探鸽智能隐私保护白皮书

深圳市探鸽智能科技有限公司

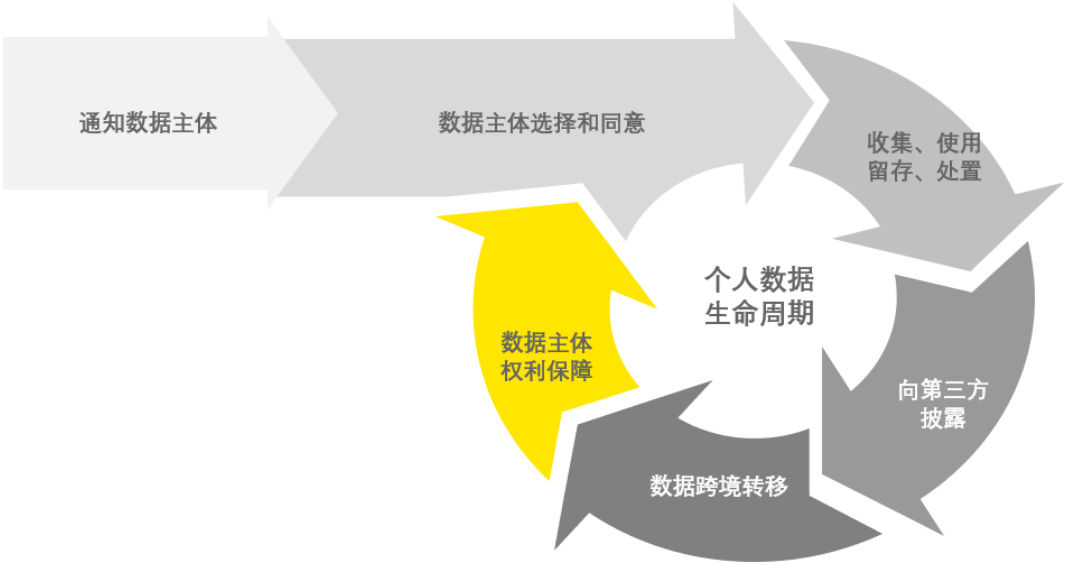
2026/6/8

目录

前言

深圳市探鸽智能科技有限公司（以下简称“探鸽”）成立于 2018 年 10 月 23 日，是一家专注于物联网音视频 PaaS 及数据服务的企业。公司通过探鸽智能物联网音视频云平台（以下简称“探鸽云平台”），向物联网设备制造商、品牌客户、解决方案提供商及外部开发者提供全方位服务。该平台具备嵌入式实时音视频通信、设备接入、云存储、4G 连接、AI 事件检索、AI 事件摘要、目标识别、开放 API 及 SDK 开发能力等核心功能。

探鸽高度重视隐私保护，严格遵守欧盟《通用数据保护条例》（GDPR）及《加州消费者隐私保护法案》（CCPA），并持续关注全球各国和地区适用的隐私保护法律法规，构建与业务规模、数据风险相匹配的隐私治理体系。本白皮书立足 GDPR 及 CCPA 监管框架，系统梳理了探鸽在内部隐私保护政策与组织、风险管理及处理的安全性、隐私审计监督、隐私设计、处理的合法性、数据主体权利、合作方管理、跨境数据管理、数据的合理保留及销毁、泄露管理以及意识培训共 11 个核心领域的实践，基于个人数据生命周期全栈管理的理念，旨在向各方展示探鸽的隐私保护管理体系。



个人数据全生命周期管理

探鸽遵循的处理个人信息处理基本原则

探鸽根据适用的法律法规确定了个人数据处理的基本原则，并通过适当的管理和技术措施，确保在处理个人数据时遵从以下基本原则：

- **目的明确：**具有明确、清晰且具体的个人信息处理目的。
- **公开透明：**以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。
- **选择同意：**向个人信息主体明示处理目的、方式、范围等规则，并征得其授权同意。
- **最小必要：**仅处理满足处理目的所需的最少个人信息类型和数量。
- **最短保存期限：**个人信息的保存期限应为实现处理目的所必要的最短时间。
- **安全保障：**具备与安全风险相匹配的安全能力，采取充分的管理措施和技术手段，保障个人信息的保密性、完整性、可用性。
- **主体参与：**向个人信息主体提供便捷渠道，支持其查询、更正、删除个人信息，以及撤回授权同意、注销账户和进行投诉举报。

探鸽隐私保护管理体系

内部隐私保护政策与组织

探鸽制定了完善的隐私数据合规政策，该政策通过飞书平台进行集中维护，并向全体员工公示。其内容涵盖数据主体权利、数据处理原则、个人信息的收集、存储、使用、共享、披露及传输、个人信息出境管理、隐私影响评估、应急管理以及隐私保护的适用范围等关键领域。此外，公司由信息安全和隐私管理小组每年开展一次法律法规符合性检查，以确保政策的持续有效。

为保障上述体系的有效运行，探鸽设立了专门的信息安全与隐私保护管理委员会及信息安全和隐私管理小组，全面负责公司信息安全和隐私体系的建立、推进、执行与持续优化。委员会由公司总经理、章程规定的高管及体系管理者代表组成，信息安全和隐私管理小组则由跨部门成员构成。

日常个人数据治理和保护工作由信息安全和隐私管理小组负责，其核心职责包括：

- **统筹管理：**全面统筹公司个人信息保护工作，制定并更新个人信息管理策略；
- **数据盘点与权限管理：**建立、维护和更新组织所持有的个人信息清单（含类型、数量、来源、接收方等），并制定授权访问策略；
- **风险评估：**开展个人信息安全影响评估，提出保护对策建议，督促整改安全隐患；
- **培训宣导：**组织开展个人信息安全培训；
- **投诉受理：**公布投诉与举报渠道，并及时受理相关反馈；
- **外部沟通：**保持与相关监管及主管部门的沟通，及时通报或报告个人信息保护及事件处置情况。

此外，为严格遵循 GDPR 的要求，探鸽已任命独立于日常业务部门的数据保护官（DPO），该职位直接向高级管理层汇报。数据保护官的主要职责涵盖：

- **合规监督：**监督企业数据处理活动，定期组织隐私保护评估（PIA）/数据保护影响评估（DPIA）

并提供专业建议；

- **监管对接：**作为公司与数据保护监管机构之间的主要联络人，协助响应监管机构的调查或审计；
- **权利响应：**建立并优化数据主体权利响应流程，保障数据主体权益；
- **培训组织：**策划并组织员工的数据保护专项培训；
- **记录与报告：**详细记录和保存组织数据处理活动的信息，定期向最高管理层汇报。

风险管理及处理的安全性

为保障探鸽云平台在符合适用法律法规的前提下持续有效支撑业务运营，公司实施了一套全面的风险管理框架，旨在提前识别、评估、管理和监控潜在信息安全及隐私保护风险。

公司已建立内部管理制度，明确了员工在风险识别、评估及处置环节的职责要求，以确保风险得到有效管控。在具体执行层面，人力资源团队每年协同各业务部门，全面梳理现有业务运营中的核心信息资产，并从业务运营、欺诈防范、内部控制、信息系统安全及隐私合规等多个维度，深入识别可能对核心资产造成负面影响的潜在风险。所有已识别的风险均由专门的责任团队负责跟踪整改，最终将整体评估过程及结果汇总形成信息安全与隐私风险评估报告。

在制度落实的基础上，为进一步夯实数据处置的安全性，探鸽采取与数据风险等级相适应的技术与组织措施，全力防范个人数据在传输、存储及处理过程中的意外或非法销毁、丢失、篡改、未经授权披露或访问。

在数据传输与存储层面，探鸽采用 HTTPS 及 DTLS 协议确保传输安全。敏感个人数据与核心业务数据均进行加密存储及逻辑隔离。针对手机号码等高敏感字段，则采用去标识化（脱敏）处理或行业通用保护算法进行存储，以防止未经授权的直接访问。

在身份与访问控制方面，公司基于最小权限原则实施严格管控，并结合签名安全校验与令牌管理机制，确保仅授权人员可访问相应数据资源。此外，探鸽定期开展系统漏洞扫描、渗透测试及安全基线核查，对发现的风险项实施即时修复与复测验证，从而确保持续的安全态势。

隐私审计监督

为确保隐私保护工作的持续改进，探鸽建立了完善的审计机制。在制度层面，公司已制定专门的审计管理制度，明确了公司在开展信息安全及隐私保护审计工作时必须遵循的检查原则、审计频率及管理流程。

在此基础上，公司每年制定具体的隐私保护审计计划，明确审计范围（涵盖内部控制、信息安全及隐私保护）、执行时间表及参与团队，并依序开展审计工作。审计结束后，公司将形成正式审计报告。针对审计中发现的问题，由人力资源团队将协同相关业务部门开展根本原因分析，确认整改方案并落实后续行动，确保内控体系的有效性与持续性。

隐私设计

探鸽建立了完善的隐私数据保护风险评估流程，坚持隐私设计（Privacy by Design）理念，将隐私保护贯穿于探鸽云平台的全生命周期。

由探鸽信息安全和隐私管理小组进行持续的监督和管理

当平台计划引入新技术、推出新功能，或对现有技术架构及功能进行调整时，公司会在版本正式投入开发前的需求分析和功能设计阶段执行 PIA 评估，评估范围涵盖以下关键方面：

- **涉及的个人数据类型**：包括敏感信息（如：定罪记录、遗传数据、政治观点或宗教信仰等）；
- **数据处理目的**：明确收集和处理个人数据的具体目标；
- **数据规模**：评估个人数据体量，以判断是否构成大规模处理；
- **跨境传输**：涉及个人数据跨境流动的情况；
- **自动化决策**：涉及自动决策及分析的场景；
- **第三方集成**：使用 Cookie，社交媒体集成或第三方开源平台的情况；
- **新技术应用**：将新技术或新解决方案纳入信息处理活动；和
- **儿童信息保护**：涉及儿童社会服务信息的收集情况。

基于 PIA 的评估结果，产品团队需先完成数据清单及数据流转图的梳理，明确数据处理目的及现有管控措施。若评估确认拟采用的新技术、新功能或调整方案可能对自然人的权利和自由构成较高风险时（例如涉及敏感个人信息处置）时，公司将进一步启动 DPIA 的评估工作。通过 DPIA 评估，明确各版本为保障个人数据安全合规需要实现的技术功能，并在上线前对功能的完成情况及效果进行严格审核。同时，公司保留每次评估的全过程记录，形成可追溯的管理闭环。

DPIA 流程涵盖五个核心维度：

- **信息概况梳理**：明确版本功能涉及的数据收集与处理情况，包括处理目的、操作类型、涉及的数据类别及主体、信息系统及第三方处理情况等；
- **必要性评估**：严格审查数据处理是否遵循最小化原则，确保收集行为合理且必要；
- **风险识别与评估**：全面识别潜在风险点，并开展定性与定量评估；
- **应对措施制定**：针对识别出的风险，制定针对性的缓解措施，落实相应的安全保障机制；

- **记录与归档：**将评估过程与结论规范化记录并归档，为上线前的审计、问责及后续优化提供可靠依据。

除上述针对常规迭代项目的专项评估外，探鸽还建立了常态化的周期性评估机制。每年，公司会对现有业务运营中的个人信息处理活动开展全面 DPIA 评估，对各平台的个人信息处理活动、字段类型及处理流程进行全面梳理，切实贯彻“最小必要”收集原则。此外，探鸽定期对数据处理活动记录（RoPA）进行评价，向相关方报告评价结果。针对识别出的流程缺陷，及时梳理改进方案并完成流程优化，确保持续合规。

处理的合法性

探鸽会根据不同业务场景与数据处理目的，严格界定适用的法律依据。在设计特定或可选性功能（如获取相机、麦克风及位置权限）时，探鸽始终将数据主体的自主选择置于首位，仅在获得明确同意后方可实施相关数据处理活动。

针对探鸽云平台核心服务的交付，探鸽基于履行合同之必要处理个人数据。同时，为切实履行法定义务，探鸽在强制性监管合规等场景下，依法依规处理必要数据。

此外，在充分评估并确保不侵害数据主体权利与自由的前提下，探鸽会基于自身或第三方的合法利益处理个人数据，例如开展内部数据分析以优化服务质量等。

数据主体权利

探鸽高度重视数据主体对其个人信息的管理权利，致力于协助其有效管理个人信息，并提供便捷、透明且合规的权利行使机制。为此，探鸽在隐私政策中明确公示了相关权利的响应渠道。

探鸽全面支持数据主体行使知情权、同意权、访问权、更正权、删除权、数据可携权、拒绝权及反对权，并已建立标准化的隐私权响应流程。针对不同数据处理场景，公司实施了差异化的协同机制：

- 在委托处理场景下，公司将及时将问题反馈至受托方，交由受托方负责跟进处置；
- 在共同处理场景下，公司建立了涵盖“请求接收、身份验证、合理性审查、数据检索、处理执行到通知反馈”的全流程响应机制。原则上，该流程将在一个月内完成。若涉及向第三方共享数据以完成处置的情形，探鸽将在收到请求后立即同步相关要求至第三方，督促其按行权要求完成处置，并在约定时间内将处理结果反馈给数据主体。

此外，公司在制度中明确了数据主体获取信息副本的场景及内容规范。如需提供副本，由授权人员按流程导出或提供相关信息，并严格执行准确性核验程序。

针对数据主体提出的撤回同意或限制数据处理请求，公司遵循共同处理场景下的处置流程。在收到请求后，对受影响数据进行人工标记，以确保能够限制对该数据的进一步分析与处理，并在规定时限内完成响应。

最后，依据 GDPR 及 CCPA 相关规定，对于明显缺乏依据、过度或与法律义务相冲突的请求，探鸽有权合法地予以限制或拒绝，并在规定响应时限内向数据主体说明具体理由。

为确保全流程的可追溯性，探鸽将对上述所有涉及数据主体权利请求的处置情况进行记录并归档，保存期限为 24 个月，以备数据主体或监管机构后续核查。

合作方管理

探鸽仅与具备完善数据安全保障能力且能落实适当技术与组织措施的第三方供应商建立合作。

在引入阶段，探鸽建立标准化合作伙伴准入流程，涵盖开展隐私合规评估等环节，确保供应商资质符合要求。针对涉及海外数据主体或新增的供应商，探鸽强制要求签署数据处理协议，以明确双方在数据传输、存储及处理等方面的法律责任与保护义务。

在合作存续期间，探鸽建立并持续维护供应商清单，指定专人进行常态化跟踪与不定期核查。此外，探鸽每年定期进行供应商信息安全评审，确保持续合规。

跨境数据管理

探鸽致力于提供全球化服务，业务覆盖多个海外区域。在获得数据主体授权或符合法律法规要求的前提下，部分信息可能会被转移到数据主体所在国家/地区的境外司法管辖区，或由境外进行访问。

为切实保障数据跨境传输的安全与合规，探鸽从协议签署、技术防护及流程管控三个维度构建全方位保障体系：

- 在协议层面，探鸽与数据接收方签署标准合同条款（DPA），明确双方责任划分与违约追责机制；
- 在技术层面，探鸽采用 HTTPS 安全传输协议，实施传输层加密；
- 在流程层面，探鸽建立了数据跨境审核标准，强制要求在数据出境前完成安全评估。审核范围涵盖传输目的、具体字段、数据规模、处理数据的法律依据、数据接收地以及接收方的安全资质等情况。

数据合理保留及销毁

探鸽遵循存储最小化原则，仅在实现数据处理目的所必要的最短时间内留存个人数据。为此，探鸽对数据保留实施分类分级管控策略：

- 对于非结构化的业务数据：探鸽在对象存储服务中配置数据生命周期管理策略，严格遵循服务预设的保留规则，在到期后自动执行数据删除；
- 对于账密数据，在终端用户注销 APP 账号后，系统将自动触发账密数据的删除流程；
- 针对数据主体行权请求：当数据主体行使删除权时，由专人执行手动删除操作，并同步保留完整的删除日志以备审计。

若法律另有规定，或为配合政府机关执法、法院判决及裁定需要，数据可依法延长存储期限。

当个人数据不再具备处理必要性时，探鸽将采取必要的技术及组织措施，对数据进行永久删除或匿名化处理，以彻底防止未经授权的访问或泄露风险。

泄露管理

探鸽建立了完善的数据泄露响应与处置机制，以有效应对个人数据泄露事件。当发生数据泄露事件时，探鸽将立即启动应急响应程序，开展数据泄露风险评估与定级。

- 若评估认定泄露可能对自然人权利与自由造成高风险，探鸽将在知悉泄露后的 72 小时内，按照法定程序向监管机构报告；
- 若泄露对数据主体造成高风险，探鸽将毫不迟延地通知受影响的数据主体。

为强化事件管理的闭环与持续改进能力，探鸽对所有个人数据泄露事件进行详细记录与归档，内容涵盖事实经过、影响评估及已采取的补救措施。针对具有代表性的事件，IT 人员将牵头组织跨部门复盘会议，深入分析原因并制定改进措施。

同时，探鸽高度重视事前防范，基于业务场景识别潜在的数据泄露风险，并按严重程度分类，形成相应的应急演练方案。探鸽每年至少执行一次数据泄露应急演练，并在演练后形成专项汇报与复盘报告，确保持续优化。

此外，探鸽在与合作伙伴签署的数据处理协议中，明确了合作伙伴就数据泄露事件中的责任与义务，确保上下游安全防线的一致性。

意识培训

公司会结合业务发展态势、业务规模及涉及的国家与地区，深入分析需关注的个人信息保护合规要求，持续完善通用合规培训体系，并按需不定期开展专项培训。

同时，公司建立了事后考核机制，对员工培训后的知识掌握情况进行评估，旨在全面提升公司全体员工的个人信息保护意识，有效降低合规风险。

结语

在物联网加速发展的时代背景下，数据已成为驱动创新的核心要素，而隐私保护则是技术信任的基石。探鸽始终将用户隐私权置于业务发展的核心位置，不仅严格遵循 GDPR 及 CCPA 等全球主要隐私法规要求，更通过制度、组织、技术与文化的深度融合，构建起覆盖“收集—处理—存储—销毁—响应”全生命周期的隐私治理体系。

我们深知，合规不是终点，而是持续进化的起点。未来，探鸽愿意长期投入，深化隐私数据保护技术应用，积极拥抱监管动态与行业最佳实践，与客户共筑可信、稳健的智能物联未来。

附件一：术语解释

- **数据主体：**个人信息所标识或关联的自然人。
- **数据保护官（DPO）:**是组织内部独立设立的合规专家，负责监督数据保护策略的执行、监测合规性并作为企业与监管机构及数据主体之间的联络人。
- **隐私保护评估（PIA）：**当某系统或项目涉及个人可识别信息的收集、使用或披露时，组织应在实施前开展系统性评估，识别潜在隐私风险并制定缓解措施。
- **数据保护影响评估（DPIA）：**在高风险数据处理活动（如大规模监控、自动化决策、跨境传输）前开展的系统性事前评估。
- **去标识化：**通过技术手段（如脱敏、哈希、替换）使个人信息在不借助额外信息的情况下无法直接识别特定自然人。
- **数据处理活动记录（RoPA）：**探鸽依法建立并维护的数据处理活动台账，包含处理目的、数据类别及接收方、留存期限及安全措施等要素，用于内部审计与监管检查。
- **数据处理协议：**探鸽与第三方合作方签署的具有法律约束力的协议，明确数据处理目的、方式、范围、权利和职责、安全事件处置、泄露响应责任等内容，是委托处理或共同处理场景下的法定合规前提。
- **匿名化：**通过不可逆的技术处理（如 k-匿名、差分隐私、强哈希），使个人信息无法再识别特定自然人，且无法复原。