隐私与安全

概述

ThinkingData 尊重和保护人们的数据隐私和权利，我们构建的 ThinkingEngine 符合行业最佳实践和全球数据安全相关法律法规法规。访问我们的隐私中心，了解我们如何遵守各种隐私准则。

采集

您通常会使用我们的 SDK 进行数据采集，在进行数据采集之前，可以按照以下步骤完成隐私合规的要求。
Android SDK
iOS SDK
JavaScript SDK
Unity SDK
Unreal SDK
Cocos2d-X SDK
小程序&小游戏 SDK
ReactNative SDK
Flutter SDK
接入我们 SDK 的应用开发完成，您通常会把应用分发到 GooglePlay 和 Appstore 平台，您可以参考以下文档进行平台分发:AppStore，GooglePlay。

传输

在数据传输层，我们提供多种技术方案，保障数据传输的安全性
•支持 Https 协议加密传输报文
•支持数据编码压缩
•支持自定义秘钥加密传输数据
•支持敏感属性脱敏或加密

存储

•提供私有化部署服务，数据会存储在您指定的存储空间
•定期备份数据，以防止数据丢失或损坏。备份数据需要存储在安全的地方，并且需要定期测试备份数据是否可用。
•支持安全的存储设备和存储介质，比如使用硬件加密的磁盘、使用专门的存储设备等。同时需要注意存储设备的物理安全，避免存储设备被盗或损坏。

使用

账号登录

我们支持 SSO 方式登录 ThinkingEngine，同时可强制所有用户启用 MFA 进行登录时的多重身份验证，保障系统使用的安全性。

访问控制

对于敏感数据，需要对访问权限进行控制，只有授权的人员才能进行读写操作。通过数据权限，可以限制成员能访问的数据表范围，并对敏感字段进行加密。管理员通过角色授权等方式，能控制成员的功能使用权限，限制对数据的查询和导出。

安全审计

根据您的需要，我们可以为您部署安全审计项目，对数据的访问和修改进行审计，记录操作人员、时间、操作类型等信息，以便发现异常操作并及时处理。

数据管理

ThinkingEngine 的数据查询和删除功能旨在帮助 ThinkingEngine 实现满足《一般数据保护条例》（GDPR）法规中概述的要求。这些 API 可以帮助用户删除他们在 ThinkingEngine 上的个人数据，也可以帮助用户查询他们在 ThinkingEngine 上存储的个人数据。这些措施旨在确保 ThinkingEngine 符合 GDPR 的规定，并保护用户的隐私和数据权利。

- 用户选择退出

虽然我们提供可用于删除或检索 GPDR 概述的个人数据的方案，但用户选择停止数据跟踪也很重要。 如果使用客户端 SDK 进行跟踪，您可以使用 SDK 提供的方法停止数据采集。

- 验证

使用我们提供的 API 查询功能之前，您必须手动生成查询秘钥。如何生成查询秘钥?

- GDPR 和 CCPA :数据查询、数据删除