旷视 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》《信息安全技术 移动互联网应用程序（App）SDK安全指南》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提供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。

为帮助使用旷视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、认识旷视提供的 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《旷视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、调用旷视API能力的开发者和运营者，本《指南》中适用于旷视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，均为旷视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，亦不构成旷视对外的任何承诺与保证。除涉及旷视自身相关事实信息以外，旷视不对本《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，不构成旷视对前述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@megvii.com 与旷视联系：

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、使用旷视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旷视可能提出的审查要求；

3、旷视的数据安全保护能力，主要向您介绍了旷视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 过程中需要使用旷视 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 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，以及您与旷视、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 中部署旷视 SDK 收集使用个人信息的目的、类型、方式和范围等，并提供符合法律法规要求、您与旷视之间约定的保护标准。

1.2 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，您谨慎地选择了旷视作为合作方，并委托旷视加工和处理终端用户的相关个人信息。

旷视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旷视 SDK 的相关情况（以下示例不代表真实业务情况），如您需要对外披露旷视的数据安全能力，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旷视 SDK/API 的必要信息，请联系旷视相应人员：

1）表格形式向终端用户明示（此种方式下您应逐个、单独列明旷视等第三方 SDK 服务商）

SDK 名称	SDK 命名空间	合作伙伴名称	合作目的	收集个人信息字段	申请的权限	SDK 隐私政策
SDK 对外产品名称	SDK 的命名空间	公司名称	APP 集成 SDK 后，SDK 提供的服务功能描述	收集的个人信息的字段及其对应的目的	申请的系统权限及其对应的目的	SDK 隐私政策链接

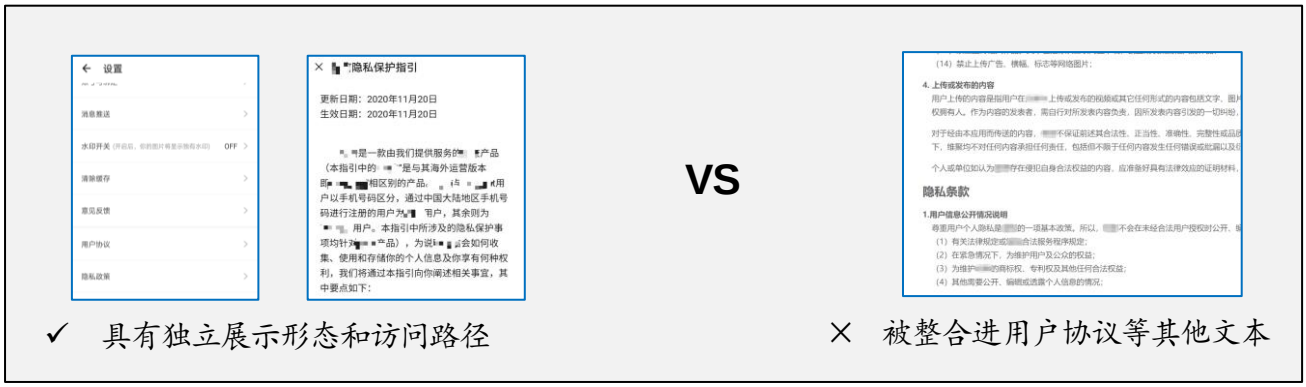
2）文字描述等方式向终端用户明示

如您不希望采用相关国家标准中推荐的方式逐个列出使用 SDK 的情况，您也可以通过文字描述等其他可用形式向终端用户进行明确告知。不过，请注意，您选择使用的其他可用形式（含文字描述等）所提供的信息及其可理解性应与表格形式相当。

1.3 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《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，您在使用旷视 SDK/API 的过程中，如果终端用户在可行期限（视您使用的具体旷视 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旷视处理后的 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旷视提供的个人信息时，请及时通过本《指南》中公示的联系方式告知旷视，按照以下（告知邮件内容示例）的格式说明具体信息，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，以及旷视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，旷视也将不再响应相关请求。请您务必理解，对于那些经旷视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）

旷视公司，

我公司是【请明确您的主体身份】。根据与旷视的合作协议，我公司产品中集成/使用了旷视 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，经此邮件向旷视提出配合请求，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) 涉及的旷视 SDK/API：【请明确具体的旷视 SDK/API 名称】
3) 对应请求的：【request_id】
4) 涉及的数据范围：【请提供可供旷视定位的具体信息，如 2020 年 12 月 31 日下午 13 点 31 分经我司调用旷视 XXX API 而向旷视传输的数据】
5) 用户提出的权利要求：【请明确权利类型、时间期限（如有）】
6) 需要旷视提供的配合与支持：【请说明旷视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；
2. 与旷视的合作协议副本，线上开通服务的可不提供；
3. 用户身份确认的证明材料，如与用户沟通、向用户确认身份的书面记录截图等；

1.5 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，亦不构成旷视对外的任何承诺与保证。除涉及旷视自身相关事实信息以外，旷视不对本《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，不构成旷视对前述 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、您使用旷视能力时的合规注意事项

2.1 您使用旷视能力前的合规自查

您在下载旷视 SDK、调用旷视 API 前，应当仔细阅读旷视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，旷视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 旷视对您的合规审查

旷视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，旷视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，您应保证通过集成旷视 SDK 或调用旷视 API 而向旷视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，旷视将可能视具体情况，在双方订立协议、开展合作前或合作过程中，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。如旷视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，如您未按时增加或补充，旷视有权拒绝您使用服务。请您知悉，该等尽职调查与风险评估纯粹属于旷视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，亦不构成旷视对外的任何承诺与保证。除涉及旷视自身相关事实信息以外，旷视不对本《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，不构成旷视对前述 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、旷视的数据安全保护能力

旷视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。旷视在开发 SDK 时注重安全性，尽最大努力保障 SDK 不存在安全漏洞，并不会从事广告刷量、隐私窃取、远程控制等恶意行为。

3.1 旷视的数据安全保护措施

旷视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，旷视可能与客户开展多种多样的业务合作。通常而言，旷视将作为个人信息处理者，与客户、供应商等合作伙伴一道，确保不会超授权范围处理用户个人信息，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

旷视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-1、密钥加密等。旷视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

旷视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，旷视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。特别的，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，FaceID 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

个人信息进入旷视系统后，旷视会在可行情况下，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。

旷视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，确保旷视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

旷视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，旷视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 旷视的数据安全保护机制

旷视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

旷视要求每位员工入职前均应签署保密协议，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

旷视的关键或敏感网络与设施被放置在安全区域内，由指定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，阻止非法访问和干扰。

3）运行维护安全

旷视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。旷视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，旷视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

旷视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

旷视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

旷视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 旷视的数据安全保护能力认证

旷视的主要系统已获得网络安全等级保护三级备案，旷视已取得了 ISO 27001 和 ISO 27701 认证。