涂鸦遵从澳大利亚 Privacy Act 白皮书

2024 年 7 月

Tuya Inc.

目录

前言

本文向我们的客户介绍有关澳大利亚隐私法（Australian Privacy Act 1988(Cth)，以下简称 Privacy Act）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 Privacy Act。我们解释了我们的数据保护功能、它们如何满足 Privacy Act 的要求，以及我们如何与客户分担合规责任。本文提供的信息适用于涂鸦所有产品和服务。

1. 隐私法和澳大利亚隐私原则

1.1. 澳大利亚《隐私法》概述

澳大利亚 1988 年隐私法是保护个人信息的主要立法。它含盖了联邦公共部门和私营部门对个人信息的收集、使用、存储和披露相关要求。《隐私法》于 2022 年 12 月进行了修订。这些修订提高了《隐私法》规定的最高处罚，并赋予澳大利亚信息专员办公室更强的执法和信息共享权力。

《隐私法》规定了 13 项澳大利亚隐私原则 (APPs)。这些 APP 适用于年营业额达 300 万澳元或以上的政府机构和私营部门组织。《澳大利亚隐私原则》（APPs）是基于原则的，它们在保护隐私的同时，不会给机构和组织带来僵化的规定负担。这些隐私原则：

- 涉及个人信息处理的各个阶段，制定个人信息收集、使用、披露、质量和安全的标准
- 为受《隐私法》约束的机构和组织规定访问和更正个人信息的义务。

澳大利亚信息专员办公室（OAIC）负责调查违反《澳大利亚隐私原则》（APPs）的行为。OAIC 的权力包括：

- 接受可执行的承诺
- 对严重或屡次侵犯隐私的行为寻求民事处罚
- 对澳大利亚政府机构和企业的隐私表现进行评估。

欲了解更多关于 Privacy Act 的详细信息，可以访问官方网站：Privacy Act 官网。客户有责任确保他们遵守《隐私法》（包括《澳大利亚隐私原则》）规定的义务

1.2. 隐私保护认证和审计 Privacy Protection Certifications and Audits

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、文档和法律承诺有助于支持 Privacy Act 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 认证由 BSI 和 CSA 联合推出，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 是一个系统性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 审计报告是由第三方根据美国注册会计师协会（AICPA）准则出具的独立审计报告，它旨在检查服务组织提供的服务，以便最终用户能够评估和解决与外包服务相关的风险。涂鸦通过 SOC 2 审计，获得了 SOC 2 和 SOC 3 报告，展示其关键合规性控制措施。

1.3. 责任共担模型

涂鸦对其提供的软件 SDK、APP、模组和云平台上的服务和数据交互进行安全管理和运营，并对其云服务平台和基础架构的安全性承担相应责任。

客户在使用涂鸦提供的服务时，应自行开发、管理和维护其接入涂鸦云的 App 或硬件嵌入式软件（包括使用 SDK），并保证其应用及数据的安全性和合规性，包括硬件和 App 的安全合规。客户应对其开发的应用程序的安全性负全部责任，并应采取适当的安全措施，以保护其应用程序和数据不受未经授权的访问、使用、泄露、破坏或干扰。

涂鸦将向客户提供必要的技术支持和安全指导，以帮助客户保障其应用程序和数据的安全性和合规性。然而，客户应自行负责其应用程序和数据的最终安全性和合规性，涂鸦不承担任何由此产生的损失或责任。

客户和涂鸦应共同合作，以确保涂鸦提供的服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。

下图为基础云服务商、涂鸦以及客户信息安全责任共同承担责任模型：

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，该团队成员曾就职于阿里、蚂蚁金服、百度等互联网公司和传统安全厂商绿盟科技、启明星辰、安恒等，支持 Tuya 云的安全质量保障、安全评估和安全运维工作。同时该团队在隐私安全合规层面，有外聘的专业隐私安全合作机构，以及专注于网络安全和隐私保护全球性、地域性律师事务所提供专业咨询服务。合规团队与涂鸦法务团队密切合作，确保对涂鸦产品与服务的安全性与可靠性有更精细、更可靠的控制。

安全风险评估与管理

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。

1) 认证、授权、审计

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。

3) 应用程序访问控制

涂鸦对各个应用及应用间调用实现权限的统一管控。涂鸦内部应用的服务访问需要使用统一的客户端组件，通过该组件实现用户身份的相互识别和权限的控制。应用鉴权通过统一的鉴权服务实现。

4) 数据库访问控制

涂鸦的数据库权限管理主要包括：应用账号、数据库平台账号等。应用账号是指为应用提供访问数据库的账号，通过识别应用所在服务器实现身份认证。

数据库平台使用的账户由 DBA 专门创建，包括执行工单的读写权限和查询模块使用的只读账户，数据库平台账户每 3 个月轮换一次。

供应商安全

1) 服务供应商风险评估

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。

2) 服务供应商的监控

实时监控服务质量，关注第三方安全管理等，当出现异常时涂鸦能够快速响应。

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，意识到即使没有主观意图也要对自己的行为负责，并承诺按要求行事。

3. 客户掌控其数据

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：

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，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。

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与隐私保护配置，使用不同的涂鸦服务，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。客户应考虑如何管理和保护个人数据安全, 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澳大利亚信息专员办公室 (OAIC) 。

客户可以决定涂鸦能否访问其数据

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。

政府访问权

如果涂鸦收到政府索要客户数据的请求，涂鸦的政策是告知政府直接向客户索要这些数据。我们有一个专业的团队根据涂鸦的政策和法律审查和评估我们收到的每一项请求。我们承诺不会向任何政府机构提供“后门”访问权限，也不会允许任何政府机构非法访问您的数据。

4. 涂鸦如何遵从澳大利亚 Privacy Act 的要求

4.1. 涂鸦为遵从 Privacy Act 做的准备

涂鸦合规与数据安全保护专家一直在与世界各地的客户合作，解决他们的问题，并帮助他们为 Privacy Act 生效后在云中运行IoT服务做好准备。这些专家还根据 Privacy Act 的要求审查涂鸦的运营和责任，以确保法律生效后涂鸦服务能够符合 Privacy Act 的规定。

✓ 我们努力确保涂鸦的产品和解决方案符合Privacy Act，客户能够放心使用我们的服务。

✓ 安全和隐私功能可帮助您遵守 Privacy Act 并更好地保护和管理个人数据。

✓ 随着监管环境的变化，我们的产品和能力也不断发展。

✓ 我们在条款中做出了强有力的数据处理、隐私和安全承诺。

4.2. 涂鸦如何遵从澳大利亚隐私原则

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Australian Privacy Principles。我们解释了我们的数据保护功能、它们如何满足 APPs 的要求，以及我们如何与客户分担合规责任。涂鸦承诺也了提供服务外，不会使用客户数据，以此来支持客户遵从Australian Privacy Principles。

数据保护义务	涂鸦如何支持 APPs 的要求
APP 1——公开透明的个人信息管理 a. 要求 APP 实体以公开、透明的方式管理个人信息 b. 实体必须有明确表达和最新的隐私政策，以描述您如何收集、使用和共享个人信息。 c. 隐私政策应以易于访问的方式免费提供	**客户关注点：** 披露如何收集、使用和共享个人数据，如制定简洁、透明、易理解、易获取的隐私政策，并通知个人数据主体。 **涂鸦做法：** 针对客户个人数据： 涂鸦通过《隐私政策》清晰地告知客户关于个人数据处理目的、方式、范围等信息。涂鸦承诺仅以合同约定或隐私政策声明的方式访问或使用您的数据来完成您订购的产品和服务。 针对最终用户个人数据： 由客户履行告知义务，在此过程中，可从涂鸦官网或联系涂鸦隐私保护办公室获取更多帮助。
APP2——匿名和假名 个人有权选择不表明身份或使用假名	**客户关注点：** 客户应用应当支持个人使用假名或昵称。 **涂鸦做法：** 涂鸦为客户提供了昵称的功能，用户可输入不表明身份的假名。
APP3——收集所请求的个人信息	**客户关注点：**

a. 普通个人信息：实体仅在该信息对实体的一项或多项功能或活动是合理必要时，才能收集。 b. 敏感信息：实体仅在个人同意后，且该信息对于一项或多项功能或活动是必要时，才能收集 c. 实体应当通过合法、公正的手段收集个人信息。	客户对其最终用户的个人数据拥有全面的控制权，客户决定数据收集的目的和方式，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。客户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，应确保所收集个人信息是业务所必须且合理的 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：** 在获得客户同意收集提供服务所必须的客户个人数据后，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目的。 对于客户个人数据，涂鸦以最小必要原则，仅收集功能所必须的数据，收集敏感数据时，涂鸦会事先征得数据主体的同意。 对于最终用户数据，由客户保证收集的合理性，并获得数据主体的同意。
APP4——处理未经请求的个人信息 当实体接收了未请求的个人信息时，实体要在合理期限内，确定是否索取了这些信息，是否符合 APP 3。 如果符合 APP 3 可以使用或披露个人信息。 如果确定不能收集，或信息未包含在联邦记录中，则应删除或匿名化。	**客户关注点：** 客户应最小化收集个人信息，仅收集与功能相关的个人信息，当收到与功能无关的个人信息时，就及时删除。 **涂鸦做法：** 作为委托处理方，涂鸦严格按照数据处理协议和合同约定处理客户数据，当客户要求删除指定数据时，涂鸦会立即执行，以帮助客户遵从 APPs。
APP5——个人信息收集的通知 在实体收集个人信息时或之前（原则上），应告知个人： a)实体的身份和联系方式， b)实体从个人以外的他人获取个人信息的事实 c)如果法律或法院要求收集，应说明收集事实 d)收集个人信息的目的 e)如果不收集全部或部分信息，对个人造成的后果 f)任何涉及的其他实体、机构或个人 g)个人如何行使访问权、更正权 h)投诉渠道，及实体如何处理投诉 i)是否有可能向海外披露个人信息 j)个人信息披露（disclose）给海外哪些国家	**客户关注点：** 客户决定并控制其收集个人信息的时间、方式和目的，并决定是否将该个人信息上传至涂鸦平台。客户还需要确保遵从其公开的处理目的。在客户与涂鸦之间，客户与其在涂鸦平台上存储个人信息的个人存在关系，因此客户能够直接与个人就个人信息的收集和处理进行沟通。因此，客户有责任满足 APP 要求，并通知个人 APP5 规定的相关事项。 **涂鸦做法：** 涂鸦按照数据处理协议和合同约定处理个人数据，涂鸦接收客户处理个人信息的指令并执行，涂鸦不会将客户数据用于任何其他目的。
APP6——个人信息的使用或披露 一般来讲，信息可被用于或披露于信息所收集的主要目的，若非主要目的，则需要获得相应的同意。在用于或披露于与主要目的相关的（在敏感个人信息的情况下为直接相关的）、个人可合理预见的信息使用或披露的次要目的时，个人信息也可无需获得同意。	**客户关注点：** 客户决定并控制其收集、使用个人信息的目的、使用对象和信息披露对象。客户必须确保仅出于允许的目的进行这些操作。 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。 **涂鸦做法：** 在获得客户同意收集提供服务所必须的客户个人数据后，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目的，也不会私自将个人信息披露给第三方。
APP7——直接营销 个人信息用于直接营销的条件是： a. 个人信息是实体向个人收集的；同时 b. 个人可能合理预见其个人信息用于直接营销；同时 c. 实体提供了易于操作的拒绝直接营销的手段。 敏感信息须在取得相关方同意后才可为被使用于直接营销。	这是客户的考虑点。
APP8——个人信息的跨境披露 实体在向海外接收方披露个人信息之前，必须采取合理措施确保该海外接收方不会违反澳大利亚隐私原则（APPs）。	**客户关注点：** 客户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。 客户可以选择其数据存储的数据中心，默认情况下，源自澳大利亚的数据将存储在 AWS 德国法兰克福节点，客户可以随时更改它。涂鸦 IoT 平台的结构设计使客户无论选择哪个数据中心存储内容，数据都能被客户有效撑控。客户应考虑是否需要向个人披露其存储或处理个人信息的位置，并在必要时从相关个人处获得关于这些位置的任何必要同意。 **涂鸦做法：** 涂鸦仅在客户选择的数据中心存储和处理客户的数据，且不会在未经客户同意的情况下移动客户数据，除非法律要求。如果客户选择在多个区域存储数据，这是客户的自主选择，无论数据在哪里存储和处理，客户将其对其数据有绝对的控制权。 客户遵守 APP 8 的义务源于向海外接收方“披露”个人信息。澳大利亚信息专员办公室（OAIC）的指导意见指出，如果客户未将个人信息的处理从其有效控制中释放出来，这可能被视为《隐私法》下的“使用”而非“披露”。因此，客户使用涂鸦云平台不构成个人信息的“披露”，因为客户保留对上传的任何个人信息的有效控制，涂鸦根据客户的指示作为数据处理者。
APP9——政府相关识别码的使用或披露 组织不得采用与政府有关的个人识别码作为其本身的个人识别码。 除非为了组织开展活动或履行职能，使用或披露个人识别码对于组织验证个人身份而言是合理必要的，否则任何组织不得使用或披露个人的政府相关身份识别信息。	客户不应把政府有关的个人识别码作为其身份标识。 涂鸦提供的产品和服务中，默认不会收集与政府有关的个人识别码。
APP10——个人信息质量 实体必须采取合理措施，确保收集的个人信息准确、最新、完整且相关	**客户关注点：** 客户对其数据有全面控制权，与个人信息主体有直接联系，应确保个人信息准确、最新且完整。 **涂鸦做法：** 涂鸦产品及服务提供了最终用户（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。
APP11——个人信息安全 客户必须采取合理措施保护其持有的个人信息不被滥用、干扰和丢失，以及不受未经授权的访问、修改或披露。在某些情况下，客户有义务销毁或去识别个人信息。	**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。客户应及时删除不再需要的信息。 **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
APP12——访问个人信息 当个人请求获得实体持有的有关他们的个人信息时，实体应当在合理期限内提供，如因涉及商业秘密、影响他人隐私等原因拒绝提供，则应书面通知个人。	**客户关注点：** 客户对其数据拥有全面的控制权。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，以响应数据主体的知情权、访问权、更正权、删除权、撤回同意权、数据导出权。 **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和产品。 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。 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。
APP13——更正个人信息 须为个人提供更正个人信息的途径，并在合理期限内免费响应个人更正请求	同 APP10

5. 关键定义

个人信息：指包括可以识别个人身份的广泛信息或意见，取决于个人是否可以被识别或在特定情况下是否可合理识别。个人信息包括：

- 个人姓名、签名、地址、电话号码或出生日期
- 敏感信息
- 信用信息
- 员工记录信息
- 照片
- 互联网协议 (IP) 地址
- 声纹和面部识别生物识别技术（因为它们收集个人声音或面部的独特特征）
- 来自移动设备的位置信息（因为它可以揭示用户的活动模式和习惯）

敏感个人数据：与 GDPR 非常相似，敏感个人数据的定义几乎相同，即“敏感个人数据涉及种族或民族血统、宗教信仰、政治观点、与工会或宗教、哲学或政治组织的隶属关系、与健康或性生活有关的数据、遗传或生物特征数据，当与自然人有关时。”

数据控制者：与欧洲法律不同，澳大利亚隐私法中没有“数据控制者”的概念。每个获取/接收个人信息的 APP 实体（即使在 GDPR 下可能被视为“数据处理者”的角色）也根据澳大利亚法律实际上被视为数据控制者，并在《隐私法》/APP 下承担自己的主要和单独的隐私义务。

数据处理者：同上。

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 Privacy Act 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 Privacy Act 具体要求的指导，因为本文不构成法律建议。