涂鸦遵从巴西 LGPD 白皮书

July 2024

Tuya Inc.

目录

前言

本文旨在帮助客户了解：涂鸦如何遵从巴西通用数据保护法（Lei Geral de Proteção de Dados，以下简称 LGPD）的要求，如何利用业界领先的数据隐私和安全功能来保护客户数据，以及涂鸦为保护个人数据安全采取的措施，同时帮助客户理解客户和涂鸦在各自服务模式下扮演不同角色以及相应的关注点。本文提供的信息适用于涂鸦及其所有产品和服务。

1. 关键定义

个人数据：指任何与已识别或可识别的自然人（即“数据主体”）有关的信息。

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。”

匿名数据：当处理时使用“合理和可用的技术手段”来消除与自然人直接或间接关联的可能性时，数据被认为是匿名的。

数据控制者：有权就个人数据处理作出决定的公法或私法自然人或法人。

数据处理者：以控制者的名义处理个人数据的公法或私法自然人或法人。

处理：对个人数据进行的所有操作，例如涉及收集，制作，接收，分类，使用，访问，复制，传输，分发，存档，存储，删除，评估或控制信息，修改，通信，传播或提取的操作；

同意：与 GDPR 类似，同意是一种“自由的、知情的和明确的表达，数据主体同意她/他为特定目的处理个人数据。”原则上，同意应该是书面的，或者以其他方式表明数据主体的表现，应该与其他合同条款区分开来，并且需要妥善记录。它可以随时被撤销。

2. 涂鸦隐私保护策略

2.1 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包括技术与管理方面的措施，以确保产品和服务能够最大化满足各个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。

2.2 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：

2.3 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、文档和法律承诺有助于支持 LGPD 合规性并满足行业隐私标准。

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。

3. 涂鸦如何遵从巴西 LGPD 的要求

3.1 巴西《通用数据保护法》概述

巴西的《通用数据保护法》（LGPD）是一项全面的数据保护法规，旨在保护个人数据的隐私和安全。它规定了数据控制者和处理者在处理个人数据时必须遵守的原则和义务，包括问责制、目的限制、数据最小化以及设计安全和隐私。LGPD 要求组织通过实施强有力的技术和组织措施，持续确保数据处理的安全性，并符合法律规定。

违反 LGPD 规定的个人或组织可能面临包括警告、暂停数据处理活动，以及最高可达违法者上一年度在巴西总收入 2%的罚款，但不超过 5000 万巴西雷亚尔。LGPD 适用于所有在巴西境内处理个人数据的个人、团体和机构，无论他们是否位于巴西境内，只要他们向巴西个人提供商品或服务或收集巴西境内个人数据。

巴西国家数据保护局（ANPD）是负责监督 LGPD 实施的主要监管机构，确保法律得到有效执行，并保障个人数据的保护。LGPD 于 2018 年 8 月 14 日签署，并于 2020 年 8 月 15 日正式生效。欲了解更多关于 LGPD 的详细信息，可以访问官方网站：LGPD 官网。

3.2 涂鸦为遵从 LGPD 做的准备

涂鸦安全与合规专家一直在与世界各地的客户合作，解决其问题，并帮助他们为 LGPD 生效后在云中运行IoT 服务做好准备。这些专家还根据 LGPD 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 LGPD 的规定。

- ✓ 我们努力确保涂鸦的产品和解决方案符合 LGPD，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 LGPD 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。

3.3 LGPD 下涂鸦的角色

根据 LGPD，控制者和处理者必须采取技术和管理安全措施，保护个人数据免遭未经授权的访问、意外或非法破坏、丢失、更改、通信或任何类型的不当或非法处理。

涂鸦同时充当数据控制者和数据处理者。数据控制者指有权就个人数据处理作出决定的公法或私法自然人或法人。 数据处理者在 LGPD 中被定义为代表控制者处理个人数据处理的自然人或法人。

1）涂鸦作为数据控制者

当涂鸦收集个人数据并确定处理该个人数据的目的和方式时，即涂鸦处理来自其直接客户(个人客户和公司客户)的数据以用于涂鸦产品和服务的帐户管理、服务访问、服务属性或联系信息以进一步支持和管理时，涂鸦充当数据控制者。

2）涂鸦作为数据处理者

当客户使用涂鸦服务处理最终用户的个人数据时，涂鸦充当数据处理者。客户可以使用涂鸦服务中提供的控制措施，包括安全配置控制，来处理和存储个人数据。在这种情况下，客户充当数据控制者，而涂鸦则充当数据处理者或子处理者。使用涂鸦本身并不能保证客户完全遵从 LGPD，客户应分析自己的业务实践、技术和组织措施，以确保遵守 LGPD，并最终承担责任。

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、用户密码策略等。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巴西国家数据保护局（ANPD）。

3.4 涂鸦如何遵从巴西 LGPD 的要求

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 LGPD。我们解释了我们的数据保护功能、它们如何满足 LGPD 的要求，以及我们如何与客户分担合规责任。

数据保护义务	涂鸦如何支持 LGPD 的要求
处理通知 在处理个人数据之前，必须通知数据主体。通知必须以清晰、充分和明显的方式提供。	**客户关注点：** ● 确保以合法方式收集个人数据。 ● 披露如何收集和处理个人数据，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。
选择和同意 ●同意必须是自由、知情且明确的表达。任何获取同意的目的的变更都需要数据主体重新同意。同意必须是明确的，这需要从数据主体那里获得明确和积极的意愿表达，而不是基于推断或以默许的方式获得或从数据主体的遗漏中获得。 ●在基于同意处理敏感数据的情况下，有必要以特定且突出的形式获得同意。 ●控制者有责任证明已获得同意	**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。 在获得客户同意收集提供服务所必须的客户个人数据后，涂鸦仅在合同约定和隐私政策声明中限定的目的范围内处理客户个人数据。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，确保客户及涂鸦业务的合法合规。
目的限制 出于向数据主体告知的合法、具体和明确的目的进行处理，并且不存在与这些目的不一致的进一步处理的可能性。	**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：** 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产品或提供广告服务。
数据传输 仅在下列情况下才允许个人数据的国际转移：	**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，

● 向提供 LGPD 规定的适当个人数据保护水平的国家或国际组织； ● 当控制者提供并证明其遵守 LGPD 中规定的数据主体原则和权利以及数据保护制度的保证时，以以下形式提供： ✓ 特定转让的具体合同条款； ✓ 标准合同条款（SCC）； ✓ 具有约束力的公司规则（BCR）；以及 ✓ 定期颁发印章、证书和行为准则； ● 当数据主体已明确并强调同意此类转移，并事先告知操作的国际性质，明确将其与任何其他目的区分开来； ● 根据数据主体的要求，为履行数据主体作为一方当事人的合同或者与该合同有关的程序所必需。	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。 **涂鸦做法：** 现阶段，巴西的数据默认存储在 AWS 美国;涂鸦提供了客户自主选择数据中心的机制（例如选择将巴西的数据存储在欧盟数据中心），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。 同时，涂鸦通过明确、透明的方式告知用户有关国际数据传输的信息，例如在隐私政策中。
保留与处置 在下列情况下，应终止对个人数据的处理： I. 确认目的已经实现，或者数据对于实现特定目的不再必要或相关； II. 处理期结束； III. 数据主体提出删除请求，或撤销同意； IV. 国家主管部门认定存在违反本法规定的行为。	**客户关注点：** 明确业务处理活动中个人数据的留存期限，留存期结束后，应对个人信息采取删除、匿名化、多次覆写擦除或销毁等处置措施。 **涂鸦做法：** 个人信息的保留期限是实现提供产品和服务目的所需的最短时间。涂鸦将根据客户要求对用户数据进行删除或匿名化处理，并在触发数据保留政策时将数据返还给客户。因此涂鸦采用了最短数据保留原则： ➢ 用户个人信息的留存仅限于获得用户明确同意的情况下，用于与服务相关的目的，未经用户同意不得用于任何其他目的。 ➢ 根据法律规定需要保留的数据，或者公司有能力证明出于业务目的所必需的数据，可以在明确的数据保留时间表规定的时间内保留。 ➢ 为实现客户或第三方的合法利益而保留的数据，仅在公司与客户或第三方有明确的合同协议或指示的情况下才能保留，例如在为客户提供服务或为其他目的提供服务时。 ➢ 客户有权根据最小数据保留原则，自行确定数据保留策略，并为了服务需要及时告知涂鸦，当客户要求删除数据或返还数据时，涂鸦将按照该明确指令执行。
数据泄露通知 控制者必须将任何可能对数据主体造成相关风险或损害的安全事件的发生在三个工作日内通知 ANPD 和数据主体。	**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。 **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。
数据处理协议（DPA） LGPD 并未对控制者和处理者协议做出具体规定，唯一的要求是数据处理者必须遵守数据控制者提供的所有指示。	**客户关注点：** 与数据者签定数据处理协议，对处理者作出书面指示。 **涂鸦做法：** 涂鸦作为数据处理者，在数据处理之前与控制控制者（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 LGPD 赋予了数据主体的知情权、访问权、更正权、删除权、反对/退出权、不受自动决策约束权、数据可携权。	**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。
数据安全	**客户关注点：**

处理机构应当采取安全、技术和管理措施，保护个人数据免遭未经授权的访问和意外或非法破坏、丢失、更改、通信或任何类型的不当或非法处理。	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。 **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
数据保护官 DPO DPO 的身份和联系信息应当以清晰客观的方式向公众披露，最好是在控制者的网站上披露。 DPO 的职责包括： I. 接受数据主体的投诉和沟通，提供解释并采取措施； II. 接收来自国家主管部门的沟通并采取措施； III. 对实体的员工和承包商进行与个人数据保护相关实践的培训。	**客户关注点：** 客户应指定数据保护官负责内部隐私和合规事宜，并将该信息对 DPA 和个人用户透明。 **涂鸦做法：** 涂鸦隐私政策中公布了涂鸦隐私办公室的联系方式，该办公室由 DPO 和隐私办公室负责，隐私办公室负责对隐私工作进行日常监控，并就涂鸦所做的努力与当局进行沟通。

4. 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 LGPD 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 LGPD 具体要求的指导，因为本文不构成法律建议。