# 数据处理协议

## 1. 背景信息

1.1. 鉴于旷视与使用 FaceID 服务的客户和/或使用 Face++人工智能开放平台开发服务的开发者（下称“客户”）双方之间已达成关于 FaceID 服务和/或 Face++服务（下称“旷视服务”或“服务”）的采购和提供的合作协议（下称“主合同”），本数据处理协议是纳入主合同约定，构成主合同条款不可分割的一部分。

1.2. **范围与生效。**本数据处理协议适用于旷视包括其子受托人（如有）与提供旷视服务有关的数据处理（下称“数据处理”）。本数据处理协议无需单独签署，双方一经签署主合同，即同时认可并接受本数据处理协议中相关约定之约束。

1.3. **结构。**附录部分纳入本数据处理协议，并构成本数据处理协议的一部分。其中，附录 1 规定了处理的性质、指示和目的，和涉及的个人信息、数据主体类别、期限；附录 2 明确了旷视在本数据处理协议下提供的、技术和组织层面的安全保障措施。

1.4. **管理。**在本数据处理协议项下，客户是本数据处理协议项下处理的个人信息委托人，旷视是本数据处理协议项下受托处理的个人信息的受托人，客户全权负责对旷视需要执行的数据处理行为所需获得的批准、授权和许可。

1.5. **术语和定义。**

1) “适用数据保护法”是指中国的个人信息、隐私权保护、网络安全及通信领域的法律法规，且该等法律法规对数据保护已有规定，包括但不限于《个人信息保护法》、《数据安全法》、《网络安全法》、《民法典》等。
2) “个人信息”是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。
3) “数据主体”是指个人信息识别或关联到的自然人。
4) “处理者”是指单独或共同决定数据处理的目的和/或方式的主体，在本协议中指客户。
5) “受托人”是指基于处理者委托、以处理者名义开展数据处理的主体。
6) “数据保护机构”是指适用数据保护法下依法履行数据保护监管职责的机构。
7) 适用数据保护法中对个人信息、数据主体、处理者、受托人、数据保护机构等的具体含义和表述另有特别规定的，本数据处理协议项下的术语同时具有适用数据保护法下所规定的具体含义。

## 2. 处理安全

2.1. **相应技术措施和组织措施。**

1) 旷视已根据当前技术发展水平，实施了主合同项下服务适用的技术措施和组织措施保护数据处理安全，具体参见*数据处理协议附录 2 – 安全措施*。
2) 客户已查看此类措施并同意，考虑目前的技术发展水平、实施成本，以及数据处理性质、范围、背景和目的，旷视正采取的相应措施是恰当的。

2.2. **变更。**旷视不得擅自调整、变更所采取的技术和组织措施，尤其是当可能降低本数据处理协议项下数据处理过程中所提供的安全保护等级时；在维持相当或更高的安全保护水平的情况下，旷视可进行变更且无需另行通知客户。

**3. 双方的一般责任**

3.1. 客户承诺并保证：

1) 客户基于本数据处理协议拟委托旷视进行的处理行为遵循合法、正当、必要和诚信原则，已具备基本的合法性基础；适用取得个人同意为本数据处理协议项下的合法性基础时，客户进一步承诺并保证已向数据主体（即客户提供的产品和/或服务的最终用户）充分说明个人信息收集及使用的目的、范围和方式，且客户已将授权内容在相应文件中进行约定并已经取得数据主体的书面同意和授权，授权包括但不限于：a) 数据主体知悉并同意客户收集其使用服务所需的个人信息，包括姓名，身份证号码与照片等身份证信息，人脸照片及视频，驾驶证、行驶证及银行卡信息，证件芯片加密的文本信息（如姓名、证件号码等）及人脸照片，应用、设备及网络信息，并由客户将前述个人信息提供给旷视；b) 数据主体知悉并同意旷视有权获得其个人信息，用于主合同所述服务，并向客户返回识别结果。c）必要时，旷视有权将数据主体的个人信息提供至必要服务商，用于主合同所述服务。
2) 如客户为持牌的金融类客户（包括但不限于银行、互联网支付企业、小额贷款企业等）或客户使用本服务从事助贷业务时，客户知悉并确认，旷视可基于FaceID服务日志，向依法运营的个人征信机构（即朴道征信有限公司）提供分析产品，用于其开展个人征信业务之目的。旷视应遵守相关法律要求，避免分析产品中涉及个人的宗教信仰、基因、指纹、血型、疾病和病史信息以及法律、行政法规规定禁止涉及的信息；客户应当依法向用户本人取得前述目的所需的授权同意，授权内容应包括：数据主体使用旷视的FaceID服务日志及日志加工成的分析产品将由旷视提供至依法运营的个人征信机构（即朴道征信有限公司），以便在产生数据主体本人信贷业务时，朴道征信有限公司查询、采集、获取并加工使用、保留数据主体的相关个人信用信息，用于开展个人征信业务之必要目的。
3) 如客户采用格式条款方式进行前述告知并取得数据主体授权同意的，应保证所使用的授权格式条款符合适用数据保护法要求，保障数据主体合法权益，确保取得合法有效、完整充分的授权同意。

3.2. 旷视承诺并保证，在代表客户处理个人信息时：

1) 向客户提供的旷视服务符合中国法律法规要求；涉及个人信息的，符合适用数据保护法的要求。
2) 根据客户以书面形式作出的指示处理个人信息，并严格落实本数据处理协议第2.1条所述的相应技术和组织措施。
3) 确保为履行旷视在本数据处理协议项下的义务，同时确保以保密协议等书面形式约束旷视相关员工严格按照本数据处理协议的约定执行相关数据处理。
4) 遵守适用数据保护法中对受托人的强制性义务及要求。

**4. 指示**

4.1. 客户明确授权，在本数据处理协议项下，旷视应履行的数据处理指示如以下*数据处理协议附录 1 - 个人信息处理指示*所示。除法律另有规定外，在代表客户处理个人信息时，旷视应且仅应根据本数据处理协议进行。

4.2. 在本数据处理协议生效期间，客户可通过书面形式告知旷视，以变更本数据处理协议第 4.1 条所述的指示。除本数据处理协议中规定的其他通知义务之外，如果旷视

认为任何指示违反了适用数据保护法（“被质疑的指示”），旷视在收到客户根据本条发出的书面告知之日起三个工作日内可以书面通知客户，并在通知中指明可能违反的适用数据保护法要求；在客户对被质疑的指示进行确认之前，旷视无需执行该被质疑的指示。

**5. 数据安全事件**

5.1. 如果发生数据安全事件（含个人信息泄露），应客户要求，旷视应及时按照适用数据保护法向客户提供必要的相关信息，法律法规或生效司法执法指令明确禁止的除外。

5.2. 数据安全事件发生后，在商业合理的范围内，应客户要求，旷视可向客户提供相关协助，以使客户履行客户在适用数据保护法中应当承担的通知数据主体和报告数据保护机构的义务。

5.3. 旷视向客户提供第 5.2 条中的协助所发生的一切合理费用，由客户承担。如客户对该等费用有疑问，应当以书面形式向旷视告知并与旷视进行协商。

**6. 响应数据主体的请求**

6.1. 根据客户的要求，旷视在技术可行、合理的范围内，根据适用数据保护法协助客户对数据主体的请求作出响应。客户应负责确认数据主体是否有权行使任何该等权利，并书面向旷视明确需要进行协助的范围与形式。

6.2. 旷视向客户提供第 6.1 条中的协助响应而产生的合理费用，由客户承担。如客户对该等费用有疑问，应当以书面形式向旷视告知并与旷视进行协商；但客户不得以此为依据，迟延向旷视支付该等费用；如客户拒绝或延迟支付该等费用的，旷视可根据情况自行决定中止或终止向客户提供第 6.1 条下的协助。

**7. 对外共享与全球性处理**

7.1. 未经客户的事先书面同意并采取适用数据保护法下必要的合规措施，旷视不得将主合同项下的任何个人信息向其他第三方共享。

7.2. 客户同意并认可，旷视将基于全球分布的基础设施提供旷视服务，并开展本数据处理协议项下的数据处理；旷视可视具体情况合理调整该等基础设施分布，且无需另行通知客户，但如果旷视对基础设施的调整影响客户正常使用旷视服务，应及时告知客户并与客户协商。目前旷视的基础设施在全球分布情况如下：

**1) Face++平台及相关服务：服务器位于中国和加拿大。**

**2) FaceID平台及相关服务：服务器位于中国、新加坡、印度尼西亚和日本。**

7.3. 客户明确授权并认可，旷视应按照以下规则在相关地区内开展本数据处理协议项下的数据处理：

**1) 涉及在中国境内收集和产生的个人信息，原则上将在中国境内的基础设施上处理；**

**2) 对于中国境外的旷视服务，客户自行决定支持的旷视基础设施，旷视按照客户选择在当地开展数据处理。**

7.4. 除法律另有规定或客户另行书面提出要求，按照第 7.3 条所述规则确定数据处理开展的地区后，旷视不得将本数据处理协议项下的个人信息传输至未经客户授权同意的其他国家和/或地区。

7.5. 客户应自行履行适用数据保护法下被有效实施和/或不时更新的数据跨境传输限制（如有），并且确保采取了适当的防范措施。确有必要的，经客户书面请求，旷视可视情况向客户提供必要的协助，以使其遵守适用数据保护法的相关，该等必要协助所发生的合理费用应由客户承担。

**8. 子处理**

8.1. 客户特此书面授权同意，旷视可根据具体需求情况，将本数据处理协议项下规定的数据处理全部或部分地委托给其他第三方（含旷视关联企业及其他经旷视明确书面授权的合作伙伴，下称"子受托人"）。

8.2. 在满足其他条件的前提下，旷视在选择子受托人时应尽合理商业努力，并特别注意它在执行数据处理业务方面的信誉和经验，以及它的技术和组织措施的适当性。

8.3. 旷视应当与子受托人签订协议，并且该等协议应当（i）对需要子受托人处理个人信息的分包服务进行描述（包括处理的个人信息类型及处理目的）；以及（ii）对子受托人必须执行的适用于该分包服务的技术和组织措施进行描述。

**9. 通知**

9.1. 除非适用数据保护法明确禁止，旷视应及时通知客户如下内容：

1) 旷视处理个人信息期间发生的：(i) 任何违反本数据处理协议任何条款的情况；和/或(ii) 任何违反客户根据本数据处理协议发出的任何指示的情形；
2) 数据保护机构针对旷视进行的数据处理有关的任何正式监管执法程序，以及在客户要求的情况下，针对客户的审查和/或程序中数据保护机构可能需要旷视提供的支持和协作；
3) 阻止旷视按照本数据处理协议及指示中的目的、方式和范围处理任何个人信息的法定或事实情形；及
4) 影响旷视实施的技术性和组织性安全措施的任何重大变化，该等变化会使旷视实施的技术性和组织性安全措施无法满足本数据处理协议项下旷视的个人信息安全义务。

9.2. 如旷视查明或事实证明以下情形，旷视应向客户发出书面通知：

1) 旷视代表客户处理的个人信息已被非法传输；
2) 第三方已非法获得访问该等个人信息的能力；和/或
3) 个人信息的完整性或保密性以任何其他方式受到重大损害。

9.3. 如果旷视收到数据主体或第三方的投诉和/或要求提供关于数据处理的具体信息，旷视应及时将该等投诉和/或问询以及相关材料书面转交客户。

**10. 违约责任**

10.1. 如果任何一方违反适用数据保护法或者本数据处理协议的义务，应当根据主合同承担相应的责任；如果主合同或者本数据处理协议中没有相关规定，则应当按照适用数据保护法承担责任。

10.2. 即使主合同确定或者由于其他原因适用的责任条款出现减损，由于任何一方违反个人信息保护义务而产生的或者与其有关的任何责任也仅受本数据处理协议的管辖。

**11. 一般规定**

11.1. **转让。**未经另一方的书面同意，任何一方均不得转让它在本数据处理协议项下的任何权利或者义务。

11.2. **可分性。**本数据处理协议中不可执行的条款将会并且仅在使这些条款可以执行的必要范围内被修改，以反映双方当事人的意图。其他条款将仍然继续有效，而不会进行任何修改。

11.3. **期限和终止。**本数据处理协议中的义务在主合同终止后继续有效，且在旷视（包括旷视在本数据处理协议项下委托的子受托人）终止代表客户处理个人信息前应充分有效。

**数据处理协议附录 1 - 个人信息处理指示**

**处理者**

- 客户。

**受托人**

- 旷视及其子受托人（含旷视关联企业及其他经旷视明确书面授权的合作伙伴，如适用）。

**数据主体**

- 指客户视其具体需求而使用旷视服务过程中涉及到相关个人信息的被采集方，包括客户的最终用户和/或雇员等。

**数据类别**

- 涉及的数据类型包括但不限于：身份信息（如姓名、性别），证件信息（如身份证件及相关信息），图片、视频和音频信息（如关于人脸、肢体动作、服饰），应用、设备及网络信息，以及其他在具体项目下客户明确提出的数据类型。

**处理操作/目的**

- 旷视被指示开展的数据处理操作包括为提供主合同或特定订单项下旷视服务而必须的数据处理行为，以及旷视为履行法定义务和主合同项下合同约定而开展的数据处理行为；
- 旷视开展数据处理操作的目的应仅限于主合同项下所明确的范围，具体而言：1）提供旷视服务之必要；2）用于安全防范、反欺诈；3）履行法律法规规定义务之必要；4）与国家安全、国防安全直接相关；5）与公共安全、公共卫生、重大公共利益直接相关；6）与刑事侦查、起诉、审判和判决执行等直接相关；7）维护旷视服务的安全稳定运行之必要；8）在合法前提下优化升级旷视服务之必要。

**处理期间**

- 旷视接受客户委托开展本数据处理协议项下所涉及的数据处理操作的期间限于旷视履行主合同（含特定订单及本数据处理协议等附件）项下全部义务的期限；
- 无论旷视是否全部履行主合同项下义务，在本数据处理协议项下所涉及的数据被妥善删除和/或返还客户（视客户要求）前，旷视作为受托人在本数据处理协议项下的相关义务持续有效，但旷视前述相关义务的有效期最长不长于旷视全部履行主合同项下义务后 6 个月。

**数据处理协议附录 2 – 安全措施**

**A. 物理访问控制。**

措施：

- 基于旷视安全政策采用相应的措施保护其资产和设施。
- 保障办公场所所在建筑物的安全，如采用智能卡门禁系统。
- 根据安全等级，可采用其他措施进一步加强场所访问安全，包括视频监控及生物识别门禁系统。
- 访问权限会依据系统和数据访问控制措施授予获得授权的个人。该措施同样适用于访客访问。
- 旷视员工和外部员工在所有旷视场所都应佩带自己的身份卡。

针对数据中心/服务器的额外措施：

- 所有数据中心/服务器都应遵守严格的安全流程，如安装防护装置、监控摄像头等。
- 仅授权代表有权访问数据中心/服务器设施中的系统和基础架构。
- 为保障数据中心/服务器的正常运行，会定期对物理安全设备（如移动传感器、摄像头等）进行维护。
- 旷视自有和所使用的第三方数据中心/服务器提供商应确保记录进入旷视专属区域的授权人员的身份和时间。

**B. 系统访问控制。**

措施：

- 设置访问敏感系统的不同权限，并根据旷视政策的流程加以管理。
- 所有人员使用唯一标识（用户标识）访问旷视的系统。
- 设定相应程序，依照旷视政策管控权限变更。如人员离开公司，其访问权限会被撤销。
- 禁止共享密码，并要求定期更改密码和更改默认密码。
- 公司网络通过防火墙等技术方案与公共网络隔离。

**C. 数据访问控制。**

措施：

- 作为旷视政策的一部分，个人信息至少需要达到旷视数据分类分级标准中与保密信息同等的保护级别。
- 采用权限概念，说明授予流程和每个账户所分配的角色（用户标识），并按照最小必需的原则授予访问个人信息的权限。
- 定期检查安全措施，保护处理个人信息的应用程序。
- 旷视政策已规定数据和数据载体的销毁机制。

**D. 数据传输控制。**

措施：

- 在旷视与其客户之间传输数据时，双方商定针对所传输个人信息的保护措施。这一点同样适用于物理数据传输和网络数据传输。
- 旷视应对旷视控制系统之内的任何数据传输负责。

**E. 作业控制。**

措施：

- 旷视采用控制和流程，确保遵守旷视与其客户、子受托人等主体之间签署的合同。
- 所有旷视员工、子受托人和/或其他服务提供商均受合同约束，遵守所有敏感信息（包括旷视、客户和合作伙伴的商业秘密）的保密性。

**F. 完整性与可用性控制。**

措施：

- 旷视采用定期备份流程，确保在必要时快速恢复关键业务系统。
- 旷视针对关键业务流程制定了业务应急计划，并为关键业务服务提供灾难恢复战略，并不时测试。

**G. 数据隔离控制。**

措施：

- 旷视利用现有可用技术实现客户的个人信息的隔离保存。
- 客户只能访问自己的数据。