Annex II: Data Processing Agreement

1. Background Information

1.1. **Whereas** Party A and Party B have entered into or intend to enter into a cooperation contract (hereinafter referred to as the "Master Contract") regarding the procurement and provision of specific products and/ or services (hereinafter referred to as "Party B's services"), this data processing agreement is incorporated into the Master Contract and becomes an integral part of the Master Contract.

1.2. **Scope and Effectiveness.** This data processing agreement is applicable to the data processing related to the provision of Party B's services (hereinafter referred to as "data processing") carried out by Party B, including its sub-processors (if any). It is unnecessary to separately sign this data processing agreement. Upon signing the Master Contract, both parties agree to be bound by relevant provisions in the data processing agreement.

1.3. **Structure.** The annexes are incorporated into this data processing agreement and form a part of this data processing agreement. Among them, Annex 1 sets forth the nature, instructions and purpose of the data processing, and the involved personal information, categories of data subjects and the term of the data processing, while Annex 2 specifies the technical and organizational security measures provided by Party B under this data processing agreement.

1.4. **Management.** Under this data processing agreement, Party A is the controller while Party B is the processor of the personal information processed hereunder, and Party A shall be solely responsible for maintaining the approval, authorization and permission for the data processing activities to be performed by Party B.

1.5. **Terms and Definitions.**

1) Applicable data protection laws; referring to the applicable laws and regulations in the fields of personal information, privacy protection, network security and communication in China or other relevant countries/ regions and such laws and regulations have provisions on data protection. If relevant country/ region does not have provisions on data protection through laws and regulations, the applicable data protection laws shall refer to the relevant requirements and principles for data protection in the constitution and other fundamental laws, regulations and systems of the country/ region.

2) Personal information; referring to information recorded electronically or otherwise, which can identify the identity of natural persons solely or in combination with other information, or relate to specific natural person.

3) Data subject; referring to the natural person identified or related to by the personal information.

4) Controller; referring to an entity that can solely or jointly determine the purposes and/ or means of data processing.

5) Processor; referring to an entity that carries out data processing on behalf of the controller based on the commission of the controller.

6) Data protection authority; referring to the authority that performs the supervision powers and duties of data protection under the applicable data protection laws.

7) Where the applicable data protection laws have other special provisions on the specific meaning and expression of personal information, data subject, controller, processor, data protection authority, etc., these terms under this data processing agreement shall also have the same meanings specified in the applicable data protection laws.

2. Security of Processing

2.1. **Technical and Organizational Measures.**

1) According to current technological development level, Party B has implemented the technical and organizational measures applicable to the services under the Master Contract to ensure the security of the data processing. See ***Error! Reference source not found.*** for details.

2) Party A has checked such measures and agrees that the measures taken by Party B are appropriate, taking into account current technological development level, implementation costs, as well as the nature, scope, background and purpose of the data processing.

2.2. **Change.** Party B shall not adjust or change the technical and organizational measures taken without permission, especially when such adjustments or changes may reduce the security protection level of the data processing hereunder. Party B may make changes without separately informing Party A if it can maintain the same or higher level of security protection.

3. General Liabilities of the Two Parties

3.1. Party A undertakes and warrants that:

1) Party A has fully explained to the data subjects (i.e., the end users of the products and/ or services provided by Party A) the purposes, scope and means of the collection and use of personal information, and Party A has specified the authorization content in relevant documents and has obtained the written consent and authorization of the data subjects. The authorization includes but is not limited to that: a) The data subject understands and agrees that Party A collects its personal information, including but not limited to its ID photo, face photo, video and other relevant information required for the technical services, and Party A will provide such personal information to Party B; b) The data subject understands and agrees that Party B has the right to obtain its personal information for the comparison and identification services set forth in the Master Contact and will return the identification results to Party A.

2) If Party A adopts standard terms to inform the data subjects of the items above and obtain the consent and authorization of the data subjects, Party A shall ensure that the standard terms used comply with the requirements of applicable data protection laws so as to protect the legitimate rights and interests of the data

subjects and ensure the consent and authorization obtained is legal, effective, complete and sufficient.

3.2. Party B undertakes and warrants that when processing personal information on behalf of Party A:

1) The services provided by Party B to Party A comply with the laws and regulations of China and/ or other relevant countries/ regions that may be involved. Where personal information is involved, the requirements of applicable data protection laws shall be complied with.

2) The personal information will be processed in accordance with the instructions given in writing by Party A, and corresponding technical and organizational measures set forth in Article 2.1 hereof will be strictly implemented.

3) Party B will fulfill its obligations under this data processing agreement and adopt confidentiality agreement or other written forms to bind Party B's employees to perform data processing in strict accordance with this data processing agreement.

4) The mandatory obligations of and requirements for the processor under applicable data protection laws will be followed.

4. Instructions

4.1. Party A expressly authorizes Party B to perform the data processing instructions under this data processing agreement as shown in ***Error! Reference source not found.***. Except as otherwise provided by law, Party B shall and shall only process personal information on behalf of Party A in accordance with this data processing agreement.

4.2. During the effective period of this data processing agreement, Party A may notify Party B in written form to change the instructions set forth in Article 4.1 hereof. In addition to the notification obligations of Party B set forth herein, if Party B considers that any instruction violates the applicable data protection laws ("challenged instruction"), Party B may notify Party A in writing within three (3) working days upon receipt of a written notice from Party A under this article, and Party B shall specify the requirements of the applicable data protection laws that may be violated in the notification. Before Party A confirms the challenged instruction, Party B should not execute the challenged instruction.

5. Data Security Incident

5.1. In case of a data security incident (including personal information leakage), Party B shall, at the request of Party A, promptly provide Party A with necessary information in accordance with the applicable data protection laws.

5.2. If a data security incident occurs, Party B may, to the extent that it is commercially reasonable and at Party A's request, assist Party A to fulfill its obligation to notify the data subjects and report to the data protection authority under the applicable data protection laws.

5.3. All reasonable expenses incurred by Party B in providing assistance to Party A in Article 5.2 shall be borne by Party A. If Party A has any doubt about such expenses, it shall inform Party B in writing and negotiate with Party B.

6. Response to Request of Data Subject

6.1. Upon request of Party A, Party B shall, to the extent that it is technically feasible and reasonable, assist Party A to respond to the request of the data subject in accordance with the applicable data protection laws. Party A shall confirm whether the data subject has such right and shall make clear to Party B in writing the scope and form of the assistance.

6.2. All reasonable expenses incurred by Party B in assisting Party A to respond to the request of the data subject in Article 6.1 shall be borne by Party A. If Party A has any doubt about such expenses, it shall inform Party B in writing and negotiate with Party B. However, Party A shall not delay in paying such expenses to Party B with such reason. If Party A refuses or delays the payment of such expenses, Party B may, in its sole discretion, suspend or terminate the assistance provided to Party A under Article 6.1.

7. Data Sharing and Global Processing

7.1. Party B shall not share any personal information under the Master Contract with any other third parties without Party A's prior written consent and taking necessary compliance measures under the applicable data protection laws.

7.2. Party A agrees and acknowledges that Party B will provide services based on its globally distributed infrastructures and carry out the data processing under this data processing agreement. Party B may reasonably adjust the distribution of such infrastructures according to the specific situation without notifying Party A. However, if Party B's adjustment of the infrastructures will affect Party A's normal use of Party B's services, Party B shall timely inform Party A and negotiate with Party A. The present global distribution of Party B's infrastructures is as follows:

1) Face++ platform and related services: Servers are located in China and Canada.

2) FaceID platform and related services: Servers are located in China, Singapore, Indonesia and Japan.

7.3. Party A expressly authorizes and acknowledges that Party B shall carry out data processing under this data processing agreement in relevant regions in accordance with following rules:

1) The personal information collected and generated within the territory of China shall be processed on infrastructures within the territory of China in principle.

2) For Party B's services outside the territory of China, Party A shall decide the supporting infrastructures of Party B at its own discretion, and Party B shall carry out data processing locally with the infrastructures selected by Party A.

7.4. Unless otherwise stipulated by laws or otherwise required by Party A in writing, after the region for carrying data processing is determined according to the rules set forth in Article 7.3, Party B shall not transmit the personal information under

this data processing agreement to other countries and/ or regions not agreed by Party A.

7.5. Party A shall be responsible to comply with the restrictions (if any) on the cross-border transmission of data effectively enforced and/ or updated from time to time under applicable data protection acts and ensure that appropriate preventative measures have been taken. If necessary, at the request of Party A in writing, Party B may provide necessary assistance to Party A as appropriate to enable it to comply with applicable data protection laws. All reasonable expenses incurred in such assistance shall be borne by Party A.

8. Sub-processing

8.1 Party A hereby authorize in writing that, Party B may, according to the specific situations, wholly or partially entrust the data processing under this data processing agreement to other third parties (including Party B's affiliates and other partners expressly authorized in writing by Party B, hereinafter referred to as "sub-processors").

8.2 When selecting a sub-processor, Party B shall make reasonable commercial efforts on the premise of meeting other conditions and pay special attention to the sub-processor's reputation and experience in performing data processing business and the appropriateness of its technical and organizational measures.

8.3 Party B shall sign an agreement with the sub-processor, and such agreement shall (i) describe the subcontracted processing of personal information to be performed by the sub-processor (including the type of the personal information to be processed and the purpose of the processing); and (ii) describe the technical and organizational measures applicable to the subcontracting service to be implemented by the sub-processor.

9. Notifications

9.1. Unless expressly prohibited by applicable data protection laws, Party B shall promptly notify Party A of the followings:

1) During Party B's processing of personal information: (i) any violation of any provisions of this data processing agreement; and/ or (ii) any violation of any instructions given by Party A according to this data processing agreement;

2) Any formal regulatory enforcement procedures related to the data processing conducted by the data protection authority against Party B, and the support and coordination of Party B that may be required by the data protection authority against Party A's audit and/ or procedures at the request of Party A;

3) Legal or factual circumstances that prevent Party B from processing any personal information according to the data processing agreement and the purposes, means and scope required in the instructions; and

4) Any significant changes that affect the technical and organizational security measures implemented by Party B, if such changes will make the technical and organizational security measures implemented by Party B lead to the result that

Party B fails its personal information security obligations under this data processing agreement.

9.2. Party B shall send Party A written notice if Party B finds out or proves the following circumstances:

1) The personal information processed by Party B on behalf of Party A has been illegally transmitted;

2) A third party has illegally obtained the ability to access such personal information; and/or

3) The integrity or confidentiality of personal information is materially damaged in any other forms.

9.3. If Party B receives complaints and/ or requests for specific information about data processing from the data subject or a third party, Party B shall promptly transmit such complaints and/ or inquiries and relevant materials to Party A in writing.

10. Responsibility for Breach of the Agreement

10.1. If either party breaches its obligations under the applicable data protection laws or this data processing agreement, it shall bear corresponding liabilities under the Master Contract. If the Master Contract or the data processing agreement does not have such provisions, it shall bear corresponding liabilities under the applicable data protection laws.

10.2. Even though the Master Contract has such provisions or applicable liability clauses have derogation due to other reasons, any liability arising out of or in connection with a breach of the personal information protection obligation by either party shall be governed only by this data processing agreement.

11. General Provisions

11.1. **Transfer.** Neither party shall transfer any of its rights or obligations under this data processing agreement without the written consent of the other party.

11.2. **Separability.** The unenforceable provisions of this data processing agreement will be modified only to the extent necessary to make them enforceable, so as to reflect the intent of the parties. Other provisions will remain in effect and will not be modified.

11.3. **Term and Termination.** The obligations in this data processing agreement shall still survive after the termination of the Master Contract and shall be fully valid before Party B (including the sub-processor entrusted by Party B under this data processing agreement) terminates the processing of personal information on behalf of Party A.

Annex 1 of Data Processing Agreement - Personal Information Processing Instructions

Controller

- Party A.

Processor

- Party B and its sub-processor (including Party B's affiliates and other partners expressly authorized in writing by Party B, if applicable).

Data Subject

- The party to whom personal information is collected during Party A's use of Party B's services according to its specific needs, including Party A's end users and/ or employees.

Data Category

- The data categories involved include but are not limited to: identity information (such as name), identification information (such as identity documents and relevant information), picture, video and audio information (such as human face, body movements, clothing), and other data categories explicitly proposed by Party A under specific projects.

Processing Operation/ Purpose

- The data processing operations instructed to be performed by Party B include the data processing activities necessary for the provision of Party B's services under the Master Contract or specific orders, and the data processing activities conducted by Party B to fulfill its legal obligations and agreements under the Master Contract.

- The purposes of Party B's data processing operation shall be limited to the scope specified under the Master Contract, specifically, they are: 1) necessary for the provision of Party B's services; 2) used for security protection and anti-fraud; 3) necessary for performing the obligations stipulated by laws and regulations; 4) directly related to national security and national defense security; 5) directly related to public security, public health and major public interests; 6) directly related to criminal investigation, prosecution, trial and execution of judgment; 7) necessary for maintaining the safe and stable operation of Party B's services; and 8) necessary for optimizing and upgrading Party B's services on the premise of being lawful.

Processing Period

- The term during which Party B accepts Party A's commission to carry out the data processing operations under this data processing agreement is limited to the term during which Party B performs all its obligations under the Master Contract (including specific orders and annexes to this data processing agreement).

- No matter whether Party B fully performs its obligations under the Master Contract, before the data involved under this data processing agreement is

properly deleted and/ or returned to Party A (as required by Party A), relevant obligations under this data processing agreement of Party B as the processor shall continue to be valid. However, the term of validity of the aforementioned obligations of Party B shall not be longer than six months after Party B fully performs its obligations under the Master Contract.

Annex 2 Data Processing Agreement - Security Measures

A. Physical Access Control.

Measures:

• Relevant measures shall be taken based on Party B's security policies to protect assets and facilities.

• The security at the building where the office is located shall be ensured. For example, a smart card access control system can be implemented.

• Depending on the security level, other measures can be taken to further enhance site access security, such as video surveillance and biometric access control systems.

• The access rights will be granted to authorized individuals based on the system and data access control measures. This measure shall be also applicable to visitor access.

• Party B's employees and external employees shall wear their own identify card at all sites of Party B.

Additional Measures for Data Centers/ Servers:

• All data centers/ servers shall follow strict security procedures such as installation of protective devices and surveillance cameras.

• Only authorized representatives have access to the system and fundamental framework in the data center/ server facility.

• To ensure the normal operation of the data center/ server, physical security devices (such as mobile sensors and cameras) shall be maintained on a regular basis.

• Party B and third-party provider of the data center/ server used shall ensure that the identity of authorized personnel and the time of the personnel entering the exclusive area of Party B are recorded.

B. System Access Control.

Measures:

• Set different permissions to access sensitive systems and manage them according to Party B's policies.

• All personnel shall use a unique identification (user identification) to access Party B's system.

• Corresponding procedures and control the change of permissions shall be set according to Party B's policies. The access rights of personnel who has left the company shall be revoked.

• It shall be prohibited to share passwords, and it shall be required to change passwords regularly, and change default passwords.

• The company network shall be isolated from public network through technical solutions such as firewalls.

C. Data Access Control.

Measures:

• As part of Party B's policies, personal information shall at least reach the same protection level as confidential information in Party B's data classification and grading standards.

• Party B shall adopt the concept of permissions, explain the permission granting process and the role (user ID) assigned to each account, and grant the permission to access to personal information according to the minimum essential principle.

• Party B shall regularly check security measures and protect the applications that process personal information.

• Party B's policy has stipulated the destruction mechanism of data and data carriers.

D. Data Transmission Control.

Measures:

• When transmitting data between Party B and Party A, both parties shall agree on the protection measures for the transmitted personal information. This applies equally to physical data transmission and network data transmission.

• Party B shall be responsible for any data transmission within its control system.

E. Operation Control.

Measures:

• Party B shall ensure that the contracts signed between Party B and Party A and sub-processor, etc. are followed through controls and procedures.

• All Party B's employees, sub-processor and/ or other service providers shall be bound by the contracts and comply with the confidentiality regulations on all sensitive information (including the trade secrets of Party B, Party A and partners).

F. Integrity and Availability Control.

Measures:

• Party B shall conduct backups regularly to ensure the rapid recovery of key business systems when necessary.

• Party B has developed emergency business plan for key businesses and provided recovery strategy for disasters of key businesses and tests them from time to time.

G. Data Isolation Control.

Measures:

• Party B utilizes existing available technology to realize the isolated preservation of Party A's personal information.

• Party A can only access its own data.