

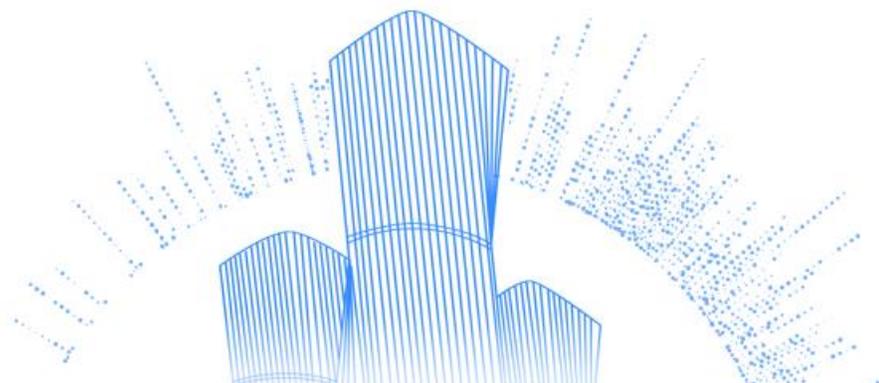


美的智慧生活隐私白皮书

Midea Smart Life Privacy White Paper

版本 V1.1

发布日期 2021年7月



版权声明©美的集团股份有限公司 2021。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

 和其他美的商标均为美的集团股份有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

用户购买的产品、服务或特性应受美的集团股份有限公司及其关联公司、经销商、终端零售商（以下简称“美的公司”）与用户签署的商业合同及产品说明书的约束，取决于用户购买的产品型号，本文档中描述的全部或部分产品、服务或特性并不适用于全部产品。除非合同另有约定，美的公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指引，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

美的集团股份有限公司

地址：广东省佛山市顺德区北滘镇美的总部大楼

网址：www.midea.com

用户服务电话：400-8899-315

用户服务邮箱：ec.user_service@midea.com

目录

1. 引言	1
1.1. 美的 IoT 简介	1
1.2. 智慧生活隐私白皮书发布目的.....	4
1.3. 名词定义.....	4
2. 美的隐私保护价值观	6
2.1. 美的 IoT 隐私保护价值观	6
2.2. 美的参考的外部法规、行业实践.....	6
2.3. 美的隐私保护责任	7
2.4. 美的隐私安全保护基本原则	10
3. 美的 IOT 致力于保护用户隐私安全	12
3.1. 美的 IoT 隐私安全保护管理措施.....	12
3.2. 美的 IoT 隐私安全保护技术措施.....	26
4. 美的在隐私安全领域获得的认证	36
5. 结语	44

1. 引言

1.1. 美的 IoT 简介

美的 IoT (Internet of Things) 公司 (以下简称“美的 IoT”或“我们”) 隶属于全球领先的家电巨头美的集团, 致力于构建面向智能家居、智能安防、人工智能等领域为用户提供全路径、全场景、全触点的以智能家电为核心的安全、便捷的物联网解决方案, 为客户提供优质的智能服务, 同时不断优化智能家居和相关服务的使用体验。

我们始终坚持“科技尽善, 生活尽美”的公司愿景, 始终坚持通过科技创新提升产品品质和服务质量, 专注于持续技术革新, 并以此贡献人类, 提高人类生活质量, 促进人类生活更舒适、更轻松、更美好, 让每个人和家庭享受到智能家居带来的美好生活。

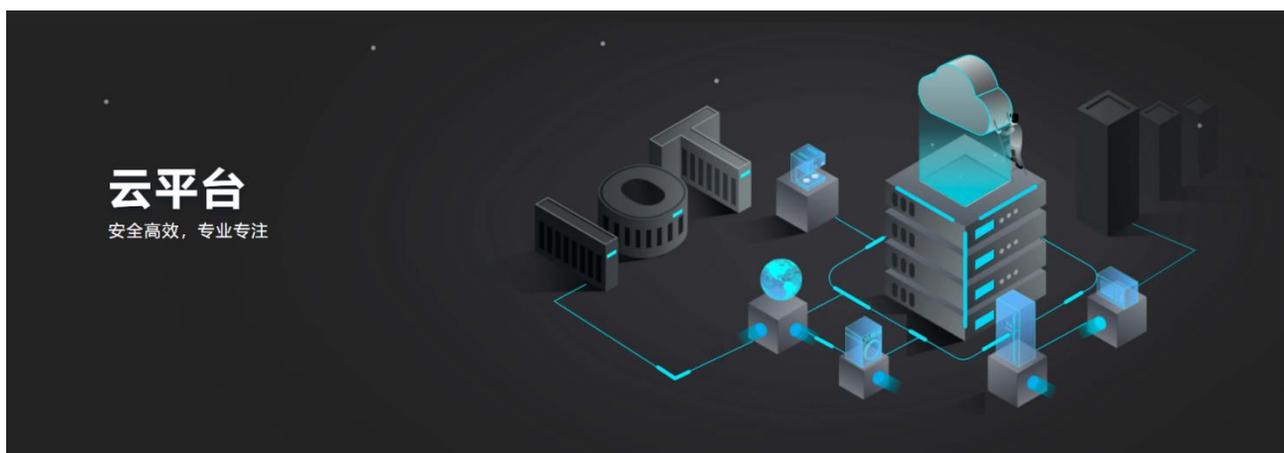


美的 IoT 是业内领先的智能家居解决方案提供商, 拥有全品类智能白电产品和海量智能硬件数据。在美的集团“全面数字化”和“全面智能化”的战略下, 美的 IoT 围绕“人和家庭”进行物联网全生态价值链建设, 探索以用户为中心的商业模式, 以“软件、内容、服务”为基础, 从美的美居 App 用户隐私安全保护、智能场景内容精细化运营、智能连接技术开发、智能家居生态品牌建设、云平台建设、AI 语音功能和大数据云管家等实现全方位突破。截至 2021 年 11 月, 美的智能场景累计执行超 3.3 亿次、智能云管家活跃数超 690 万。美的云平台与设备日均交互次数约 2 亿次。目前, 美的美居为用户提供智能食谱超过 1 万道, 可联动智能设备烹饪的超级食谱超过 7000 道。

美的 IoT 通过强大的创新及研发能力，推出了物联网平台及美的美居为智能家居产品提供服务支持。

1.1.1. 美的物联网平台

目前，美的 IoT 已在全球范围内部署了美的物联网平台，为全球用户提供高可用、安全、稳定的接入服务和快速、稳定的可自适应弹性伸缩扩展的服务。美的物联网平台拥有亿级的海量数据和支持千万级设备的并发连接的高性能处理能力，能够提供高可用、高稳定的不间断服务。通过整合亚马逊云、阿里云等全球服务节点资源，美的物联网平台高效应对海量智能硬件设备接入的挑战，不断丰富物联网云端设备连接、管理、互联互通、运营和大数据等能力，保障高效稳定的 IoT 设备使用体验，依托中国智造服务全球用户。



美的物联网平台为智能设备提供从售前咨询，售后使用及维修保障的全链路数据与服务支持，通过开发、测试、运行等周期管理智能设备，并支持自定义的设备管理服务。通过开放性架构和设计提供智能硬件全方位的应用层、感知层、接入层的可扩展性，为硬件厂商提供功能齐全的 SDK 和 API，最大限度地降低研发成本，提高智能产品的研发效率。同时，美的物联网平台通过美的内部的大数据平台将全品类智能家居数据进行整合，并通过数据洞察深度挖掘智能设备功能潜力及用户的数据价值，全面提升美的物联网平台用户体验，持续增强用户满意度。

1.1.2. 美的美居



美的美居是美的 IoT 全力打造的智能家电管理移动应用程序，支持美的集团旗下所有品牌以及加入美的美居生态链的智能家电和设备。通过美的美居，用户可以完成手机与智能硬件之间便捷快速的交互，并实现智能设备之间数据的互联互通，按照自己的使用习惯设置个性化的智能家居场景，打造一个健康、个性的未来之家。

1.2. 智慧生活隐私白皮书发布目的

美的 IoT 十分重视用户的隐私安全，并希望通过智慧生活隐私白皮书带领用户深入了解美的 IoT 隐私保护政策及数据安全保护措施。本文档从以下方面讨论帮助用户了解我们的隐私保护实力以及如何保护用户的个人数据：

- 美的 IoT 的隐私保护价值观；
- 美的 IoT 在个人数据保护方面的管理措施与技术能力；
- 美的 IoT 的数据安全及隐私保护认证资质。

1.3. 名词定义

- **IoT**：即物联网（Internet of Things），通过各种信息传感器、射频识别技术、全球定位系统、红外感应器各种装置与技术，实时采集任何需要监控、连接、互动的物体或过程，采集各种需要的信息，通过各类可能的网络接入，实现物与物、物与人的泛在连接，实现对物品和过程的智能化感知、识别和管理。
- **网络安全法**：《中华人民共和国网络安全法》，在中华人民共和国境内建设、运营、维护和使用的网络，以及网络安全的监督管理所适用的法律。
- **GDPR**：欧盟通用数据保护条例（EU General Data Protection Regulation）的简称，是全球最严格、最权威的数据保护法之一。
- **CCPA**：加利福尼亚州消费者隐私保护法案（California Consumer Privacy Act）的简称，对处理加州居民个人数据的营利性实体进行限制，以保护消费者个人数据。

- **CNAS**：中国合格评定国家认可委员会（英文缩写为：**CNAS**）是根据《中华人民共和国认证认可条例》的规定，由国家认证认可监督管理委员会（英文缩写为：**CNCA**）批准成立并确定的认可机构，统一实施对认证机构、实验室和检验机构等相关机构的认可工作。
- **数据主体**：指其个人信息被作为个人数据在网络中以或明或暗的方式加以披露的自然人。
- **数据控制者**：能单独或联合决定个人数据的处理目的和方式的自然人、法人、公共机构、行政机关或其他非法人组织。
- **个人数据（或“隐私数据”）**：指任何指向一个已识别或可识别的自然人（“数据主体”）的信息。该可识别的自然人能够被直接或间接地识别，尤其是通过如姓名、身份证号、地址数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份等信息识别。
- **处理**：是指针对个人数据或个人数据集合的任何一个或一系列操作，诸如收集、记录、组织、建构、存储、自适应或修改、检索、咨询、使用、披露、传播或其他的利用，排列、组合、限制、删除或销毁，无论操作是否采用自动化的手段。
- **SDK**：即软件开发工具包（**Software Develop Kit**），为特定的软件包、软件框架、硬件平台、操作系统等建立应用软件时的开发工具的集合。
- **DPIA**：即数据保护影响评估（**Data Protection Impact Assessment**），用来描述个人数据的处理、评估处理的必要性和相称性、并识别和管理自然人因处理个人数据而产生的风险，并提供针对这些风险的处理方法。

2. 美的隐私保护价值观

2.1. 美的 IoT 隐私保护价值观

温馨智能家庭来自安全的保障，美的 IoT 以智能互联为驱动，在科技智能连接家居的同时，我们把保障用户个人数据的安全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。

2.2. 美的参考的外部法规、行业实践

美的 IoT 一直致力于遵循各国的数据安全与隐私保护法规的要求，如我国的《网络安全法》《欧盟通用数据保护条例（“GDPR”）》以及《加州消费者隐私法（“CCPA”）》等保护用户的隐私安全。美的作为消费者信赖的全球化科技集团，严格遵守我国《消费者权益保护法》，并依据我国权威部门发布的《App 违法违规收集使用个人信息行为认定方法》、《GB/T-2020-35273 信息安全技术-个人信息安全规范》、《工信部 APP 侵害用户权益专项整治 8 项要求》的要求提升美的的美居在 App 端的合规性及个人信息保护能力。

同时美的 IoT 落实国际权威的安全标准及行业最佳实践，如 ISO27001 信息安全管理体系及 ISO 27701 隐私管理体系，建立并形成了具有美的特色的智慧家居隐私管理与安全体系。



美的 IoT 是中国家用电器协会、和电信终端产业协会和智能家电云云互联互通工作组的成员，是智能家电云云互联互通工作组-安全组的组长单位，牵头制定了《中国智能家居云云互联互通信息安全标准》。此外，美的 IoT 还加入了中国通信标准化协会，参与了相关的物联网标准的制定和撰写，包括《信息安全技术 智能家居安全通用技术要求和测试评价方法》、《智能家用电器个人信息保护要求和测评方法》等行业标准的制定。

美的 IoT 参与美国 ASTM 材料实验协会对联网消费产品安全标准的意见征集，该标准主要为解决消费者产品具备互联功能后逐渐担心的安全隐患问题，旨在用作互联消费产品制造商的指南，确保其连接功能相关的物理安全。

美的 IoT 参与编纂了由国家市场监督管理总局、中国国家标准化管理委员会发布的《家用和类似用途电器专用 WLAN 通信模块技术规范》，针对其信息安全要求中的固件安全、数据保护、安全审计等规范提出修订建议并被采用。

美的 IoT 携手信息安全检测设备及技术研发商纽创信安、中国科学院的密码学家王小云院士成立智能家居终端安全与国密密码算法研究技术联合实验室，针对智能家电的终端安全、协议安全、适配国密密码算法安全等核心技术和应用展开研究，推进相关核心技术的产业化、产品化，增强终端安全的攻防实战能力。

2.3. 美的隐私保护责任

用户在使用美的 IoT 产品及美的美居的过程中，美的基于运营支持及服务开展需收集用户个人数据，部分数据的收集、处理过程由美的 IoT 协同第三方供应商共同进行并共同承担个人数据的保护责任。其中，美的 IoT 负责美的物联网平台内的服务和数据交互的安全管理和运营，对其提供的美的物联网平台和基础架构的安全性负责；第三方供应商的云服务安全、SDK 的个人数据保护责任由美的 IoT 和供应商共同承担。

我们将基于下图的责任模型介绍美的 IoT、供应商需要承担的隐私保护责任和义务。



美的 IoT 的责任：

美的 IoT 负责美的美居的服务和数据交互的安全管理和运营，对向用户提供的服务的隐私保护及安全性负责，其中安全责任覆盖数据安全和用户隐私权利保障。美的 IoT 提供 APP 的安全运维和运营服务，切实保护美居的安全运营，以及保障用户个人数据的安全，包括但不限于：

- **数据安全：**对收集的用户数据实施管理措施，包括收集与识别、PIA 评估、分类与分级、权限与加密以及隐私合规等方面；
- **访问控制管理：**对存储在美的物联网平台的用户个人数据进行严格且合理的访问权限控制，包括用户管理、权限管理、身份验证等；
- **数据主体权利响应：**根据《中华人民共和国网络安全法》等适用法规中对用户权利响应的要求，美的 IoT 隐私声明中描述了美的保障用户的知情权、访问权、删除权、更正权等权利的责任，并通过美的美居或 DPO 邮箱，对客户各项主体权利提供切实的支持。

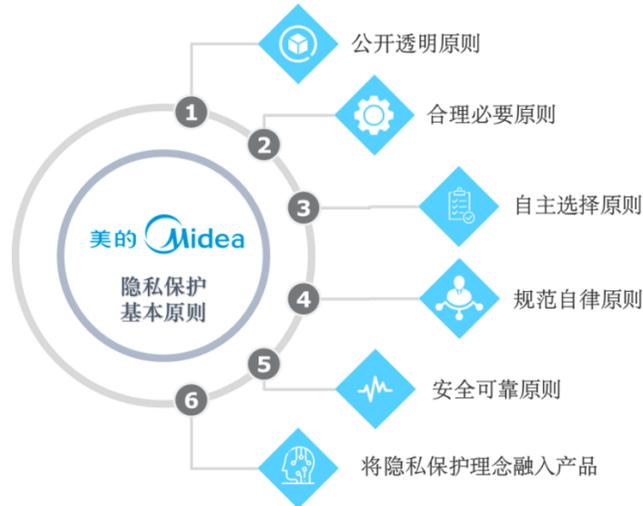
美的 IoT 与第三方供应商共同承担的责任：

美的将与第三方供应商共同维护美的物联网平台以及第三方 SDK、第三方云服务的安全。主要包含：

- **美的物联网平台安全：**美的 IoT 选择全球知名的云服务供应商亚马逊云、阿里云等全球领先的云计算供应商进行合作，并在签订的合同中对服务可用性及安全服务提出要求，确保云服务的基础设施、物理设备的安全和可靠。
- **供应商隐私管理：**美的 IoT 和第三方供应商合作的时候，供应商需要严格按照美的 IoT 的安全配置和接入要求执行。对于美的 IoT 的数据安全合规、隐私政策等相关信息，我们严格遵循相关的法律和规章制度，与此同时，供应商也必须提供和遵循数据安全和隐私保护的解决方案和服务，确保用户个人数据安全。

2.4. 美的隐私安全保护基本原则

参考适用的隐私保护法律法规与 ISO 27701 标准的要求，美的 IoT 确定了六大隐私保护基本原则，覆盖产品设计、数据收集、数据保护及数据主体权利响应等方面。具体原则如下：



- 公开透明原则

我们将以明确具体，通俗易懂且不设障碍的方式在隐私政策及隐私协议中向用户告知我们收集个人数据的原则，以及收集个人数据的方式、目的、范围和期限。若数据处理的目的、收集的个人信息类型发生变更，我们将更新我们的隐私政策，并告知用户，重新获取用户的同意。

- 合理必要原则

我们严格遵守“合法、正当、必要”的个人数据保护的原则，明确仅收集为提供服务所必须的个人信息。为给用户带来更好的产品用户体验，我们所提供的产品及服务将尽可能最小限度地向用户申请收集最少量的、为提供服务所必需的个人信息。此外，为保障数据私密性，数据处理也会尽可能地在设备本地进行，减少个人信息上传尤其是跨境传输。

- 自主选择原则

用户有权要求访问、更正、删除我们持有的与个人信息，可自主选择允许或拒绝提供个人信息。我们为用户提供完善的主体权利响应机制，用户可以通过 DPO 邮箱与我们联系，确保数据主体权利得到保障。

- **规范自律原则**

我们在内部建立系统化的隐私合规审查机制，确保各业务部门同样重视您的个人数据安全。我们的合规审查机制贯穿产品全生命周期，从产品设计到开发、测试、上线，都有专业审查团队进行数据保护影响评估及安全性测试。

- **安全可靠原则**

用户的个人信息是无价的，对于用户的个人数据，无论是传输或者存储，我们都采用严格健全的保护措施，降低数据泄漏风险。传输过程采用了 **HTTPS** 安全传输、敏感信息哈希混淆、传输链路保护等方式最大程度保障传输安全性；数据存储方面，本地存储采用文件级加密、密钥分离等保护方式，云端存储则采取了安全等级分类、多种加密保护等保护方式。

- **将隐私保护理念融入产品**

为保障用户获得更加安心舒适的产品服务体验，在产品或服务的计划，评审，开发，测试等各个环节，将法律、开发、产品、设计等多因素融入隐私保护理念，在产品服务的全流程加强对用户个人隐私数据的保护。

3. 美的 IoT 致力于保护用户隐私安全

美的 IoT 深知隐私管理方法与隐私管理技术同样重要，因此从隐私管理层面建立隐私管理制度以及全公司的隐私保护文化，同时加大隐私安全技术投入，不断增强保护用户隐私安全的能力。我们将从管理和技术两个方面介绍美的如何保护用户个人数据的安全。

3.1. 美的 IoT 隐私安全保护管理措施

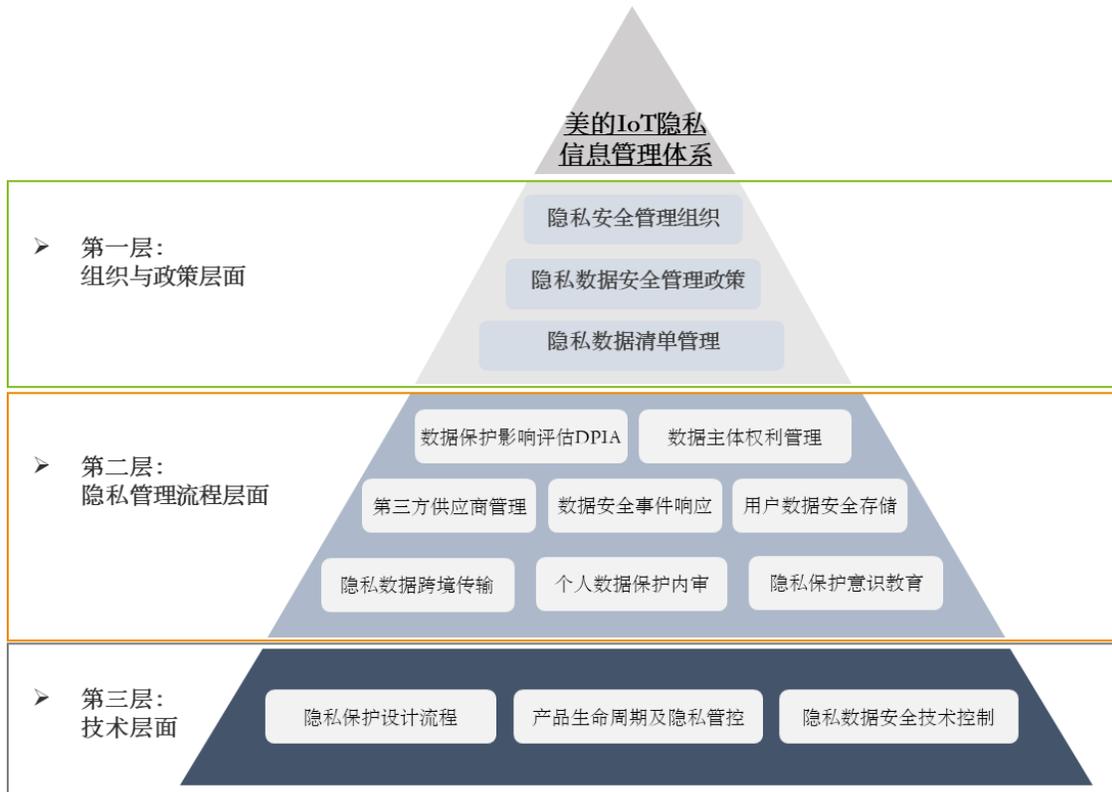
3.1.1. 领导层的声音

美的领导层高度重视智能家居领域的隐私安全，将个人数据安全和隐私保护作为公司最核心的战略之一，通过自上而下的治理架构来实现。在组织方面，数据保护办公室（Data Protection Office, 简称 DPO）作为公司最高的数据安全与隐私保护机构，决策和批准公司的总体的安全策略和安全解决方案。美的集团首席合规官（Chief Compliance Officer, 简称 CCO）、美的集团信息安全 IT 部长和美的 IoT 首席安全官（Chief Security Officer, 简称 CSO）及其办公室负责领导和制定美的隐私保护管理体系。美的集团信息安全 IT 部长和美的 IoT CSO 直接向美的集团首席信息官 CIO 汇报。

秉承美的隐私安全保护的战略和规范，美的 IoT 安全与隐私保护部门对本领域安全工作进行自主规划和管理。全面实现隐私安全保护业务的研发运维运营组织合一，一方面需要满足业务部门快速持续研发、交付与上线的进度要求，另一方面要保证必需的安全质量标准，有效控制安全风险。依托着美的安全工程能力、安全服务和安全解决方案的设计、开发和运维等职能，构建美的 IoT 安全合规运营能力，切实保障用户利益。基于隐私安全对美的 IoT 的特殊重要性，安全与隐私保护部门直接向美的 IoT CSO 汇报。

3.1.2. 美的隐私保护管理体系

参考 ISO27701、ISO27001、网络安全法、GDPR 等要求，结合美的 IoT 发展战略及隐私保护现状，形成了由组织及政策（如下图绿色框）、隐私管理流程（如下图橙色框）及技术（如下图灰色框）三个层面组成的隐私管理体系。



第一层：组织及政策层面

- 个人数据安全组织

参考法律法规要求，美的 IoT 在公司内部设立了由承担数据保护及隐私保护职责的数据保护办公室（Data Protection Office，简称 DPO）、安全与隐私保护部门、各业务部门数据保护代表（Data Protection Representative，简称 DPR）及业务部门具体实施的相关员工组成的四级数据安全及隐私保护组织。



数据保护办公室（DPO） 由美的集团首席合规官、IT 信息安全部长以及 IoT 美的 IoT 首席安全官组成，履行集团个人信息保护指导与监督的职责，包括跟踪监管机构发布的数据保护、隐私保护领域隐私法规和相关标准，衔接监管机构和数据主体之间的沟通，识别数据安全与隐私风险，开展公司隐私保护文化建设。

安全与隐私保护部门 美的 IoT 安全与隐私保护部门，负责美的 IoT 的信息安全及隐私保护相关工作，亦作为 DPO 与业务部门之间的桥梁，负责 DPIA 评估，隐私保护及安全需求的导入，隐私保护意识的宣贯工作。部门的主要职责包括：

- 基于产品开发生命周期导入隐私保护及安全要求，建立贯穿全生命周期的 PbD 流程，包括安全需求分析、DPIA 评估、隐私编码安全要求等；
- 积极实施隐私及安全评估，开展漏洞扫描、渗透测试等相关技术测试，监控、排查并解决识别的安全漏洞及威胁；
- 梳理不同国家、地区的个人数据保护相关法律法规及全球隐私保护最佳实践，识别适用于美的 IoT 的隐私保护要求；
- 推进业界相关隐私保护及安全领域认证的获取，推动美的 IoT 内部隐私保护体系建设，提升内部员工的隐私保护意识；

数据保护代表（DPR） 作为安全与隐私保护部门及各业务部门的员工沟通的联结者角色，传达数据保护办公室发布的隐私保护相关政策，协助业务部门员工开展隐私保护活动，并对隐私活动的效果进行评估及审核。

各业务部门的相关员工 负责隐私保护活动的具体执行及监控，若发生数据泄露事件应及时向数据保护代表报告。

- **个人数据安全管理制度**

美的 IoT 依据 ISO 27701 的体系标准，建立健全了自身的隐私管理体系制度文件，共对应体系中的 18 个控制域（一级文档信息安全与隐私管理政策和适用性声明对应的信息安全策略、系列二级制度文档对应信息安全组织、人力资源安全、资产管理、访问控制、密码学、物理和环境安全、操作安全、通信安全、系统获取开发和维护、供应商关系、信息安全事件管理、信息安全业务连续性管理、符合性，外加收集和处理条件、PII（可识别个人信息）主体的义务、隐私保护设计和默认隐私保护、PII 共享、传输和披露），从制度上全面指导员工遵循公司的隐私价值观，承担隐私保护责任。

02

个人数据保护附加管控要求

除在信息安全管理体系统基础上增加的隐私保护要求外，ISO27701针对PII控制者和处理者提出了四个领域的管控要求，分别是：收集和~~处理~~PII的条件、对PII主体的义务、默认隐私设计、PII共享、转移和披露

02 个人信息附加管控要求

01 隐私管理体系管控要求

01

隐私管理体系管控要求

ISO 27701在ISO27001的14个控制域的基础上增加了32条适用的隐私保护相关要求，包括资产管理、风险评估、系统开发、运行安全、供应商管理、信息安全事件等领域提出要求；

- 个人数据清单管理

在用户使用美的 IoT 设备及美的美居的过程中，为了保障基本的服务需要以及产品更好的服务，美的 IoT 基于数据最小化原则收集个人数据。美的 IoT 收集以下 5 种场景的个人数据：账号数据、电商数据、社区及食谱数据、美的美居智能服务数据、美的美居运行数据，均为提供指定服务所必需，且在收集前通过签署隐私协议获取用户的明示许可。



用户注册时可能会收集的个人信息包含手机号码、用户 ID、密码、昵称、头像、性别等；电商数据包含配送地址、收货姓名、安装及维修地址等；社区及食谱数据为优化推荐功能，会收集用户的性别、年龄、身高、过敏食材、偏好菜系等信息；美的美居智能服务可能收集体重信息、血糖信息、食材信息及交互所必须的语音数据；另外在使用过程中基于网络安全保护的要求系统可能收集设备 IMEI 号码、硬件型号、IP 地址、位置信息、MAC 号码、图像及视频、上网记录。美的 IoT 收集的所有个人信息均会在隐私协议中进行说明，用户可在 APP 查看具体收集的个人信息清单。

美的 IoT 将持续维护可能收集到的个人信息清单并制定与之匹配的隐私保护措施，保障全面、适当地管理个人信息。

第二层：隐私管理流程层面

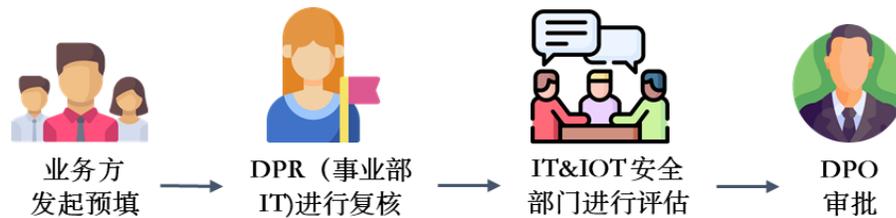
- 数据保护影响评估

美的 IoT 依据 GDPR 的要求开展 DPIA 数据保护影响评估，以系统地分析、识别和最小化项目的数据保护风险。DPIA 评估主要涉及以下几个方面的内容：



DPIA 评估的业务流转过程如下图：在开展常规的数据处理之前，数据控制者将进行数据收集及处理影响评估，在涉及到使用新技术、拟使用个人信息进行用户画像及自动化分析等数据处理时，美的 IoT 也会开展数据保护影响评估。

评估流程：由业务人员预填 DPIA 评估表，并提交业务部门 DPR 复核。业务部门复核完毕后，DPIA 评估表流转至 IT 及 IoT 安全部门进行评估：对收集的个人信息尤其个人敏感数据进行梳理，分析上述数据处理行动对数据主体权利可能造成的影响，评估使用个人信息可能存在的风险，兼顾产品设计及用户的隐私保护。IT 及 IoT 评估完成后，将汇总评估意见，交由 DPO 数据保护办公室进行最终审批。



- 数据主体权利管理

美的 IoT 基于 GDPR 的要求回应数据主体的权利请求，全面支持数据主体的知情权、访问权、更正权、被遗忘权、数据可携带权、拒绝权等。

知情权:

- 隐私协议中已明确美的美居中收集的所有用户数据类型及与之相对应的用途；同时，已针对用户所拥有的主体权利和义务进行阐述；
- 隐私协议中列明了美的 IoT 对个人数据的处理方式，如：数据收集、删除、迁移、保存；
- 隐私协议如有更新将通过 App 告知用户，并重新获取用户的同意。

访问权:

- 用户可在美的美居中访问美的 IoT 收集的个人信息，无需另外技术支持；
- 用户可通过 DPO 邮箱向美的 IoT 发送邮件，要求告知对其数据的处理和使用情况。

更正权:

- 用户可在美的美居中对其个人信息进行更正修改；
- 用户可通过 DPO 邮箱向美的 IoT 发送邮件，要求对其数据进行更正。

被遗忘权（数据删除权）：

- 用户可在美的美居中注销账户，除法律另有要求外，注销后其个人信息将被删除。

可携带权（提供副本）：

- 用户可通过 DPO 邮箱要求美的提供所收集的個人資料的可读副本。

拒绝权：

- 用户可通过 DPO 邮箱拒绝美的对其个人数据进行处理。

为了让用户方便快捷地行使其自主选择权及其他数据主体权利，美的 IoT 提供便利的个人信息管理机制，方便用户自主删除、修改、查询其在美的产品及服务中所提供的个人数据，并且可自主选择同意或者撤回收集个人数据相关权限。针对限制处理权、获取个人数据副本的权利等无法自主管理的权利，用户可向隐私协议中的 DPO 邮箱发起书面申请，美的 IoT 的专门的服务团队将于法规限定的时间内回复并响应数据主体请求。



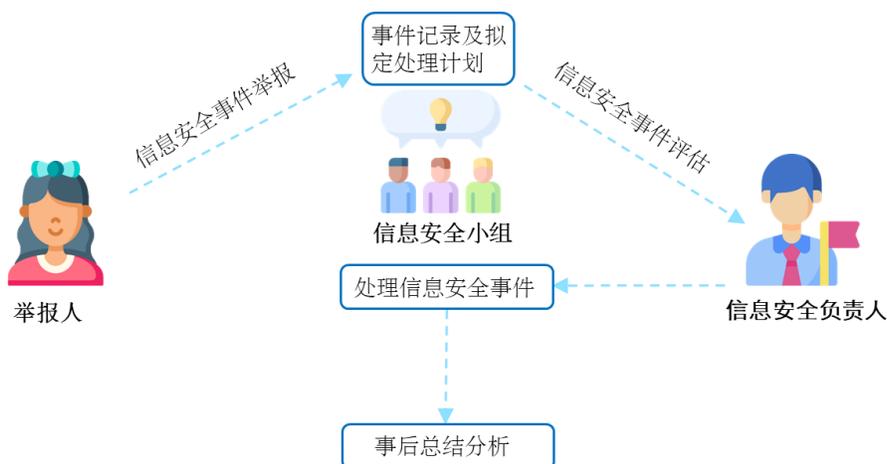
- **第三方供应商管理**

美的 IoT 可能会基于用户服务的必要，会将用户的部分脱敏数据提供给第三方进行委托或共同处理，如共享语音数据给第三方供应商进行识别并转化为家电控制指令、第三方供应商验证恶意手机号码等，我们提供给第三方的数据不包含用户的个人数据。美的基于隐私安全的基础对供应商设立了严格的供应商引入和管理流程。所有美的 IoT 的供应商均需同美的 IoT 签署《数据处理协议（Data Process Agreement）》，《数据保密协议》和《数据保护承诺（Data Protection Agreement）》。同时，美的 IoT 将对第三方 SDK 进行检测，扫描 SDK 数据收集情况，评估其信息收集的合理性。

- 《数据处理协议》中会明确美的 IoT 和供应商的信息安全职责，并对供应商人员的资历要求进行规定，检测供应商是否履行协议中规定的信息安全条款；
- 《数据保密协议》明确了供应商需要的保密信息并履行相应的保密义务；
- 《数据保护承诺》从供应商的义务、通知义务、技术与数据安全、分包、数据的终止、返还和删除等多个方面约束了供应商在数据保护方面的要求；
- SDK 引入流程：SDK 的信息收集与传输、安全技术评估、SDK 代码扫描供应商需提供 SDK 信息收集与数据传输现状，然后由安全与隐私保护部门评估 SDK 收集用户信息的合理性，并使用 SDK 代码扫描工具作验证 SDK 信息收集与数据传输是否涉及用户个人数据；
- 云云对接数据范围：美的物联网平台的用户个人数据和归属合作平台的数据，不会执行任何未获授权的使用和披露，但是以下情形除外：在国家机关依法查询或调阅用户个人数据时，平台将按照相关法律法规或政策文件要求提供配合，并向第三方或者行政、司法等机构基于最小化原则进行披露。。

• 数据安全事件响应

美的 IoT 已建立全面有效的安全事件管理机制，包含监控、识别并记录数据泄露、系统入侵等安全事件的流程，流程中涉及到的员工的相关责任与具体的操作规范，以及事件后续处理、向监管机构或数据主体的报告。同时我们建立了良好的反馈机制，及时总结事件中的经验，避免类似的事件再次发生，持续提升数据安全保护能力。



- 用户数据安全存储

美的 IoT 收集的数据主要存储在中国、美国和德国的云供应商数据中心。

- 中国：数据保存在中国杭州及上海机房，由阿里云提供基础云计算支持；
- 美国：美国数据中心位于美国俄勒冈机房，由 Amazon AWS 提供基础云计算支持；
- 欧盟地区：数据保存在德国法兰克福机房，由 Amazon AWS 提供基础云计算支持；
- 其它国家：根据就近原则选择俄勒冈或法兰克福机房存储。

- 个人数据跨境传输

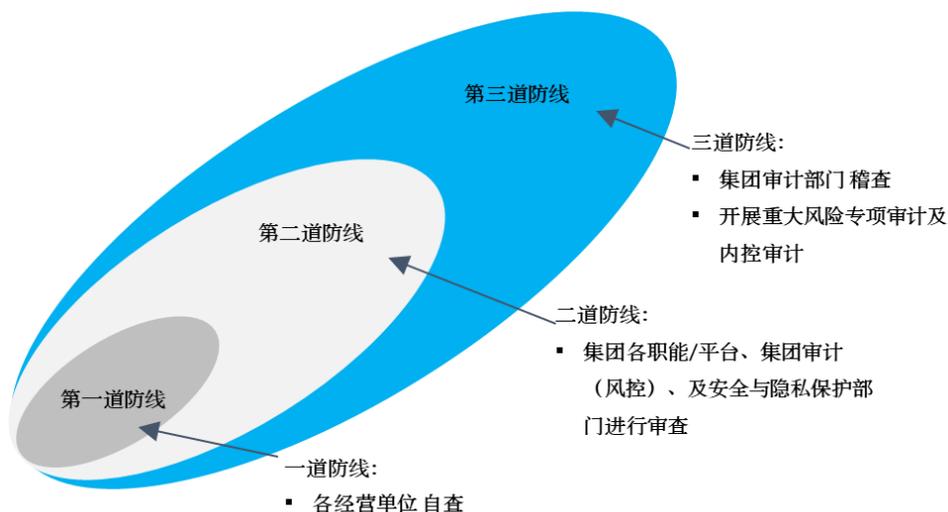
美的美居：美的物联网平台与广受认可的云服务商建立了合作关系，在国内使用了国内最大的云服务商——阿里云作为美的物联网平台的供应商。由于美的美居主要服务于国内用户，因此用户的个人数据、操作数据的传输、存储均位于国内的服务器，不会进行跨境传输。

MSmartLife（国际版美的美居）：其他国家的用户，使用全球领先的亚马逊云（AWS）进行平台支持，根据实际需要存储在美国及德国的服务器，跨境传输前通过隐私协议告知用户并通过 App 取得数据主体对其个人数据可能转移到其他国家或地区的同意，传输过程均会进行加密或匿名化处理，并遵循 GDPR 中关于跨境传输的要求。



- 个人数据保护内审

美的集团建立了三级风控防线制度，其中审计部门作为第三道防线，独立、公正地开展年度集团审核以及针对各类信息安全的专项审计，定期监察数据安全、隐私保护落实情况，确保重大风险得到有效管控，对重大、共性风险案例进行剖析保障制度、流程、标准在隐私保护效果的有效性。



- 隐私保护意识教育

为提升全员的隐私保护意识，降低隐私安全事件发生的风险，保证业务的合规、正常的开展及运营，美的 IoT 针对美的集团全体员工定期开展隐私保护培训。

通过美的的内部培训系统“美课”定期安排隐私保护相关培训，平均每两个月至少开展一次隐私保护教育的线上学习，保证隐私保护意识的持续宣贯和普及。

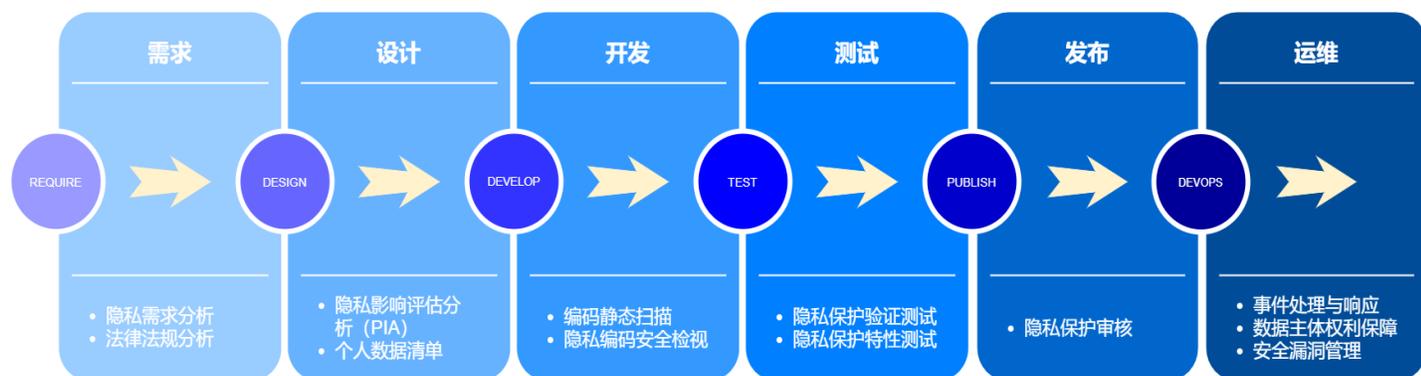
培训亦会向员工介绍美的的内部建立的隐私保护相关政策和制度，以及在隐私保护领域获取的认证，确保其了解需要遵循的基本的隐私保护法规或相关行业标准的要求，可以识别哪些是个人一般数据和敏感数据，哪些操作和行为是不适当、不可接受的，确保将正确妥当的操作落实到日常的工作中。

第三层：技术层面

• 隐私保护设计（Privacy by Design）流程

美的 IoT 以用户的个人数据为中心，在尊重用户的隐私、主动保护个人数据的基础上，贯彻隐私保护设计，在需求分析和产品设计阶段将个人信息保护纳入考虑范围，在产品开发和测试阶段将编码安全检视和隐私保护验证融入流程，在产品发布和运维阶段将隐私保护审核、数据主体响应和安全漏洞管理运作嵌入机制，基于隐私全生命周期保护个人数据安全，严格遵循美的的 PbD 设计指引，贯彻适用于个人数据的创建、收集、存储、共享和删除等处理过程的 8 项个人信息保护设计原则。

• 美的 IoT 产品生命周期及隐私管控



需求： 在产品的需求分析过程中，我们会对适用的隐私法律法规、行业标准进行分析，整理出各国法规或行业标准中需要遵循的隐私保护相关要求，确保产品需求符合法律与标准。同时针对业务部门或产品团队提出的需求进行评审，确定新需求是否满足美的 IoT 内部的隐私保护原则、是否可以充分响应消费者作为数据主体的权利，从内部到外部分析产品需求在隐私保护层面的合理性。

设计： 在产品的设计阶段，我们会梳理涉及的所有个人数据类型并记录，通过 DPIA 评估识别潜在风险，确保收集的数据符合安全隐私合规要求。我们会严格遵从美的 IoT 安全设计原则、规范、安全设计基线，在安全需求分析和设计阶段根据数据流图、业务场景、组网模型进行威胁建模。威胁建模使用的引导分析威胁库、消减库、安全设计方案库来源于美的的所有产品的安全积累和行业最佳实践。识别威胁后，设计工程师会根据消减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求和功

能，并根据公司的测试用例库完成安全测试用例的设计，确保产品的最终落地，保障产品服务的安全。

开发：我们严格遵从美的 IoT 对内发布的多种编程语言的安全编码规范，在产品的开发阶段通过编码静态工具扫描及隐私安全编码检视，所有产品在发布前均需完成静态代码扫描和告警高中危漏洞清零，防范开发过程中的安全风险。

测试：在产品测试阶段，所有隐私特性需通过安全专家和自动化工具的严格审视和测试，确保隐私需求和设计在产品中实现。我们开发和部署了自动化隐私安全测试平台，可通过自动化扫描 App、SDK 获取其申请的权限信息、调用的 API 接口等信息，将信息综合分析后可准确识别第三程序收集用户个人数据的情况。安全专家将根据工具输出的扫描结果对第三方 App、SDK 进行隐私安全评估，在测试阶段严守用户隐私安全。

发布：为确保产品满足属地法律法规、客户安全需求，在产品的发布前需要提交隐私保护审核流程，我们的数据保护办公室（DPO）将会参与到审核流程中，共同分析、判断其相关版本或服务是否符合属地安全隐私合规要求。同时产品团队在上线过程中需进行自检，自检结果也同步提交给美的 IoT 安全与隐私保护部门，通过更多的投入、在短时间内执行更严格的上线检测和审批，确保产品及时安全发布，保障用户利益。

运维：在服务持续运维运营阶段，我们通过严格的账号认证、权限管控和日志审核防止非授权访问和处理个人数据，保障数据主体权利，确保云服务持续的隐私安全。与此同时，我们建立了漏洞感知、管理、响应和处理制度。美的 IoT 安全应急响应中心公开了收集漏洞页面，鼓励社会白帽子、供应商、安全公司、组织、安全研究者和美的员工等提交美的产品或解决方案的漏洞。我们对所有收集的漏洞进行严重性评估，并结合漏洞在产品中被利用的风险评估结果决定处理优先等级，根据优先等级及时响应和修复漏洞，防止漏洞被恶意利用影响用户。

- **个人数据安全技术控制**

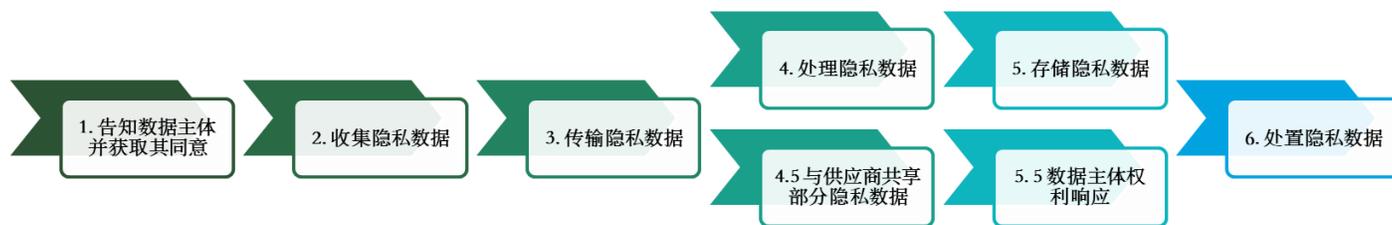
美的 IoT 建立了一系列安全规范、使用多种安全技术保障个人数据的安全。美的强大的 IT 团队致力于保障隐私安全技术实现，如产品侧与 App 侧终端安全、云端安全保障、业务安全与风控系统、个人数据安全保护技术等，落实隐私安全管理政策。

本文将在 3.2 章节详细介绍美的 IoT 如何使用信息技术保障个人数据全生命周期安全。

3.1.3. 用户隐私数据生命周期

美的 IoT 定义了其在 IoT 业务模式下的个人数据生命周期，将其分为了 6 个主要阶段，并以此为框架对用户个人数据进行全生命周期管理，以保障在所有阶段个人数据都将合法合规、安全处理。

由于根据个人数据处理需求需要与供应商共享个人数据，或在个人数据收集并存储需要响应数据主体的权利请求，将这两种特殊场景分别纳入 4.5 及 5.5 阶段。这两部分内容已在前文进行介绍，本章仅介绍在其他个人数据生命周期内，美的 IoT 如何确保数据处理合规和数据安全。



图表 1 美的 IoT 隐私数据生命周期

阶段 1 告知数据主体并获取其同意

用户注册美的物联网平台或美的美居时，将会以弹窗等方式向用户展示隐私协议，只有在获得用户明确同意，即点击“同意”按钮后，我们才会开始收集用户的个人数据。其中隐私协议参照网络安全法及 GDPR 的要求，告知用户收集个人数据的类型、收集目的、保存期限、数据主体权利及美的 DPO 的联系方式，以落实美的 IoT 的公开透明原则。

阶段 2 收集个人数据

美的 IoT 基于合理必要原则收集用户的个人数据，严格遵循不收集超过用户授权范围之外的个人数据，并且参考 GDPR 的合法性原则保证收集、使用用户个人的方式及目的遵循相关法律规范且合理明确，收集的用户个人数据应仅限定用于隐私协议中规定的目的。

因此我们针对美的物联网平台及美的美居均进行了数据保护影响评估，对二者涉及的个人数据类型进行梳理，复核两者收集的个人数据是否仅用于隐私协议中规定的指定目的，评估其是否为满足最小化原则。

阶段 3-6 传输、处理、存储、处置个人数据

遵循美的 IoT 的保护个人数据的安全可靠原则是这四个阶段的重点。首先个人数据仅通过 APP 进行收集并传输至云端，所有智能家居设备不会收集或发送用户的个人数据。在 App 端及数据中心

之间传输过程中，美的 IoT 使用 无线网络 SDK、MSmart 协议、AES 加密方法等措施保障个人数据的传输安全。存储过程中使用了多种手段保护个人数据准确、不被非法篡改及披露，如通过大数据平台发现异常账号及异常设备、严格监控输入流量、使用全平台日志记录系统、定期审计系统安全特性等。

同时美的公司建立了员工账号权限管理系统，按照角色设定其对用户个人数据的访问权限，保障其权限仅为实现个人数据收集目的的必要最小权限，避免由于员工权限过高导致的可能的数据泄露。

在美的物联网平台及美的的美居的隐私影响评估中对个人数据处理过程进行梳理，保障处理流转过程中的个人数据保护。

在到达隐私协议约定的存储时间或用户注销账户后，美的 IoT 将及时删除涉及的个人数据，以满足 GDPR 等法律法规中要求的存储时长最小的原则。

3.2. 美的 IoT 隐私安全保护技术措施

每一阶段的数据安全都至关重要，美的 IoT 引入多种安全保护技术重点保护个人数据生命周期中的收集、传输、处理、存储过程中的数据安全。

3.2.1. 家居产品侧终端安全与隐私保障

智能家居的终端产品种类繁多数量惊人，不仅包含直接与物理世界进行交互的传感器或执行器，也包含与虚拟世界通信的联网模块，由此而增加的计算功能、数据存储和网络连接等功能，提升了智能家居设备效率和技术能力，但同时也带来了新的安全风险，智能家居终端、固件及其通信协议的安全性至关重要，美的 IoT 从终端安全相关的硬件安全、固件安全、通信安全和数据安全四个方面出发，实施和管理适当的安全管控措施，降低智能家电终端遭受攻击的风险，提升用户的安全感知。

- 硬件安全

硬件作为智能家居终端设备的有形实体，其安全性毋庸置疑，美的 IoT 在芯片选型上开始把控，保证智能家居设备从芯片端开始，便工作在安全的物理环境中，从基础可信根、调试安全、运行安全、物理安全等多个角度进行安全把控，如安全启动、设备唯一 ID、真随机数、硬件加密引擎、安全存储、代码保护机制等安全功能均作为芯片的检查要点。

从整个硬件设计过程中美的智能家居设备便导入安全需求、安全评审和安全测评环节，确保从整个业务流程上出发，基于木桶原理考量，降低安全风险，做到安全可控；在每个设计环节，均设置了安全元素，在安全需求环节输出基于风险评估的安全评估报告，安全评审环节基于《美的 IoT 终端安全测评标准》输出安全评审建议，安全测评环节基于《美的 IoT 终端安全分级测评方法》输出测试报告。

- 固件安全

万物互联，作为连接物理和虚拟世界最为关键的“固件”，美的 IoT 将固件识别为威胁模型中的一项重要资产，并针对其建立机密性、完整性和可用性的安全目标至关重要，提升固件安全的防御优先级，定期更新固件并启动可用的安全功能及策略，不断提升美的 IoT 产品的“安全弹性”。

固件开发阶段，美的 IoT 遵循源代码开发规范，从源码端避免代码缺陷、危险配置、硬编码敏感信息、缓冲区溢出等高危漏洞，并定期关注国际物联网漏洞标准 OWASP IoT Top10、CVE 漏洞平台、国际代码安全漏洞平台 CWE，优化并持续更新内部编码规范。

固件检测阶段，综合分析对比业内优秀的固件自动化检测平台，基于多种开源的固件检测工具，美的 IoT 搭建了自有的固件自动化平台检测工具，包含 CWE 漏洞检测、CPU 架构分析、加密算法分析、IP&URL 查找、elf 分析、已知漏洞检测、敏感信息检测等 20+漏洞检测功能，并且可以持续优化规则，集成检测插件，美的 IoT 固件检测平台具有固件解包、固件分析和固件比较三个主要模块，均支持任务调度和插件集成，除此之外，自动化分析完成后，美的 IoT 还会进行手动的渗透化测试，确保在人机结合的前提下，最大程度降低固件风险，由此平台和人工渗透检测出的漏洞和可能存在的风险会反馈固件开发阶段，形成闭环操作，整体提升固件的安全性。

- **通信安全**

智能家居终端设备实现智能必不可少的存在通信，狭义上来讲智能家居终端设备包含内部通信和外部通信，对于这两部分通信，美的 IoT 采取相应的安全措施来保证通信安全：智能家居终端的通信模块具备唯一标识并开启安全机制，且使用 WPA2 及以上的安全机制；外部通信前，通过密钥协商建立其会话密钥，且此会话密钥在重新建立会话或意外重启时，重新协商，通信时终端设备开展传输数据完整性保护，避免遭受篡改、删除、插入等攻击；内部通信即家电主控板和联网模块之间的通信采用美的自有的安全指令协议，存在完整性校验机制且遵循保密性原则，对于美的智能家居终端设备我们要求联网模块与家电主控板之间建立绑定关系，避免遭受仿冒风险，提升安全等级。

- **数据安全**

数据安全一直是美的智能家电的深耕领域，包括且不限于数据的存储、传输以及处理等，在智能家电终端我们要求数据安全存储的同时存储期限为实现功能所必须的最短时间且不超过智能家电终端的生命周期，比如用户路由器的账户和口令信息，采用对称加密算法加密存储，且密钥长度不低于 128 位；智能家电终端进行数据的传输时，我们采用加密或非明文等安全措施，比如智能家电系统组件之间数据传输应先进行基于口令的用户身份鉴别；智能产品终端的数据处理有严格要求，如我们智能产品存在复位操作，可以一键清除用户的个人信息，确保家电回收、转售无数据泄露风险。

3.2.2. App 侧终端安全与隐私保障

- 客户端程序保护

客户端本身作为智能家居终端设备的控制和管理中心，可以连接到云端和家庭网关，通过互联网和云端服务器，实现设备远程控制、设备管理、消息反馈等功能，其安全性直接关系到家庭终端设备的安全性，很可能成为智能家居网络的风险入口。由于安卓系统自身开放性、碎片化等特点，导致安卓应用很容易被逆向，攻击者通过逆向分析 App 的安装包，可以进行代码分析，绕过安全逻辑，修改内存数据，进行动态调试，窃取用户隐私信息等。为了防护攻击者攻击客户端，确保客户端的安全性，需要对程序代码进行混淆保护，或借助安全加固技术以对抗这种攻击行为。美的的美居的 App 客户端保护采用二进制字节码级别进行加固，包括针对客户端反编译、防篡改、代码混淆、Root 环境检测、模拟器检测拦截、Hook 插件检测、界面防劫持、反调试和注入保护等。美的的美居的 App 客户端保护，包括针对客户端反编译、防篡改、VMP（虚拟化指令技术）、代码混淆、Root 环境检测、模拟器检测拦截、Hook 插件检测、界面防劫持、反调试和注入保护等。

- 通信安全

App 到云端、设备端通信全程采用 TLS 加密，保障数据传输安全。并且 App 中启用了证书校验机制，有效防止第三方劫持攻击，降低数据泄露的可能性。

App 到云端、设备端通信敏感数据使用 AES 加密算法进行加密，加密密钥是基于每个用户 ID 在服务器动态生成的唯一动态密钥，有效保障了用户网络的安全，减小降低数据泄露的可能性。

- 组件安全

Android 组件包括：Activities(活动)、Services(服务)、Content(内容)、Intents(意图)、Broadcast Receivers(广播接收器)、Notifications(通知)，通过严格限制组件的使用和访问权限、严格的权限和输入校验，保持 SDK 较高版本，第一时间进行更新和漏洞修复，确保 App 的组件安全。

- 数据安全

美的的美居客户端针对存放在客户端本地的数据安全进行严格的保护。

内存数据：重要操作时，采用虚拟化技术进行用户数据保护。

数据存储：本地配置文件全程采用加密方式保存。**APK** 读写本地数据库全程采用透明加密，本地数据库不会存储任何个人敏感信息。

密钥数据：采用自主研发的密钥分存技术保护密钥，严令禁止密钥硬编码于代码中。

日志安全：正式的客户端不打印和存放任何 **logcat**、日志文件与个人信息。

3.2.3. 云端安全保障

- 物理安全

美的 IoT 一直致力于为每一个智能家居用户提供安全、稳定、可靠的物理基础设施。美的物联网平台遵循相关国际标准与国内外监管法律法规，建立适用于智能家电业务场景的全方位安全管理体系，将安全管理的理念充分融入到日常管理和维护中，来保证数据中心的物理安全。

- 高可用基础设施安全

美的 IoT 使用全球知名的云主机服务商 AWS、阿里云、微软云、腾讯云等，为客户提供更加安全可靠、稳定持续的物理设施基础。

美的 IoT 使用阿里云、AWS 自带的容灾备份机制保证数据的安全性，国内部署覆盖在杭州、上海等地区，海外则部署于美国、欧洲等地区，并灵活将数据和系统部署于不同的数据中心进行容灾备份。

- 网络安全

- 网络安全技术

美的 IoT 云拥有成熟完善的网络安全防护技术，包含防火墙、WEB 应用防火墙、DDoS 防护、漏洞扫描、主机安全防护、操作日志审计、堡垒机、身份认证鉴权、网络隔离、API 访问控制、黑产情报识别、大数据风控等机制，可有效地应对来自互联网的各种风险威胁，针对不同的威胁和攻击进行有效防范。通过负载均衡对 TLS 加密传输进行解密，多层高级边界防护机制可对 API 网关流量进行监控，对攻击执行阻断。在高级边界防护的基础上，API 网关作为云服务特有的安全边界提供多种防护措施：

(1) 防火墙：通过防火墙配置 ACL，限制外部恶意入侵；

(2) WEB 应用防火墙：通过 Web 应用防火墙等设备进行恶意入侵阻断。

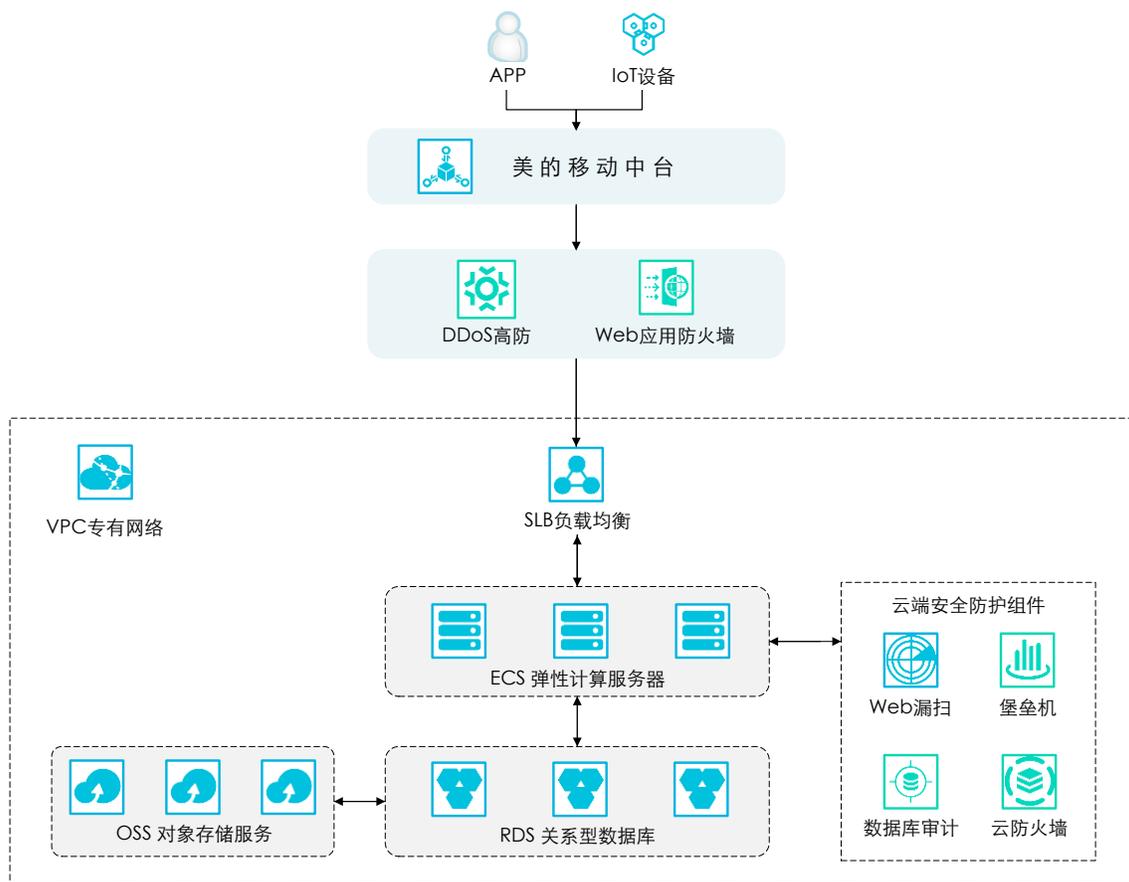
(3) 主机监控：部署 WebShell 检测模块，实时检测引擎，实时检测、删除和上报 WebShell。部署主机登录异常检测，可识别非堡垒机方式登录操作。安全红线检测，可识别机器是否按照安全红线配置上线。主机漏洞检测，可识别主机在应用层和系统层面的漏洞，并提醒安全人员及时进行漏洞修复。

(4) 入侵检测 IDS：通过对所有云服务器实例、应用、网络等进行实时的日志审计和分析，能够快速识别安全风险，告知安全团队。通过调用第三方威胁情报接口，如果涉及异常的 IP 地址、域名地址等威胁情报信息，则自动化进行防火墙和 WAF 的阻断。

(5) 入侵防护 IPS：通过 WAF 和防火墙等设备进行外部入侵进行阻断。

(6) 数据库审计：针对数据库的登录、增删改查、退出等操作进行完备的日志审计，并对数据库访问权限进行严格管理和限制，有效防止数据库的非法访问情况发生，并使数据库操作行为可溯源。

(7) 病毒查杀：可对从所有接口上传而来的文件进行自动化检测，并定期检查服务器中文件的安全性，包括是否存在病毒，具有风险的可执行文件等。



- 网络冗余

美的物联网平台依托阿里云构建了高可用的灾备能力，能够最大化地减小非人为因素导致的网络故障的业务影响。

通过冗余的网络建设方式，同时在同城也采用了多区域的机房部署，能够实现网络的便捷性和基于流量负荷的工程调度，确保网络服务不会因为单点故障而中断，实现同城容灾。

- 数据通信安全

美的 IoT 云端与 App 端通信使用 HTTPS 加密传输协议和证书安全校验机制，降低通信过程中数据遭受中间人攻击的风险。鉴权签名数据在通信传输过程中均额外使用安全的 HMAC-SHA256 签名算法，保证信息传输的完整性。

设备端与云端的数据交互则采用美的 IoT 自研 SST 私有加密协议，在数据传输过程中对用户数据进行加密，确保用户数据在设备与云端间通讯过程中不会遭受中间人劫持以及篡改。

- 网络隔离与访问控制

美的 IoT 内部实施严格完善的网络隔离规则与制度，可确保非授权人员无法访问美的 IoT 内部网络的任何资源。员工在进行日常生产网络运维工作时，需经过堡垒机的严格审批和权限控制，方可访问使用授权之内的资源与功能。

云端用户如需访问云服务，需经过云服务内部的私有网络身份验证、会话 ID 校验以及安全 token 鉴权等安全机制，并使用受限制的权限登录生产系统，确保用户只能合法访问相关数据，不会越权访问其他数据，实现用户之间的访问隔离，且用户在登录后所进行的操作均有日志审计，并可对操作日志进行溯源审查。

美的 IoT 在部署网络应用时，将正式生产环境与测试环境分隔开，分开网段进行部署与隔离，开发测试在测试环境开展，开发测试不影响生产环境的稳定性，可有效避免因测试环境被入侵而影响正式环境的安全性。

- API 接口安全

美的物联网平台所有业务 API 接口均不对外公开，APP 请求接口均通过移动中台进行转发，而美的 IoT 的各项服务均可通过移动中台依据 API 的功能不同而实施不同的安全策略，如对敏感 API 的日志进行数据风控，限制接口的访问次数，识别非法访问动作，设立黑白名单机制限制非法访问等措施，保障中台接口访问的安全性。移动中台可通过管理平台进行配置，对外发布的 API 进行管理和审计。

- 身份认证和鉴权

美的 IoT 应用服务接口访问的对外开放，对每一个 API 请求都进行身份验证，确保身份验证通过的请求才能访问云端信息以及请求云端服务，并且传输通道使用 HTTPS 协议进行加密处理。身份验证方式使用令牌（token）认证，来自美的美居的认证请求均需包含一个认证的 token，该 token 由用户登陆时从中台生成，且具有随机性、时效性。

3.2.4. 业务安全与风控



构建智能产品风控大脑，利用应用大数据、机器学习、人工智能方式，识别智能场景各业务潜在攻击风险。

IoT严格遵循ISO 27001推荐的PDCA质量管理循环进行管理，通过风控平台践行监控（Check）和处理（ACT），实时监控帐号和设备异常数据，并及时进行跟踪整改，持续提升隐私保护能力。业务风控是基于业务场景，结合IP画像、手机、账户画像、家电状态指纹、用户行为等多维度信息识别潜在攻击风险，有效识别和解决家电设备接入、设备绑定、云云对接、营销活动等场景安全威胁与作弊问题。

业务风控是云服务体系的基础，所以针对账号的注册、登录、密码找回、多设备登录、设备控制等进行严格的安全管控和日志审计。同时，针对账号体系的数据存储、查询和修改进行强力保护。针对撞库、API滥用等常见账号风险来源开展策略保护。目前在所有登录、重置密码等登录相关的接口，全都使用滑动式的验证码，保障了业务人机识别的能力，防止恶意注册、撞库等攻击行为。

风控平台也会对设备，即智能产品的上线、运行及绑定情况进行监控，并通过预设的安全规则对异常的设备访问、连接进行分析，快速发现潜在的设备安全风险，从初期掐断可能存在的安全风险。

所有业务风控的异常数据、安全告警事件都会进行跟踪与闭环。

3.2.5. 个人数据安全保护技术

数据访问控制和身份认证技术：访问个人数据的权限控制按照最小化原则，根据不同职位职责定义并管理不同访问权限，员工仅拥有职位所需的最低权限，并在不需要时立即删除。同时，制定严格的密码策略和运维管理办法，对访问个人数据的权限进行严格控制。

加密技术：对客户个人数据进行加密存储和传输，确保个人数据存储和传输中的安全。

日志记录和审计技术：美的物联网平台会记录每个人对关键系统的访问、操作和查询日志，定时对日志进行监控和审计，及时发现和纠正隐私保护方面可能存在的不合规行为；同时分析潜在的隐私保护和个人数据安全隐患，以便及时迅速做出反馈，解决问题。

统一身份认证服务：统一身份认证服务（C4A）为用户提供统一身份认证服务，包括美的电商、IoT 等美的服务。

影子虚拟设备：保证了设备授权信息被盗取后不影响原有设备的正常使用，同时使用设备匿名化技术保障用户隐私安全。

通道加密：App 端到云端，全链路 TLS1.2 数据加密传输协议。设备端到云端，全程使用美的自研的 MSmart 协议。

4. 美的在隐私安全领域获得的认证

美的 IoT 在遵循全球数据安全及隐私保护法规的前提下，持续提升自身的隐私保护能力，致力将美的 IoT 打造成消费者信赖、行业认可的隐私安全标杆品牌。为确保信息安全与隐私保护策略的贯彻执行，美的 IoT 在 2019 年正式成立隐私保护办公室，通过流程制度、技术防护、审查和评估机制等建立完善的安全管理体系。同时，美的聘请全球知名律师事务所和咨询机构作为数据合规供应商，确保美的符合各国法律合规要求。为向用户提供符合适用法律法规及行业领先的业务运行环境及服务，美的 IoT 已开展全球化数据合规治理工作，并接受外部监管机构的定期评估和审查。

截至目前，美的 IoT 已经具有较为成熟的数据安全及隐私保护管理制度，以及相对应的隐私保护能力，并通过了全球多个广受认可的信息安全与隐私合规领域的认证。美的 IoT 承诺，将持续进行隐私安全 and 信息安全认证和合规认证，为用户数据和隐私安全保驾护航。美的已通过的认证如下：

- **ISO 27701 隐私信息管理体系认证**



ISO/IEC 27701 是在隐私保护方面对 ISO/IEC 27001 和 ISO/IEC 27002 的扩展，针对保护可能受到个人信息收集和处理影响的隐私提供了更多相关指南。设计的目的在于借助更多的要求增强现有 ISMS，以建立、实施、维护和持续改进隐私信息管理体系 (PIMS)。该标准概述了适用于个人身份信息 (PII) 控制者和 PII 处理者的框架，以有效管理隐私控制，降低个人隐私权面临的风险。这些附加要求和指南的编写，对于任何规模和文化环境的组织都具有实用性和可用性。

- **ePrivacyApp 个人数据保护技术认证**



ePrivacy 是一家全球知名的、被德国 ULD 认可的隐私认证机构，ePrivacyApp 认证是其发布的从技术维度对手机 App 端的个人数据保护能力进行评估的认证。ePrivacyApp 以欧洲各数据保护法规、安全技术标准等为基础，从 APP 登录保护、数据传输、加密、个人数据保护、主数据保护等领域提炼出超过 150 项评判标准，对美的美居的个人数据保护技术进行了包括代码检查、App 进出流量检查、黑客攻击测试等领域的检查与评估，确认美的美居从各个方面均达到了认证要求的隐私保护水平。通过该认证表面美的美居在隐私保护技术能力达到了国际领先标准。

- **ISO 27001 信息安全管理 体系认证**



ISO 27001 是由国际标准化组织发布的信息安全领域权威标准，标准指导企业从安全策略、信息安全组织、信息安全管理、人力资源、物理环境、访问控制等共 11 个领域由上而下为各类组织建立并运行信息安全管理 体系提供指引。通过该认证，证明美的 IoT 公司高度重视隐私安全的保护，建立了符合国际标准的、体系化的组织体系和安全管理制度，并将其应用于公司运营过程中，有效保护用户数据及经营信息的机密性、完整性和可用性。

- **TRUSTe 企业隐私体系认证**



TrustArc 是国际权威隐私合规评估机构，已经为全球多家知名企业提供了隐私认证服务。TRUSTe 认证整合了各国隐私法规要求，国际版美的美居此次通过认证，标志着美的 IoT 的应用系统及美的物联网平台的隐私管理、政策及实践达到了欧盟-美国及瑞士-美国隐私保护（EU-U.S. Privacy Shield and/or Swiss-U.S. Privacy Shield）的要求，在隐私保护领域达到了国际一流水平，美的 IoT 建立了全面符合 TRUSTe 标准的隐私保护体系，更好的保护消费者的个人数据。

- **PCI DSS 认证**



PCI DSS 是由 PCI 协会制定的银行卡交易数据安全标准，是目前全球最严格、保障级别最高的金融机构安全认证标准。该标准对数据的网络保护、存储保护、传输保护、物理设施保护、访问控制及信息安全政策等执行严格要求。美的 IoT 始终致力于最大程度保障数据安全，不断提升对于智能产品使用场景中的安全与隐私保护能力。通过 PCI DSS 数据安全标准，意味着美的美居、美的物联网平台等系统服务已经具备了金融级别的数据传输、存储及处理的安全保障措施，为智能产品行业的隐私保护能力提升树立了标杆。

亚太经济合作组织跨境隐私规则认证（APEC CBPR）



亚太经济合作组织跨境隐私规则系统（简称 APEC CBPR）由 APEC 经济体开发，旨在建立消费者、企业和监管机构对个人信息在 APEC 组织成员之间跨境流动的信任，从而减少全球信息流通的壁垒。美的新加坡（Midea Electric Trading (Singapore) Co. Pte. Ltd.）为海外智能家居产品用户推出的 MSmartLife 和 Toshiba HA 两款应用于 2021 年 10 月通过 APEC CBPR 认证，标志着美的对海外用户数据的安全与隐私保护体系达到国际一流水平，取得个人数据在包括美国，日本，新加坡等 9 个亚太经合组织成员之间跨境传输的许可，同时美的也是中国同行业首家获得此认证的企业。

- IT 智能家居产品安全认证



美的集团旗下国际高端科技家电品牌 COLMO 获得中国网络安全审查技术与认证中心(以下简称网安中心)颁发的 IT 产品信息安全认证证书（智能家居产品），是国内首个通过信息安全认证的智能家居产品。该标准将智能家居设备、控制端应用和智能家居应用服务平台（软件）整体作为评估对象，从智能家居设备、控制端应用、智能家居应用服务平台（软件）、通信安全及个人信息保护等方面对智能家居产品提出安全要求，覆盖了现有智能家居典型应用场景下对应的安全威胁，为智能家居产品信息安全认证工作提供了科学有效的评估依据。通过该认证，不仅标志着以 COLMO 为代表的美的集团达到智能家居产品安全标准水平，同时也将促进智慧家居行业在产品安全保障能力方面的提升。

- ETSI 303645 消费者物联网信息安全:基准要求



根据欧洲电信标准协会 2020 年发布的 ETSI EN 303645 IoT Security 标准要求，第三方国际检测认证机构 TUV 南德对美的智能家用空调，洗碗机产品、无线网络通信模组，App 与云端进行了评估和验证，结果表明美的产品在 13 个安全与 5 个隐私数据保护标准均达到 ETSI EN 303645 的要求，是全球首个通过 TUV 南德智能产品隐私保护认证的智能家居厂家。

- 移动互联网应用程序安全认证



为规范移动互联网应用程序（以下称 App）收集、使用用户信息特别是个人信息的行为，加强个人信息安全保护，根据《中华人民共和国网络安全法》《中华人民共和国认证认可条例》，认证以《信息安全技术 个人信息安全规范》作为主要依据规范开展，通过该认证意味着美的美居个人信息安全保护体系受到中国网络安全审查技术与认证中心的认可，也意味着符合国家最新个人信息保护安全标准。美的美居是同行业第一个通过该认证的智能家居 App。

- 物联网安全联盟 ioXt 认证



ioXt (internet of secure things) 联盟由制造商、行业联盟和政府机构组成，是行业领先的全球物联网设备安全和认证联盟，联盟包括谷歌、亚马逊、T-Mobile、Comcast 等在內的技术和设备制造领域巨头。ioXt 成立目的，旨在分享最佳的安全实践和建立主导型性标准，为零售商和消费者增加对

产品的信心。随着主要制造商和技术颠覆者加入 ioXt 董事会，ioXt 的会员正逐渐壮大，目前已经有 200 多家领先的 OEM、无线运营商、标准组织、合规实验室和政府组织成员、六个授权实验室作为独家测试提供商。ioXt 认证计划依照 8 项不同的 ioXt 承诺原则来评估产品的安全等级。美的 IoT 多个设备和 App 通过了实验室或自我认证的测试，ioXt 联盟将会认为此设备是符合 ioXt 安全标准且可以得到一个 ioXt SmartCert 认证标签。

- NISTIR 8259



NISTIR 8259 系列标准是美国国家标准与技术研究院（NIST）制定的面向物联网设备制造商的网络安全指南。它提供了产品上市前进行风险识别和适当的安全控制措施以及设备投放市场后如何满足客户的网络安全需求。在北美区域，NISTIR 8259 已经成为确定物联网设备安全合理性时的重要参考。经过专业认证机构认证，美的包括分体/移动空调、窗机、除湿机、洗碗机、冰箱、洗衣机、烤箱和微波炉等多个产品品类的数十种型号产品已经符合 NISTIR 8259 的安全要求。

- 物联网设备互联互通组件 EAL4+认证



美的智慧家电安全组件于 2020 年 6 月通过了中国网络安全审查技术与认证中心的评估保障级（EAL）4+认证，符合 GB/T 18336-2015 《信息技术 安全技术 信息技术安全评估准则》和 CCRC-EAL-TR-025-2020 《物联网设备互联互通组件安全技术要求（评估保障级 EAL4+级）》中的安全技术要求，这意味着美的智慧家电安全组件整体安全水平达到了国际化标准水平，其安全性是具有保证，并且值得信赖的。美的智慧家电安全组件为美的自主研发，在几乎所有的美的智慧家居产品中使用，能够为智慧家居产品提供设备配网、设备注册、设备控制、升级更新等功能以及安全存储和安全通信的能力，为用户的安全和隐私提供充分保证。

CSA STAR 云安全认证



CSA STAR 认证是由 CSA（Cloud Security Alliance，云安全联盟）和 BSI 共同发展的全球性云安全评估与认证标准，云安全、信任、保障和风险(Cloud Security Alliance Security, Trust, Assurance and Risk - CSA STAR)认证是针对云服务提供商安全等级评价的严格独立的第三方评审和注册，采用云计算安全的行业黄金框架——CCM（Cloud Control Matrix，云安全控制矩阵）。CSA STAR 认证是通过严格的第三方独立评审过程对云服务供应商安全的合格评定，属于技术中立（technology-neutral）的认证。该评估在帮助企业有效提升云计算服务安全水平、管理策略的同时，证明其安全水平领先于云服务提供者行列。CSA STAR 的认证范围包含美的云平台的开发、运维、运营和客户服务。美的作为行业首家获得这项资质的物联网云服务提供商，这将进一步巩固其在国内领先的地位。

CNAS 安全实验室资质授权



美的智能家居安全实验室通过了相关智能家居装置的安全隐私测试，成功获得了中国合格评定国家认可委员会（CNAS）的认可。获得该认可表明美的可以为智能家电及周边相关产业和生态链产品等领域提供综合的安全测试服务。

美的智能家居质量检测中心（CNAS L15572）依据国际 ISO/IEC 17025:2017 及相关认可规则的要求建立和实施管理体系以及检测过程，具备提供准确和可靠的测试能力，覆盖能力范围包含智能家居设备端安全、控制端安全、服务端安全、通信安全、个人信息保护等。

此次获得 CNAS 认可，表明着美的智能家居安全实验室的技术和管理达到国际认可水平；未来美的 IoT 将与更多海外认证机构或实验室进行多边合作并加强与各界交流，为消费者与生态行业打造安全与可靠的智慧生活。

ISO37301 合规管理体系认证



2021年4月13日，国际标准化组织 ISO 发布并实施了《ISO37301:2021 合规管理体系 要求及合规指南》，该指南是 ISO19600:2014 的升级版，规定了企业建立、运行、维护和改进合规管理体系的各项要求，企业可贯彻执行该标准提升合规管理。本次认证 BSI 从策划-执行-检查-改进四步骤，完整覆盖了美的合规管理体系建设、运行、维护和改进的全流程，充分认证了美的的合规管理能力和美的的合规管理体系及合规三级管理架构的运行有效性。

5. 结语

美的 IoT 始终践行美的公司“为人类创造美好生活”的愿景，致力于让每个人和家庭都享受到智能家居带来的美好生活。在为用户提供便利、愉悦、健康、安全的智能产品的同时，保障用户隐私安全也是美的 IoT 公司至关重要的使命。

为此，美的 IoT 将密切关注各个国家隐私保护领域发布的法律法规，采用先进科技，开展行业最佳实践，不断优化自身的管理能力与技术，为用户提供更便捷、更安全、更可信赖的智能产品。