多品类家电获取Nist8259隐私认证

2021.08
美的多款品类家电/APP获取IoXt安全认证

2021.7
美的物联网组件通过EAL4+ 认证

2021.10
美的云平台获取CSA STAR云安全认证

2021.11
美的集团获取新加坡政府颁发APEC CBPR认证

2021.12
美的IoT安全实验室正式通过中国CNAS /国际ISO 17025资质

2022.01
美的集团获取ISO 37301合规认证

2022.05
美的美居获得CNAAC APP安全认证

基本原则

温馨智能家庭来自安全的保障,我们把安全与隐私合规作为美的产品与服务的核心生命线，让用户随时随地享受智能便利、安全舒适的智能家居服务。

合法、公平和透明

个人数据以透明的方式对数据主体进行公平和合法的处理 。

目的限制

个人数据仅用于一个或多个特定和合法目的，不得以任何与目的不符的方式进行处理 。

数据最小化

个人数据是适当的、相关的，并仅限于它们被处理的目的所必需的。

准确性

个人数据是准确的，必要时更新，并采取所有合理措施立即删除或更正与其用途不准确的个人数据 。

存储限制

个人数据的维护形式允许仅在处理个人数据等所需的时间内识别数据主体。

确保安全

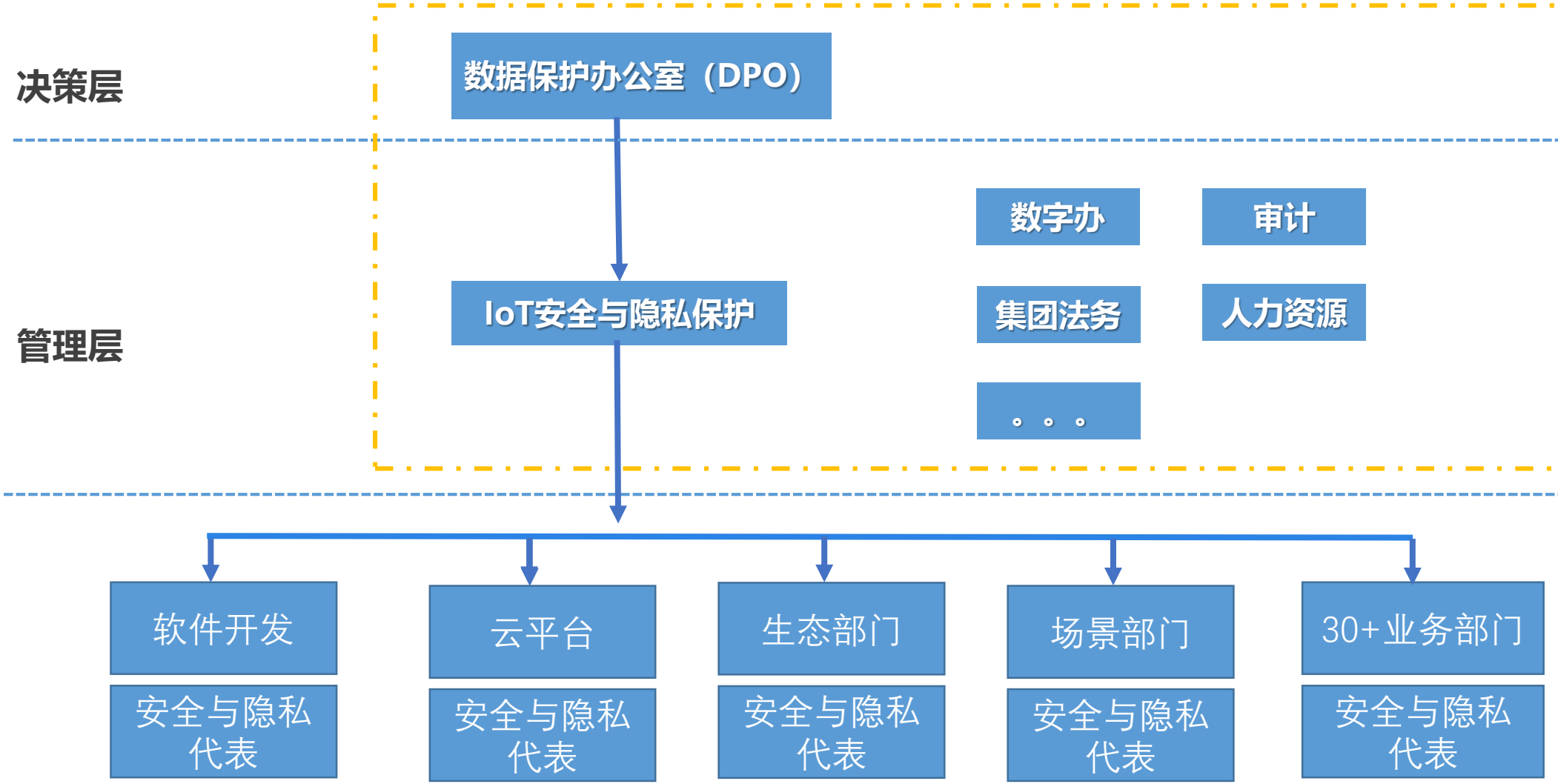
用适当的技术或组织措施,以确保个人数据处理的安全性,包括防止未经授权或非法处理以及意外丢失、破坏或变质 。

目的限制	• 仅为指定、明确和合法目的而收集 • 除非有法律另行说明的理由，否则不允许进一步处理
归责性	• 控制者要能举证证明自己的处理是合法、合理、正当、透明、获得同意的

组织架构

Midea
智慧生活可以更美的

安全与隐私保护体系



安全研发生命周期

Midea
智慧生活可以更美的

安全与隐私嵌入研发生命周期，通过标准/流程/技术,保障智能家居安全与隐私合规。

安全研发生命周期管理与控制

将安全与隐私保护要求嵌入研发各流程

需求概念	需求评审	开发		验证	发布与维护
安全需求评审	安全设计	安全设计	编码安全	安全测试样例	安全发布
STRIDE威胁建模	隐私合规	源代码扫描	第三方引入评估	安全测评报告	应急响应

通过安全能力的积累与提升，确保安全流程的有效执行

安全分析能力	安全设计能力	安全编码能力	安全测试能力	响应能力

全链路技术防护框架

针对个信息保护，提供“全场景守护，全链路安全隐私支撑”的技术框架

场景

智能家居　电商　会员　服务　售后　支付　.....

技术框架

服务安全	帐号体系安全	API接口安全	APP安全隐私检测	网关/WAF防护
	配网安全	应用签名防护	风控预警体系	APP隐私感知
数据安全	数据安全备份	国密算法支持	数据加密	数据脱敏
	数据权限管理	密钥安全管理	文件加密	数据运维管理
系统安全	系统加固	破解行为识别	OTA升级安全	
	系统安全启动	系统完整性保护		
家电硬件安全	解绑设备信息清除	eFuse 安全存储	PUF 安全技术	白盒加密方案

用户隐私感知 1/2

二级菜单中展示双清单列表

二级菜单中展示双清单列表

提升信息通信服务感知

美的IoT积极响应工信部《关于开展信息通信服务感知提升行动的通知, 建立“双清单”等相关要求，完成了全面排查与提升优化。充分保障广大用户知情权、选择权

用户隐私感知 2/2

Midea
智慧生活可以更美的

权限用途用户告知说明

告知用户获取和使用权限的理由，帮助用户决策，提升应用隐私保护透明度，增强终端用户隐私保护感知

访问摄像头权限

访问麦克风权限

检测平台

APP端**构建个人信息保护检查技术能力**,提前对风险进行识别与防护。

APP安全与隐私检测平台

SDK安全与隐私评估：支持1000+SDK隐私评估

权限评估：应用权限问题检测

硬编码安全评估：应用编码安全检测

漏洞评估：APP漏洞风险检测

黑灰产安全评估：黑灰产行为检测

敏感行为检测：隐私风险监控

安全实验室（CNAS认证）

Midea 智慧生活可以更美的

安全与隐私测试符合**国际标准的质量管理**体系,签发**安全测试报告**, 为美的智能化事业部安全性, 提供**客观公证能力。**

安全体系管理

组织管理	人员管理
设备管理	物联环境安全
样品管理	记录控制
报告签发	提测流程
内部审查	体系提升
质量控制	方法管理

技术检测能力

通信安全	个人信息保护
硬件安全	Zigbee通信安全
操作系统安全	业务逻辑安全
编码安全	蓝牙通信安全
OTA安全	安全审计
固件安全	数据保护

智能家居

安全与隐私测试（评估）报告

CNAS

报告专用章

专项治理

积极响应APP隐私合规相关治理工作，及时完成**自查与自纠**，审视和**刷新内部安全标准**,支持APP隐私安全治理工作

《个人信息安全规范》
《关于开展APP违法违规收集使用个人信息专项治理的公告》
《工业和信息化部关于开展信息通信服务感知提升行动的通知》
《中国消费者协会 - 50款APP账号注销及自动化推荐测评报告》
《APP侵害用户权益专项整治行动的通知》
《APP违法违规收集使用个人信息自评估指南》
《GB-T 35273—2020 信息安全技术 个人信息安全规范》
《信息安全技术 移动互联网应用程序（APP）个人信息安全测评规范》
《164工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》
《常见类型移动互联网应用程序必要个人信息范围规定》
……

1、要求解读 差距对标
2、自查自纠 需求整改
3、每版本复查 安全培训
4、形成隐私红线 制定内部标准

安全实践

Midea
智慧生活可以更美的

通过IoT官网、隐私白皮书、App以**开放透明**的方式，向用户传递我们针对用户**隐私保护的理念**与**努力态度。**

美的IoT官网

美的智慧生活隐私白皮书

APP隐私功能

权威认证

美的智慧生活隐私白皮书

IoT云端 + 美的管理体系

行业首家

- APEC CBPR
- 隐私信息管理体系认证
- 信息安全管理体系认证
- CNAS 智能家居安全实验室
- PCI DSS 认证
- 企业隐私体系认证
- 合规管理体系认证
- 等保2.0标准体系
- CSA STAR

APP端

- ePrivacyApp 个人数据保护技术认证

行业首家

- 移动互联网应用程序安全认证
- ioXt APP安全认证

行业首家

- CNAAC应用安全标识安全认证

家电端

行业首家

- IT 智能家居产品安全认证

行业首家

- ioXt 智能设备安全认证

行业首家

- ETSI 303645 欧洲隐私认证
- NIST8259 IoT安全隐私标准

行业首家

- 智能联接模组 EAL 4+
- 新加坡 CLS

Midea
智慧生活可以更美的

QA环节