涂鸦英国 GDPR 遵从性说明

2024 年 7 月

目录

前言

本文向我们的客户提供有关英国通用数据保护条例（UK General Data Protection Regulation，以下简称 UK GDPR）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 UK GDPR。我们解释了我们的数据保护功能、它们如何满足UK GDPR 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及其所有产品和服务。

1. 关键定义

个人数据：是指电子环境中以符号、字母、数字、图像、声音或类似形式存在的、与特定个人相关或有助于识别特定个人的信息。个人数据包括个人基本数据和个人敏感数据。

敏感个人数据：指与个人隐私权相关的个人数据，一旦受到侵犯，将直接影响个人的合法权益，如病历中记录的健康状况和私生活（不包括血型信息），有关个人身体属性和生物特征的信息，通过定位服务确定的个人位置数据等。

数据控制者：决定个人数据处理目的和方式的组织或个人。

数据处理者：通过与数据控制者签订的合同或协议代表数据控制者处理数据的组织或个人。

同意：指明确、自愿、肯定地表示允许处理数据主体的个人数据。

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 UK GDPR 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. 涂鸦如何遵从英国 GDPR 的要求

3.1 英国《通用数据保护条例》概述

UK GDPR（英国通用数据保护条例）是英国在脱欧后基于欧盟的 GDPR（General Data Protection Regulation）制定的隐私和数据保护法规。该条例旨在保护个人数据的隐私和安全，确保数据处理过程中的合法性、公平性和透明性。UK GDPR 强调数据处理的核心原则，如数据最小化、准确性、存储限制和保密性，要求数据控制者采取适当的技术和组织措施来保障个人数据的安全。

UK GDPR 适用于所有在英国境内运营的企业和组织，以及那些虽然位于英国境外但处理英国居民数据的企业和组织。无论是提供商品或服务给英国居民，还是监控其行为的企业，均需遵守这一条例。通过这些规定，UK GDPR 旨在提升数据保护标准，增强公众对数据隐私的信任，并确保数据处理者对其数据处理活动负有明确的责任和义务。

总体而言，UK GDPR 不仅继承了欧盟 GDPR 的核心理念，还结合了英国的具体法律需求，形成了一套既具普遍适用性又具灵活性的个人数据保护法规。

3.2 涂鸦为遵从 UK GDPR 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，解决其问题，并帮助他们为 UK GDPR 生效后在云中运行 IoT 服务做好准备。这些专家还根据 UK GDPR 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 UK GDPR 的规定。

- ✓ 我们努力确保涂鸦的产品和解决方案符合 UK GDPR，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 UK GDPR 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 UK GDPR 下涂鸦的角色

根据 UK GDPR，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。

根据 UK GDPR，涂鸦同时充当数据控制者和数据处理者。数据控制者根据 UK GDPR 的定义，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 UK GDPR 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终端用户的个人数据，将终端用户的个人数据传输到涂鸦云时，涂鸦将充当数据处理者。客户可以使用涂鸦服务中提供的功能（包括安全配置控件）来处理和存储个人数据。在此情况下，客户充当数据控制者，而涂鸦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 UK GDPR，客户应分析自己的业务实践、技术和组织措施，以确保遵守 UK GDPR，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英国数据保护机构（ICO）。

3.4 涂鸦如何遵从 UK GDPR 的要求

数据保护义务	涂鸦如何支持 UK GDPR 的要求
数据最小化原则 充分、相关且仅限于与处理目的相关的必要信息（“数据最小化”）	**客户关注点:** 1、仅收集和处理相关的必要信息，不能在用户未同意情况下收集非必要信息 **涂鸦做法:** 1、涂鸦只收集和处理为实现特定目的所必需的最少量个人数据。通过定期审查数据处理活动，确保数据收集和处理的必要性。
合法性、公平性和透明度 在处理个人数据之前，必须通知数据主体，并且以合法、公平和透明的方式处理与数据主体相关的信息	**客户关注点:** 1、确保以合法方式收集个人数据。 2、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**: 1、涂鸦确保所有数据处理活动均具有合法依据，如数据主体的同意、合同履行的必要性或法定义务的履行。涂鸦通过隐私政策和通知向数据主体透明地展示其数据将如何被处理。
目的限制 个人数据仅能出于个人数据控制者、个人数据处理者、个人数据控制者和处理者、第三方关于个人数据处理的声明所注册和声明的目的进行处理。	**客户关注点**: 1、应确保个人数据的收集、使用或披露仅限于已声明的指定的合法目的。 客户应确定数据处理的目的与告知数据主体的一致。 **涂鸦做法:** 1、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。
存储限制 以能够识别数据主体的形式保存，保存时间不得超过实现个人数据处理目的所需的时间，保障数据主体的权利和自由	**客户关注点:** 1、个人数据仅在实现处理目的所需的期间内保留，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:** 1、达到保留期限后，涂鸦将按照合同约定返还或者删除/匿名化客户个人数据。
数据主体的知情权、访问权、更正权、删除权、反对/退出权、数据可携权（数据导出权）	**客户关注点:** 1、客户对其数据拥有全面的控制权， 应建立个人权利响应流程，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: 1、涂鸦帮助客户提供了数据主体能够访问、更正、删除、导出数据的功能。
选择和同意 ●处理个人数据需要征得同意，除非法律另有规定。如果同意作为合法依据，则同意必须是由数据主体自愿的并且明确表达（如书面、语音、检查同意框、选择同意技术设置等）。沉默或不回应并不构成有效的同意。 ●在处理敏感个人信息时必须通知数据主体此类处理，并告知数据主体要处理的数据是敏感数据。 ●数据主体可以撤回同意，此时应通知数据主体撤回同意可能引发的后果和损害。	**客户关注点**: 1、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**: 1、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。
数**据保护政策** UK GDPR 要求公司内部制定全面的数据保护政策，涵盖数据处理的各个方面，并定期审查和更新，以保持合规性。	**客户关注点:** 1、要求数据处理者提供数据保护政策：确保处理者有适当的数据保护政策，并定期审核其合规性。 2、确保合同规定：在合同中明确规定处理者必须遵守 UK GDPR，并列出处理者的具体义务。 **涂鸦做法**: 1、已经制定并实施数据保护政策: 确保所有处理活动都符合 UK GDPR 的规定。同时也会定期审查和更新政策以反映最新的法规变化和公司内部流程。 2、定期组织员工培训：对所有相关员工进行数据保护培训，使他们了解 UK GDPR 的要求及其在日常工作中的应用。
数据安全 从个人数据处理之初以及整个处理过程中均采取个人数据保护措施 个人数据在处理过程中受到保护和安全措施，包括使用技术措施防止违反个人数据保护规定以及防止因事件而丢失、毁坏或损坏 在处理敏感个人数据时，除了安全措施和基本措施外，必须满足以下要求: (a) 必须指定负责个人数据保护的部门和人员（并通知网络安全和高科技犯罪预防司； (b) 必须通知数据主体敏感个人数据将被处理。	**客户关注点**: 1、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:** 1、涂鸦对个人数据全生命周期做了全面保护，在数据采集阶段做了最小化处理和严格的账号认证机制； 在传输阶段做了传输通道和内容双重加密；在存储阶段对个人数据均做了高强度加密，每个用户密钥均不相同；在展示阶段做了脱敏处理；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
数据泄露通知 数据处理者在发现数据泄露后，应当尽快通知数据控制者。数据控制者应当在数据泄露发生后 72 小时内通知网络安全部门。如果无法在 72 小时内通知，则需要说明理由	**客户关注点**: 1、在发生数据泄露事件，需要在 72 小时内向第三方监管机构进行通报。内部也需要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**:

	1、涂鸦发现数据泄露后，将第一时间通知数据控制者。
数据披露 披露个人数据需要获得数据主体的同意，除非法律另有规定。	**客户关注点**: 1、确保个人数据的披露合法并获得的数据主体同意。 2、对个人数据接收方进行尽职调查，选择具备足够保护水平的接收方进行合作，保障披露的个人信息安全。 **涂鸦做法**: 涂鸦不会使用或披露客户个人数据，除非是客户授权同意，或者是为遵守适用的法律法规或政府机关的约束性命令（如果有）。
数据保护影响评估(DPIA) 当某种处理类型，尤其是使用新技术的处理类型，考虑到处理的性质、范围、背景和目的，可能对自然人的权利和自由造成高风险时，控制者应在处理之前对预期的处理操作对个人数据保护的影响进行评估	**客户关注点:** 在处理高风险数据之前，必须执行 DPIA，识别和减轻潜在风险。 **涂鸦做法**: 当处理高风险数据时，涂鸦会协助客户进行 DPIA，并提供必要的信息和支持 2、基于 DPIA 的结果，涂鸦会提出数据保护措施的改进建议，帮助客户减轻数据处理中的风险。
数据处理协议(DPA) UK GDPR 要求数据控制者和数据处理者必须签订处理个人数据的协议或合同。	**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。
数据保护官(DPO) UK GDPR 要求，企业必须任命一名数据保护官，适当且及时地参与与个人数据保护相关的所有问题	**客户关注点**: 客户作为数据控制者，应当任命一名 DPO，需要了解 DPO 职责并且将联系方式公开在隐私政策当中 **涂鸦做法:** 涂鸦已任命 DPO，负责监督数据保护策略的实施并作为数据保护问题的主要联系人。DPO 的联系方式公开在我们的隐私政策中
数据传输机制 UK GDPR 要求，若正在处理或准备在转移到第三国或国际组织后进行处理的个人数据的转移，只有在控制者和处理者遵守本章规定的条件的情况下，才应进行	**客户关注点**: 1、客户作为数据控制者，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。将个人数据传输至英国外第三方前应先取得个人同意。 **涂鸦做法**: 1、在英国范围内的用户数据都存储在欧洲数据中心中，并且涂鸦向欧盟外的国家进行数据转移，都会采用 UK GDPR 认可的合规机制，如标准合同条款（SCCs）、或 ICO 批准的适当保护措施

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