Prepared and Administered by Tuya Compliance Team

涂鸦遵从日本 APPI 白皮书

2024 年 10 月

T u y a I n c .

Classified as Limited Access and Copyrighted
版权所有 未经允许 不得抄印

目录

前言

本文向我们的客户介绍有关日本个人信息保护法（Act on the Protection of Personal Information，以下简称 APPI 或该法案）的信息以及涂鸦如何利用业界领先的数据隐私和安全功能来存储、处理、维护和保护客户数据。我们致力于与客户合作，利用涂鸦的合规能力帮助客户遵从 APPI。我们解释了我们的数据保护功能、它们如何满足 APPI 的要求，以及我们如何与客户分担合规责任。本文将重点讨论放置在涂鸦平台中的客户的最终用户的个人信息，对于客户直接向涂鸦平台作为服务提供商提供的个人信息，请参阅我们的隐私声明。

本白皮书仅供参考。它不是法律建议，不应被视为法律建议。由于每个客户的要求各不相同，Tuya 强烈建议客户就其隐私和数据保护要求咨询法律专家。

1. 日本个人信息保护法概述

日本的《个人信息保护法》（APPI）于 2003 年首次通过，此后多次修订。最近一次更新是 2021 年 6 月，并于 2022 年 4 月 1 日生效。日本政府于 2016 年成立了个人信息保护委员会 (PPC)，作为 APPI 的主要监管机构，负责监督 APPI 的遵守情况。

APPI 适用于在日本提供商品或服务并处理日本居民个人信息的企业经营者。与欧盟 GDPR 不同，APPI 并未严格区别数据控制者和数据处理者，APPI 适用于处理个人信息数据库的所有企业经营者。

如需了解更多 APPI 信息，可访问其官方网站 https://www.ppc.go.jp/en/legal/

2. 涂鸦数据保护和责任共担模型

涂鸦强大的安全和隐私控制措施，使客户能够放心地使用涂鸦平台，以符合日本《个人信息保护法》(APPI)的要求。此外，我们始终致力于不断提升隐私和安全能力，帮助客户实现合规。

2.1. 隐私保护认证和审计

截止目前，涂鸦已经获得众多全球性或行业特定的安全合规权威认证，全力保障客户部署业务的安全与合规。涂鸦行业领先的第三方审计和认证有助于支持 APPI 合规性并满足行业隐私标准。查看证书和审计报告。

认证/鉴证	描述
CCPA 验证性报告	《加利福尼亚消费者隐私法案》（CCPA）是保护加州居民个人信息的法律，涂鸦已完成 CCPA 合规审核。
GDPR 验证性报告	欧盟通用数据保护条例 (GDPR) 旨在保护欧盟数据主体的基本隐私权和个人数据安全，全方位提高了个人数据隐私保护的标准。涂鸦已完成 GDPR 验证并优化内部数据安全保护和合规要求。
ISO/IEC 27001:2022	国际信息安全管理体系认证标准，以风险管理为核心，确保信息安全管理体系持续有效运行。
ISO/IEC 27017:2015	针对云计算信息安全的国际认证，提供云服务供应商安全控制实施指导。
ISO/IEC 27701:2019	针对隐私信息管理体系的国际权威认证，涂鸦通过此认证表明其在个人数据保护具有健全体制。
CSA STAR	CSA STAR 是国际云安全水平的权威认证，旨在解决云安全问题，帮助云计算服务商展示其服务成熟度。
ISO 9001:2015	ISO 9001 是一个保证公司产品质量及运作的指导性纲领和规范架构，确保满足客户及相关法律规要求。
SOC 2 Type II & SOC 3	SOC 审计报告是由独立第三方根据美国注册会计师协会（AICPA）准则出具的审计报告，SOC2 报告的目的是评估与安全性、可用性、完整性、机密性和隐私相关的组织信息系统。

2.2. 涂鸦安全合规战略

涂鸦作为一家专注于 AI+IoT 的技术型科技公司，从上至下非常重视安全合规问题。涂鸦的安全合规战略涵盖技术和管理措施，旨在确保其产品和服务尽可能满足各地区的安全和合规标准及要求。

安全合规团队

涂鸦拥有专业的安全合规团队，致力于涂鸦云平台的安全质量保障、安全评估和安全运维工作。在隐私合规方面，涂鸦与外聘的专业隐私保护机构紧密合作，同时有网络安全与隐私保护全球性律师事务所为涂鸦提供专业咨询服务。合规团队与法务团队密切协作，确保涂鸦产品和服务获得更严格的保障。

安全风险管理

涂鸦的安全团队负责漏洞管理和挖掘，能够发现、跟踪、追溯和修复安全漏洞。在业务代码上线前，他们进行安全渗透测试，并定期对线上业务进行黑盒测试。每年，涂鸦与第三方安全机构合作，对云服务、移动客户端、硬件产品及公司 IT 基础设施进行渗透测试。涂鸦支持外部白帽子通过涂鸦 SRC（https://src.tuya.com/）或安全邮箱提交漏洞，并对优质高危漏洞提供最高 10 万美元的奖金。

访问控制

涂鸦对 IT 系统的系统权限、服务器权限、数据权限等进行统一管理，实现零信任权限管理模型，基于用户身份、应用身份、应用功能类型实现极简权限管控。

对于内部系统的身份认证，涂鸦为所有内部应用实现了单点登录（SSO），同时，SSO 实现了 OTP 的能力，除了满足所有密码管理需求外，还增加了每次登录的动态密码验证能力。

涂鸦对内部系统的访问权限验证有统一的权限管理体系（ACL），遵循“最小权限原则”和“知必所需原则”，实现对应用、应用功能、数据的授权，平台有完善的审批流程管理。

对于客户数据访问，涂鸦设置了严格的组织和技术控制措施，确保只有在客户授权情况下，才能访问客户数据，且每次访问都有流程审批和日志记录。

供应商安全

涂鸦针对平台软件供应商制定了筛选机制和定期评估机制，除了硬件产品的安全指标、软件服务的安全标准外，涂鸦还需要深入了解各类服务商在信息安全评估、隐私合规等方面的实践。信息安全评估涉及安全渗透测试、供应商安全能力评估等。

安全意识与培训

为增强全员网络安全意识，涂鸦智能发布了《涂鸦智能员工信息安全手册》，并定期对员工进行网络安全意识教育和隐私保护培训，要求全体员工持续学习网络安全知识，理解手册中的政策和制度，牢记哪些行为是可以接受的，哪些行为是不可以接受的，意识到要对自己的行为负责，并承诺按要求行事。

2.3. 责任共担模型

使用涂鸦平台构建物联网应用会在客户和涂鸦之间建立责任共担的合作模式，因为双方在安全运营和管理中都扮演着重要的角色。涂鸦负责保障各个组件的安全，从软件 SDK、APP、云平台到涂鸦芯片模组安全。客户则需管理其自有的软件、硬件和 App（若有），并对其安全性与合规性负责。同时客户应妥善保管涂鸦平台账号和密码，依据自己公司的安全策略合理配置应用功能和安全配置。

客户和涂鸦应共同合作，以确保开展业务的安全性和合规性。如果发现任何安全漏洞或合规问题，客户和涂鸦应立即通知对方，并共同协作解决问题。

客户和涂鸦在共享责任模型中的各自角色如图 1 所示：

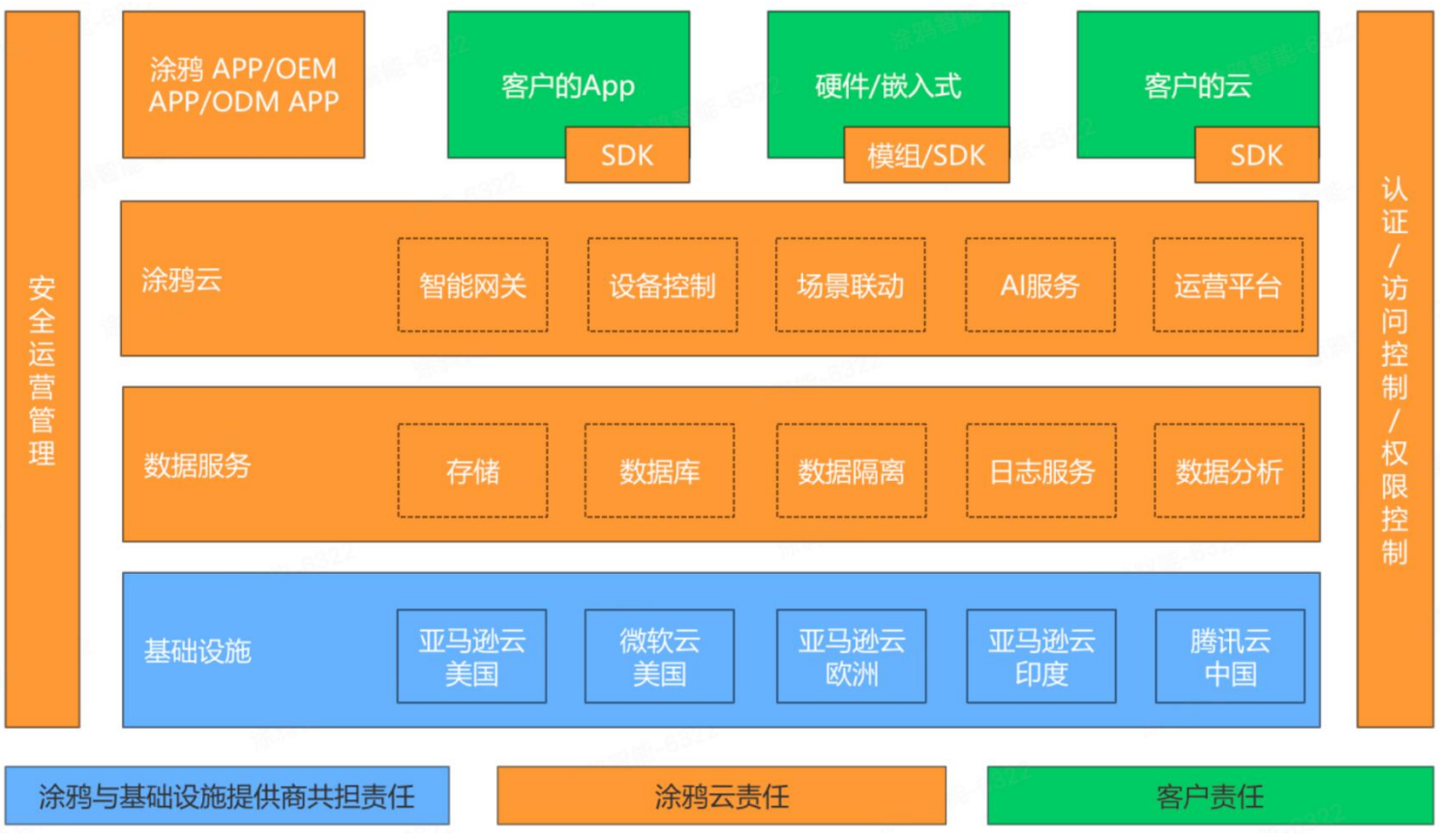

图 1 - 涂鸦责任共担模型

3. 客户掌控数据权

数据是客户的数据，而不是涂鸦的数据。我们仅根据与客户签定的协议处理其数据。涂鸦为客户提供了控制和访问其数据的能力，同时也为客户提供了安全配置的能力，以帮助客户符合其组织的一贯安全策略。涂鸦平台上存储和管理的客户数据仅用于根据合同为客户提供服务，不得用于其他目的。客户使用涂鸦服务的过程中，拥有对其内容数据的全面控制权。

3.1. 客户可以决定内容数据存储的区域

涂鸦目前在全球多个区域包括欧洲、美洲、亚洲等拥有数据中心，每个区域的数据中心物理隔离，如客户对地域位置有特殊需求，可按照不同的需求选择不同区域，例如客户可以在涂鸦平台构建自己的 App 时，选择数据存储的区域。没有获得客户的明确同意或者其他法律义务要求时，涂鸦不会将客户的内容数据转移到其他区域。凭借涂鸦数据处理协议和标准合同条款，欧洲客户可以合规的开展其全球业务。

涂鸦目前在全球多个区域包括欧洲、美洲、亚洲等拥有数据中心，每个区域的数据中心物理隔离，客户在涂鸦平台构建自己的 App 时，可以自主选择数据存储的区域。没有获得客户的明确同意或者其他法律义务要求时，涂鸦不会将客户的内容数据转移到其他区域。凭借涂鸦数据处理协议和标准合同条款，欧洲客户可以合规的开展其全球业务。

图 2 - 涂鸦全球数据中心

3.2. 客户可以决定其内容数据保护的策略

客户通过涂鸦平台的安全设置，可以决定其是否开启多因素认证、使用何种用户密码策略、自定义会话时长等。客户可以随时要求涂鸦删除其数据，或者导出其数据。客户应考虑如何管理和保护个人数据安全，保管好其涂鸦平台账号和密码，防止出现个人数据泄露，如有泄露事件，应依据相应的法律法规及时通知监管部门和受影响的数据主体。

3.3. 客户决定谁能访问其数据

涂鸦非常重视您的隐私，客户可以控制谁可以访问数据。涂鸦对涂鸦平台如何处理客户上传的用户数据保持透明，并且客户可以随时访问、删除其数据，也可随时配置其数据访问策略。除非客户明确授权，否则涂鸦不会访问客户的任何数据，涂鸦承诺不会将客户数据用于合同约定和隐私政策声明以外的其他目的。

3.4. 政府访问请求

涂鸦必须遵守运营所在国家（包括日本）的法律。执行机构通常会向其调查对象发出数据请求，很少会向处理其调查对象 PII 的云平台提供商发出请求。涂鸦处理政府请求时会仔细审查，以确保其合法、可执行且范围正确。不合法的请求将被拒绝。

4. 涂鸦如何遵从日本 APPI 要求

我们在下面的表格中总结了 APPI 对数据保护的要求。同时，我们还讨论了与这些要求相关的Tuya实践。

数据保护要求	涂鸦如何支持 APPI 的要求
通知和同意 PIC 必须告知个人收集其个人信息的目的，并在获取主体的敏感信息之前，取得个人的同意。	**客户关注点：** 客户对其数据拥有全面的控制权，扮演着数据控制者的角色，应确保个人数据收集基于合法、具体、明确的目的，告知数据主体并获取数据主体的同意。客户在收集和处理儿童的个人数据时，应告知其父母或法定监护人并获取明确的同意。客户可使用涂鸦产品和服务提供的功能或自身构建的能力，更好地践行通知与选择同意、撤回同意等要求。 **涂鸦做法：** 涂鸦针对个人数据的使用开发了不同层级的同意机制:积极选择加入机制。 ✓ 涉及营销解决方案和个性化的数据处理活动的积极选择机制; ✓ 一旦客户做出决定，同意将被技术记录; ✓ 用户很容易撤回同意，并且撤回同意的方法已经定义。 涂鸦在产品和服务开发阶段，以 Privacy by Design 为核心原则，帮助客户设计了多样的选择同意功能，且仅在功能使用时，才会申请对应权限或个人数据，并且如果收集的是敏感个人数据，会单独获得用户的同意，确保客户及涂鸦业务的合法合规。
目的限制 未经个人明确同意，PIC 不得超出目的范围进行处理个人信息。	**客户关注点：** 客户对其最终用户的个人数据拥有全面的控制权，可自主决定是否使用涂鸦服务来收集和使用其用户的个人数据，应确保个人数据的收集、使用或披露仅限于已声明的合法、具体、明确的目的。 客户应确保数据处理的目的与告知数据主体的目的一致。 **涂鸦做法：** 涂鸦仅出于合同约定和隐私政策声明中限定的目的处理客户个人数据，不会将您的数据用于任何其他产品或提供广告服务。
准确度 PIC 必须尽力保证收集的个人信息准确且最新。	**客户关注点：** 确保个人信息准确且最新 **涂鸦做法：** 涂鸦不参与维护客户个人信息的准确性，不过涂鸦会确保放置在我们服务中的数据的完整性。
数据传输 PIC 获取个人同意后，才可将其个人信息传输至外国的第三方，以下情形除外： ● 数据传输到欧盟或英国；或者 ● 接收方实施与 APPI 同等的标准；或者 ● 接收方获得 APEC CBPR 体系认证。	**客户关注点：** 作为数据控制者，应建立数据跨境传输评估机制，充分了解数据跨境法规要求，选择合适的数据存储方案，并以透明的方式告知个人用户有关国际数据传输的情况，例如在隐私声明中。将个人数据传输至日本国外第三方前应先取得个人同意。 **涂鸦做法：** 现阶段，日本的数据默认存储在涂鸦美国 AWS 数据中心；涂鸦提供了明确的指导，说明我们的数据中心部署在哪里。涂鸦也为客户提供了自主选择数据中心的机制，客户可合理选择对应的数据中心，以确保数据传输合规。无论您选择涂鸦哪个数据中心，安全和隐私保障策略是一致的，是完全有保障的。
数据保留 一旦使用目的已实现，必须立即删除相关个人信息。	**客户关注点：** 明确业务处理活动中个人数据的留存期限，一旦目的已实现或个人提出要求，就删除个人信息。 **涂鸦做法：** 客户可以在任何时候选择删除他们的涂鸦云上的数据。涂鸦将根据合同约定保留、返还、销毁或删除客户数据。如果客户删除其数据，涂鸦承诺在 7 天内将其从我们的系统中删除。
数据泄露通知 ● 发生数据泄露时，PIC 必须在 3-5 天内通知 PPC（通过填写在线表格的方式）和受影响的数据主体。 ● 如果 PIC 将个人信息委托给数据处理者，而数据处理者遭遇数据泄露，则 PIC 和数据处理者都有义务报告泄露事件。 ● 无论是个人通知还是一般通知，都应使用日语。	**客户关注点：** 维护个人数据泄露事件响应应急制度和流程，定期开展培训和演练。与处理者建立顺畅的沟通渠道，以及时接收可能的安全事件。 **涂鸦做法：** 涂鸦制定了《事件和数据泄露响应计划》，对数据泄露事件进行补救并通知数据数据控制者。涂鸦承诺在意识到事件发生后立即通知数据控制者。
数据处理协议（DPA） PIC 必须对受委托处理个人数据的任何第三方进行必要和适当	**客户关注点：**

的监督。此类监督措施包括 PIC 与服务提供商之间签订协议，规定服务提供商应采取的适当安全措施，以及 PIC 有权就服务提供商受托处理个人数据的情况对其进行指示和调查。	与数据处理者签定数据处理协议，对处理者作出明确书面指示。 **涂鸦做法：** 涂鸦作为数据处理者，在数据处理之前与数据控制者（客户）签署数据处理协议，严格按照协议开展数据处理。
数据主体权利 APPI 赋予了数据主体知情权、访问权、更正权、删除权和选择退出权。	**客户关注点：** 客户对其数据拥有全面的控制权，扮演数据控制者角色。客户应建立个人权利响应流程，并通过隐私政策等方式公开个人行使权利的渠道，以响应数据主体权利。 **涂鸦做法：** 涂鸦制定了《隐私权个人权利处理程序》，细化了数据主体权利执行的内部流程。 针对客户的个人数据：涂鸦保障客户行使其作为数据主体访问和更正其个人数据的权利。涂鸦提供专门的渠道（参见涂鸦隐私政策）接收和响应客户的相关请求和诉求。 针对最终用户的个人数据：涂鸦帮助客户提供了最终用户（数据主体）能够访问、更正、删除、导出数据的功能。涂鸦协助客户响应个人请求。
数据安全 PIC 必须实施安全控制来保护他们处理的个人信息。	**客户关注点：** 客户对其数据拥有全面控制权，应制定和实施足够的个人数据保护策略以保护个人数据安全。根据业务和个人数据保护的需求进行安全配置工作，例如设置恰当的访问控制策略和密码策略。 **涂鸦做法：** 涂鸦对个人数据生命周期做了全面保护： a. 在数据采集阶段做了最小化处理和严格的账号认证机制； b. 在传输阶段做了传输通道和内容双重加密； c. 在存储阶段对个人数据做了 AES 256 加密，每个用户密钥均不相同，高敏感数据采用不可逆算法进行保护，同时通过密钥管理系统（KMS）统一保护密钥，并通过 KMS 进行管理和分发；对于图像或视频等敏感数据，涂鸦将根据特定用户和特定设备生成唯一密钥来加密数据； d. 在使用阶段对个人进行逻辑隔离；在展示阶段做了脱敏处理； e. 在销毁阶段，所有个人数据将被自动进行零值覆盖。 涂鸦提供了详细的信息，客户可以通过以下链接了解我们的安全实践： ● 我们的安全与隐私保护认证资质 ● 我们的安全合规白皮书

5. 关键定义

个人信息控制者（PIC）：使用个人信息数据库进行业务运营的经营者。有时也表示为“处理个人信息的经营者”。

个人信息：有关在日本生活的个人的信息，可根据该信息确定个人身份（包括可通过简单参考或与其他信息结合而识别身份的信息）；“个人信息”包括“个人识别码”，其中包括字符、数字、符号和/或其他计算机使用的代码，代表某些特定的个人身体特征（例如 DNA 序列、面部外观、指纹和掌纹），足以识别特定个人，以及某些识别号码，例如护照、驾驶执照和居民卡上的识别号码，以及“我的号码”个人社会保障 ID 号码。

敏感个人信息： 是指有关可识别个人的种族、信仰、社会地位、病史、犯罪记录、遭受犯罪损害的事实或其他识别信息，或政令规定的同等信息。

6. 总结

涂鸦致力于为客户提供一致、可靠、安全和符合法规要求的 IoT 接入服务，切实地保障客户及其用户的数据的可用性、机密性和完整性。涂鸦承诺以数据保护为核心，以云安全能力为基石，依托涂鸦独有的物联网解决方案，打造业界领先的竞争力，构建完善的云平台安全保障体系，并一以贯之地将信息安全保障作为涂鸦云的重要发展战略之一。

为实现各地区开展的业务符合当地隐私保护法规的要求，涂鸦持续洞察相关法律法规的更新，并将法规的新要求转换为涂鸦内部的规定，优化内部流程，以保证涂鸦开展的各类活动满足法律法规的要求。涂鸦根据更新的法律法规要求不断发展和持续推出隐私保护相关的服务和方案，帮助客户满足的隐私保护法律法规的新要求。

遵循隐私保护法律法规的要求是一项长期和多方位的活动，涂鸦愿意在未来持续提升能力，满足相关法律法规的要求，为客户构建安全、可信的云平台。

涂鸦客户需要评估其个人数据处理方式，并确定 APPI 的要求是否适用于他们。我们建议您咨询法律专家，以获取有关适用于贵组织的 APPI 具体要求的指导，因为本文不构成法律建议。