原力金智 SDK/API 合规与安全指南

引言

为有效治理App强制授权、过度索权、超范围收集个人信息等现象，保障个人信息安全，2019年1月，中共中央网络安全和信息化委员会办公室、工业和信息化部、公安部、国家市场监督管理总局联合发布了《关于开展App违法违规收集使用个人信息专项治理的公告》。同时，受四部门委托，全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会成立App违法违规收集使用个人信息专项治理工作组（下称“App专项治理工作组”），具体推动App违法违规收集使用个人信息评估工作。

自2019年至今，《App违法违规收集使用个人信息行为认定方法》《App违法违规收集使用个人信息自评估指南》《App系统权限申请使用指南》《网络安全实践指南-移动互联网应用基本业务功能必要信息规范》《网络安全实践指南-移动互联网应用程序（App）使用软件开发包（SDK）安全指引》等文件陆续发布，为监督管理部门认定App违法违规收集使用个人信息行为提供参考，同时也为App开发者和运营者、SDK开发者等主体自查自纠提供了指引。

综上，App（包括App嵌入的第三方代码、插件、SDK，以及通过API调用的第三方技术接口等）对于个人信息的收集使用及对个人信息主体权益的保障问题作为相关主管部门的重拳治理事项，虽然《个人信息保护法（草案）》等强制性法律法规的立法推进，监管力度也随之日益加大，监管标准亦日益趋严。

为帮助使用原力金智SDK/API的App开发者和运营者（以下简称“您”）更好地落实终端用户个人信息保护相关事宜，避免因涉及第三方相关业务实践而违反相关法律法规、政策及标准的规定，同时，也便于您更清楚地理解、认识原力金智提供的SDK产品与API能力的合规性和已采用的安全保护技术能力，特别是保护个人信息和隐私的方法和措施，我们特编写《原力金智SDK/API合规与安全指南》（以下简称“《指南》”），供您参考。由于目前相关法律法规、政策及标准中主要对SDK产品的应用提供相关指引，以下将统一以SDK视角描述相关内容，如您是集成、调用原力金智API能力的开发者和运营者，本《指南》中适用于原力金智API能力的部分同样可供您参考。

为免歧义，本《指南》中的“合规要求”、“注意事项”等内容，均为原力金智基于自身对国家相关法律法规、政策及标准的理解而起草，仅作为参考内容向您提供，不构成也不应被视为对任何法律法规、政策及标准的有权解释、法律意见或法律建议，亦不构成原力金智对外的任何承诺与保证。除涉及原力金智自身相关事实信息以外，原力金智不对本《指南》中的任何规定本身及对规定理解的时效性、准确性、正确性承担任何责任。您与您所具体开发、运营的App是否达到或满足本《指南》中所述的任何内容，不构成原力金智对前述App合规性的担保或保证，您仍应独立对所开发、运营的App合规性承担相关责任。

指南正文

本《指南》主要包括以下三方面内容，如有任何问题，请通过business@yljz.com与原力金智联系：

1. 开发者个人信息保护的合规要求，主要向您介绍了通常情况下开发、运营一个 App 所必须关注的个人信息保护要求；
2. 使用原力金智能力时的合规注意事项，主要包括您应当进行的自查工作和原力金智可能提出的审查要求；
3. 原力金智的数据安全保护能力，主要向您介绍了原力金智所具体采取的数据安全保护措施与机制。

1. 开发者个人信息保护的合规要求

本部分主要针对的是，您在开发、运营一个App过程中需要使用原力金智SDK的场景，并重点向您提供您作为开发者需要关注的个人信息保护合规基本要求，主要包含有关个人信息收集使用的合法授权及主体权益保障的重点合规要求解读。

1.1 用户个人信息处理规则的告知

您应当告知用户您所开发或运营的 App 对于个人信息的处理规则，以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项，并在相关事项发生变化时，以适当方式通知用户：

1）App 涉及个人信息处理活动的个人信息处理者的名称或者姓名和联系方式。

2）App 涉及个人信息的处理目的、处理方式，处理的个人信息种类、保存期限，并应完整、清晰、区分说明各业务功能所收集的个人信息。每个业务功能在说明其所收集的个人信息类型时，应逐项列举，不应使用“等、例如”等方式概括说明；涉及处理敏感个人信息的，还应当向用户告知处理敏感个人信息的必要性以及对用户权益的影响。

3）针对嵌入的第三方代码、插件（如 SDK）收集个人信息，应当说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式以及 SDK 服务提供方的个人信息处理角色（注：例如可采用隐私政策、弹窗提示、文字备注、文本链接等方式说明，具体可参考我们在下文中的举例）。

4）App用户作为个人信息主体行使适用法律规定权利的方式和程序。

5）法律、行政法规规定应当告知的其他事项。

特别地，针对接入和使用原力金智的 SDK 产品和/或服务前，您应当满足以下告知义务：确保终端用户 首次启动应用时单独弹出《人脸信息处理协议》，在终端用户主动点击同意《人脸信息处理协议》后， 再初始化本 SDK。且《人脸信息处理协议》的内容应包含：使用的 SDK 名称、SDK 的处理目的、 处理方式及处理的个人信息类型。

1.2 App 上线需要面向终端用户制定哪些配套的合规文件？

您至少需要制定一份独立的隐私政策。隐私政策（或命名为个人信息保护政策等类似名称），是说明 App 的个人信息收集和使用情况，获得用户的合法授权以及保护用户个人信息主体权利的重要文档。隐私政策的内容应符合国家相关法律法规、政策及标准的规定，以及您与原力金智、您与终端用户 的具体约定。特别是：

1) 符合《GB/T35273-2020 信息安全技术 个人信息安全规范》（您可以通过国家标准全文公开系统查询该文件内容，http://openstd.samr.gov.cn/ ），该文件的四份附录对您理解个人信息保护要求和隐私政策起草亦具有重要的参考价值，即：

   附录 A ：个人信息示例

附录 B ： 个人敏感信息判定
附录 C ： 保障个人信息主体选择同意权的方法
附录 D ： 隐私政策模板

2) 您的隐私政策应向终端用户明示您在App 中部署原力金智SDK 收集使用个人信息的目的、方式 和范围等，并提供符合法律法规要求、您与原力金智之间约定的保护标准。

1.3 App 上线的隐私政策中应披露第三方 SDK 的哪些内容?

您应在隐私政策中向终端用户逐一明示您嵌入的第三方 SDK 名称、提供方、第三方 SDK 所收集使用个人信息的目的、方式和范围。您应当明确告知终端用户，您谨慎地选择了原力金智作为合作方， 并委托原力金智收集、使用、加工和处理终端用户的相关个人信息。

原力金智建议您在隐私政策中的数据共享与披露章节，可参考如下条款表述向终端用户明示原力金智 SDK 的相关情况（以下示例不代表真实业务情况），如您需要对外披露原力金智的数据安全能力，请见本《指南》第三部分，如您在特定业务场景下需要了解更多原力金智 SDK/API 的必要信息，请联系原力金智相应人员：

1) 文字描述方式向终端用户明示

“为了【人脸身份验证功能（示例）】之目的，我们的产品可能会集成由合作方原力金智提供的【FinAuth（示例）】SDK 或其他类似应用程序，因此，我们需要通过SDK 收集您的【面部图像特征（示例）】，用于实现核验功能。为了您的信息安全，我们已与原力金智等第三方SDK 服务商签署严格的合作与数据安全保密协议，这些公司会严格遵守我们的数据隐私和安全要求。为使您可以更好地了解原力金智【FinAuth（示例）】SDK 收集的数据类型及用途，以及保护个人信息的方式，
您可以访问并查阅FinAuth个人信息与隐私保护政策FinAuth个人信息与隐私保护政策（示例）。
”

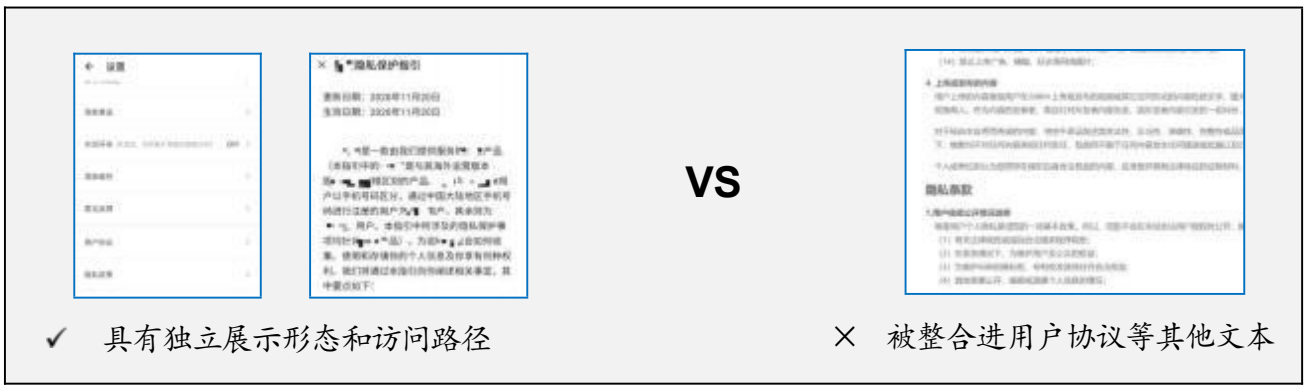
2) 表格形式向终端用户明示（此种方式下您与原力金智等第三方服务商之间的协议约定应单独表述）

第三方SDK 提供方	第三方SDK 名称与版本号	使用目的	涉及的数据类型	原力金智 SDK/API 隐私政策链接
原力金智（北京）科技有限公司	FinAuth（示例）SDK V0.1	用于提供人脸验证功能 （示例）	面部图像特征 （示例）	FinAuth个人信息与隐私保护政策FinAuth个人信息与隐私保护政策（示例）

1.4 App 隐私政策的展示方案

您应遵从国家相关法律法规、政策及标准的要求，对App 隐私政策进行展示。

您应当保证隐私政策的独立性和明显提示性。隐私政策应单独成文，而不是用户协议或其他文件的一部分（如下图所示）。App 首次运行时应通过弹窗等明显方式提示终端用户阅读隐私政策的收集使用规则，此后，再初始化SDK 或调用API 进行信息收集与处理。



您应当保证隐私政策的易读性和易访问性。隐私政策会使用明确易懂、符合逻辑与通用习惯的语言，并提供简体中文版。终端用户进入App主功能界面后，通过4次以内的点击或滑动，就能够访问到隐私政策。

您应向终端用户明示收集使用个人信息的目的、方式和范围，如果仅仅是改善服务质量、提升用户体验、定向推送信息、研发新产品等非终端用户使用 App 的必要目的为前提，不能成为强制用户同意收集其个人信息的理由。

隐私政策应由终端用户自主选择是否同意，不应以默认勾选同意的方式或是欺骗诱导的方式取得终端用户授权。

1.4 如果终端用户不希望其个人信息被处理或提出其他请求，应当如何应对？

首先，您应当充分了解，根据相关法律法规，终端用户享有多方面的个人信息相关权利。具体而言，在目前我国的生效法律法规（即《网络安全法》和即将生效的《民法典》）中，除最基本的知情同意权利以外，终端用户还拥有查阅复制权、更正删除权、受保密权等权益内容；而在《信息安全技术 个人信息安全规范》等相关文件中，还在法定权利之外，进一步提出了更为丰富的个人信息相关权益，包括但不限于撤回同意、注销账户、自动化决策的说明和拒受约束等。

按照现有法律要求，您应当告知终端用户其个人信息不希望被处理或其他请求的提出途径、联系方式，在收到终端用户的请求后及时核验终端用户身份，并及时进行相应处理。关于您如何响应和实现终端用户的行权请求，您可以参考《信息安全技术 个人信息安全规范》等相关文件；同时考虑到应对该等事件相对复杂，如您的确收到了类似的用户行权请求，我们建议您及时获取内部法务部门、外部法律顾问等专业人员的支持，以确保履行相关法定义务。

特别需要提醒您的是，您在使用原力金智 SDK/API 的过程中，如果终端用户在可行期限（视您使用的具体原力金智SDK/API 产品种类与约定，通常为您将终端用户个人信息提交给原力金智处理后的1 个月内） 内，提出了个人信息相关的行权请求，并且您已确定该等行权请求涉及到了您向原力金智提供的个人信息时，请及时通过本《指南》中公示的联系方式告知原力金智，按照以下格式说明具体信息，并附上必要的 书面证明材料。我们将及时核验相关材料，并按照相关法律法规，以及原力金智相关产品已对外公示的隐 私政策等法律文本中明确的规则，为您提供相应的支持与配合。如果终端用户未在上述可行期限内提 出个人信息相关的行权请求，因系统原因，该等终端用户的个人信息将被自动覆盖、删除或消除个人 身份标识，原力金智也将不再响应相关请求。请您务必理解，对于那些经原力金智确认认为不合法或不合理的、无端重复或需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益 带来风险或者非常不切实际（例如，涉及备份磁带上存放的信息）的请求，我们可能会予以拒绝。

（告知邮件内容示例）

（标题）请配合响应XXX 产品终端用户的【请明确权利类型】权利请求

（正文）

原力金智公司，

我公司是【请明确您的主体身份】。根据与原力金智的合作协议，我公司产品中集成/使用了原力金智

SDK/API，我公司目前收到终端用户请求，要求响应其个人信息权利，我司已确认用户身份和请求的真实性，经此邮件向原力金智提出配合请求，并确认自行承担此邮件请求引发的法律后果。

具体请求的相关信息如下：

1) 我公司产品：XXX【请明确具体的APP、网站等名称】
2) 涉及的原力金智 SDK/API：【请明确具体的原力金智SDK/API 名称】
3) 对应请求的：【request_id】
4) 涉及的数据范围：【请提供可供原力金智定位的具体信息，如2024 年12 月31 日下午 13 点31分经我司调用原力金智XXX API 而向原力金智传输的数据】
5) 用户提出的权利要求：【请明确权利类型、时间期限（如有）】
6) 需要原力金智提供的配合与支持：【请说明原力金智需要为您提供的配合和/或支持，如在业务系 统中删除涉及的图片与视频】

（附件）

1. （您的）主体身份证明，如营业执照副本等；

1.5 其它 SDK 合规说明

原力金智对原力金智 SDK/API 进行如下合规说明，如您在使用原力金智 SDK/API 的过程中对下述情形或其它任何情形有任何困惑，可以随时联系原力金智进行解释。

1）原力金智SDK/API 各项扩展业务功能介绍及对应关闭的配置方式：

针对 FinAuth SDK 活体以外的拓展业务功能：设备风险检测、活体采集的视频/图片在 SDK 留存、活 体界面是否显示并报读业务相关提示、活体过程中是否录屏留证；客户可以通过 FinAuth SDK 对应 的产品的控制台控制对应功能的开启、切换、关闭。

2）原力金智SDK/API 各项可选个人信息使用目的、场景及对应关闭的配置方式：

原力金智SDK/API 个人信息使用目的、场景详见各原力金智 SDK/API 官网展示的《隐私政策》（详见 1.5 条 4）项）； 如您不需要相关安全功能，具体可联系原力金智售后（联系方式：business@yljz.com）更换 降级版本。

3）原力金智SDK/API收集个人信息不同频次、精度使用目的、场景及对应选择的配置方式：

原力金智 SDK/API 个人信息的采集频率：您每调用一次原力金智 SDK/API 即进行一次采集；具体原力金智 SDK/API 的精度使用目的与场景详见各原力金智SDK/API 官网展示的《隐私政策》（详见 1.5 条4）项）； 如您要选择、更换相关配置方式，具体可联系原力金智售后（联系方式：business@yljz.com）进行选择 或更换获取降级版本。

4）原力金智SDK/API 所需的系统权限申请时机，及系统权限与各业务功能间的关系：

原力金智 SDK/API 启用阶段会进行权限授权以及相关的信息采集动作，系统权限与各业务功能间的关系 详见各原力金智 SDK/API官网展示的《隐私政策》，具体链接如下：

A) FinAuth 业务相关的SDK/API的《隐私政策》链接为：
https://assets.yljz.com/yljzopen/privacy-policy.html

5）原力金智SDK/API 初始化及各项业务功能接口合规调用时机，是否涉及第三方登录方式？

当您因业务需要调用原力金智 SDK/API 时，会触发原力金智 SDK/API 的启动，原力金智 SDK/API 启动后才会进行相关的接口交互与信息采集。不涉及第三方登录方式。

1.6 重要说明

如本《指南》引言部分所述，本部分合规要求的解读仅作为参考内容向您提供，不构成也不应被视为对任何法律法规、政策及标准的有权解释、法律意见或法律建议，亦不构成原力金智对外的任何承诺 与保证。除涉及原力金智自身相关事实信息以外，原力金智不对本《指南》中的任何规定本身及对规定理解的 时效性、准确性、正确性承担任何责任。您与您所具体开发、运营的App 是否达到或满足本《指南》 中所述的任何内容，不构成原力金智对前述App 合规性的担保或保证，您仍应独立对所开发、运营的App 合规性承担相关责任。在完整阅读本《指南》的基础上，我们仍强烈建议您充分了解现有及可能不时 发布、更新的有关个人信息保护的法律、法规、政策、标准和执法检查要求等。

2. 您使用原力金智能力时的合规注意事项

2.1 您使用原力金智能力前的合规自查

您在下载原力金智 SDK、调用原力金智API前，应当仔细阅读原力金智官网所公示的相关服务协议及隐私政策（或同样性质的类似法律文件），并依据您的App 产品收集使用个人信息的情况进行合规自查。

您应至少确保在 App 首次运行时通过明显方式提示终端用户阅读您的隐私政策并取得终端用户的合法授权，请您知悉，原力金智提供给您服务的前提是您已经：

1) 获得终端用户充分必要的授权、同意和许可，尤其是涉及到人脸数据等生物识别特征时的明示、单独同意（若您的App是针对不满十四周岁的儿童设计和开发的，您应已采取必要的技术措施，保证已获得其监护人的授权、同意和许可）；

2) 遵守并将持续遵守适用的法律、法规和监管要求，包括但不限于制定和公布有关个人信息保护的相关政策；

3) 向终端用户提供易于操作的选择机制，说明终端用户如何以及何时可以行使选择权，并说明行使选择权后如何以及何时可以修改或撤回该选择；

4) 向终端用户提供可行、便捷的个人信息相关权利行使方式。

2.2 原力金智对您的合规审查

原力金智作为服务提供者已在与您达成的服务协议中明确各方的安全责任和义务，原力金智已通过官方 网站公示自身产品与能力所适用的隐私政策，其中明确说明了收集终端用户信息的范围及使用目的。 您被明确要求，您应保证通过集成原力金智 SDK 或调用原力金智 API 而向原力金智提供的终端用户数据来源合 法，明确告知最终用户其被收集的数据内容、目的及且具备一定的必要性，获得最终用户的相应授权。

请您知悉，为确保您切实获得终端用户的授权，且您已满足上述的明确要求，原力金智将可能视具体 情况，在双方订立协议、开展合作前，对您进行必要的数据合规尽职调查与风险评估，包括但不限于：
1）要求您提供所共享的个人信息的合法来源证明，2）查阅您官网及其他公开渠道可获取的用户协议/服务条款与隐私政策等文本文件，3）试用您的 App 以审查同意授权与告知机制等。如原力金智发现存 在不合规情形，您可能会被要求增加或补充相关合规措施。请您知悉，该等尽职调查与风险评估纯粹 属于原力金智内部必要的合规程序，不构成任何形式的承诺与保证，不具有对外部相对方的法律效力。

2.3 重要说明

如本《指南》引言部分所述，本部分合规要求的解读仅作为参考内容向您提供，不构成也不应被视为对任何法律法规、政策及标准的有权解释、法律意见或法律建议，亦不构成原力金智对外的任何承诺 与保证。除涉及原力金智自身相关事实信息以外，原力金智不对本《指南》中的任何规定本身及对规定理解的 时效性、准确性、正确性承担任何责任。您与您所具体开发、运营的App是否达到或满足本《指南》中所述的任何内容，不构成原力金智对前述App合规性的担保或保证，您仍应独立对所开发、运营的App合规性承担相关责任。在完整阅读本《指南》的基础上，我们仍强烈建议您充分了解现有及可能不时 发布、更新的有关个人信息保护的法律、法规、政策、标准和执法检查要求等。

3. 原力金智的数据安全保护能力

原力金智不仅专注于技术实践积累、完善产品服务，同时也在积极践行个人信息与公共数据的保护， 严格遵守国家的法律法规、政策与标准。

3.1 原力金智的数据安全保护措施

原力金智非常重视个人信息保护，并在数据生命周期的各个不同阶段都采取了不同的措施来保障个人信息的安全。

1）数据采集安全

在不同的业务场景下，原力金智可能与客户开展多种多样的业务合作。通常而言，原力金智将作为个人信息处理者，与客户、供应商等合作伙伴一道，确保所收集和处理的个人信息满足授权同意的前提，且所使用、保留的个人信息均是业务流程的实现是必要的。

2）数据传输安全

原力金智已建立内部数据分类分级制度，并在传输前对不同的数据设置不同的数据保密等级，从而采用不同的加密方式，如sha-256 、密钥加密等。原力金智根据内外部数据传输要求，采用适当措施（如 HTTPS 协议）来保障传输的通道、节点和数据的安全，防止数据在传输过程中泄露。

3）数据存储安全

原力金智在业务实践中可能根据您已获得的用户授权，视您的独立决策而存储数据（比如来自于您的调用记录等），并根据不同的数据密级应用不同的安全存储机制，如加密存储、隔离存储等。此外，原力金智严格控制数据访问权限，并留存数据访问审计日志以追溯操作记录，防止人为的数据泄露。请您知悉并理解，由于业务性质和数据的敏感性，为保护用户个人信息与隐私安全，FinAuth业务中所涉及的用户身份数据和生物识别特征数据将不会留存。

4）数据处理与使用安全

个人信息进入原力金智系统后，原力金智会在可行情况下，严格按照法律法规的要求以及内部管理要求进 行脱敏和去标识化处理，以兼顾数据可用性和安全性。

原力金智严格遵守相关法律法规、与客户约定及终端用户的明确授权，确保原力金智的数据使用行为具有 合理、正当的法律基础，不侵犯第三方的合法权益。

5）数据销毁安全

原力金智会针对不同类型的业务数据制定不同的数据存储周期策略和数据老化策略，防止因对储存媒体重大数据进行恢复而导致的数据泄露。同时，原力金智还会定期安排人员对储存介质进行物理摧毁，通过建立有效的数据销毁规程与技术手段，以防止数据泄露的风险。

3.2 原力金智的数据安全保护机制

原力金智从不同的维度建立了数据安全保护机制来保障数据安全，并根据法律法规的政策性变化不 断完善内部的合规制度。

1）组织与管理

原力金智要求每位员工入职前均应签署保密协议（NDA），并严格控制第三方的访问和外包服务，分析安全影响并制订相应措施。

2）物理与环境安全

原力金智的关键网络与设施被放置在安全区域内，由设计的的安全边界予以保护。针对不同的安全区域，采取了不同等级的安全防护和访问控制措施，阻止非法访问和恶意干扰。

3）运行维护安全

原力金智建立了网络管理和操作制度流程，并尽可能地实现职责分离。原力金智部署了合理有效的安全防护软件、数据防泄漏软件，并定期进行系统安全漏洞评估。此外，原力金智也制定了信息存储介质的管理制度和处置流程，特别加强对可移动存储介质和系统文档的管理。

4）访问控制

原力金智基于业务和安全需求，制定访问控制策略，以实现最小化授权的原则，并明确用户职责，加强用户访问控制管理和日志记录，并在公司的网络边界设置合适的接口，采取有效的用户和设备验证 机制，控制用户访问。

5）开发与维护

原力金智系统的开发遵循系统性的安全生命周期管理流程，严格执行开发流程管理，包括对开发、测试和生产环境的变更控制，以保证系统软硬件和数据的安全。

6）安全事件响应与安全审计

原力金智已制定个人信息安全事件应急机制，并会定期组织员工进行应急响应培训和应急演练，并遵 从国家法律及政策相关安全要求，定期检查网络与信息系统安全，检验安全政策和技术规范的执行情况。

3.3 原力金智的数据安全保护能力认证

原力金智的主要系统已获得网络安全等级保护2.0三级备案，原力金智已取得了 ISO 27001 和 ISO 27701 认证。