FaceID PERSONAL INFORMATION AND PRIVACY PROTECTION POLICY

Last updated on: [September 30, 2020]

Foreword

Beijing Kuangshi Technology Co., Ltd. and its affiliates (hereinafter referred to as “we” or “MEGVII”) highly respect and are committed to protect personal information and privacy. As the face-based identity verification and KYC platform provided by MEGVII, FaceID Platform (hereinafter referred to as the “Platform”) aims to provide users with various KYC verification services from end to cloud. The Platform will process personal information in strictly accordance with the requirements and standards set up in the *MEGVII Personal Information and Privacy Protection Policy* (hereinafter referred to as “MEGVII Policy”). In order to further clarify the personal information processing practices that may be involved in this Platform, we have formulated the FaceID Personal Information and Privacy Protection Policy (hereinafter referred to as the "FaceID Policy") to introduce the details of the collection, use, retention and other processing in this Platform.

PLEASE NOTE that the FaceID Policy does not fully cover all the measures and efforts of MEGVII in protection of personal information and privacy. We promise to strictly abide by applicable laws, regulations and regulatory requirements, and highly respect the legal rights related to your personal information. To ensure you have a full picture of our basic information, our personal information and privacy protection principles, and other relevant content, please read the MEGVII Policy at the same time.

In addition, in specific scenarios that the business is further developed and provided based on this Platform, our clients (hereinafter referred to as the "Clients") or we may separately provide the end users (hereinafter referred to as "Users" or "you") with specific privacy policies or similar legal texts. PLEASE also completely read the privacy policies or similar legal texts under these business scenarios to ensure that you are fully aware of the complete practices related to personal information processing. The FaceID Policy only applies to this Platform provided by MEGVII, and is completely independent of the privacy policies or similar legal texts that our Clients or any third parties may or need to provide to you.

The FaceID Policy will help the Clients and the Users understand the following:

1. **How we collect and use personal information**
2. **How we retain and disclose your personal information**
3. **How we protect your personal information**
4. **How your personal information is transferred globally**
5. **Your rights to personal information**
6. **How we process personal information of minors**

7. How to contact us
8. How we update the FaceID Policy

In the FaceID Policy, "personal information" refers to various information recorded electronically or in other ways that can identify a specific natural person alone or in combination with other information, and/or reflect the activities of a specific natural person. Unless otherwise stated, other relevant definitions and terms under this FaceID Policy shall have the same meanings as those in *Cybersecurity Law*, *Information Security Technology - Personal Information Security Specifications* and other laws and regulations, regulatory documents, and national standards.

1. How we collect and use personal information

In different business scenarios, MEGVII will carry out various business cooperation with Clients. We will work with the Clients and suppliers to ensure that the personal information collected and processed has obtained your complete and valid authorization and consent, except in the following cases:

1) Where the request is related to fulfilling obligations under laws and regulations;
2) Where the request is directly related to national security and national defense;
3) Where the request is directly related to public security, public health and significant public interests;
4) Where the request is directly related to investigations into crimes, prosecutions, court trials, execution of rulings, etc.;
5) Where refusing the request is to protect your or other individuals' life, property and other vital legal rights and interests, but it is difficult to obtain your or other individual's authorization and consent;
6) Where the involved personal information is voluntarily disclosed to public by yourself;
7) Where it is necessary for the conclusion and performance of a contract according to your request;
8) Where the personal information is collected from legally publicly disclosed information, such as legal news reports, government information and lawful public datasets;
9) Where the processing is necessary to maintain the security and the stable operation of the products or services provided, such as discovering and dealing with any failures of the product or service;
10) Where the personal information controller is in news industry, and the processing is necessary for it to engage in lawful news reporting;
11) Where a) the personal information controller is an institution for academic research, b) the processing is necessary to engage in academic researches or statistical activities for public interest, and c) the personal information included in the academic research or its description has been de-identified when providing any third parties with such results.

<u>What personal information we collect and why</u>

As far as this Platform is concerned, we, together with the Clients, will collect and use your

personal information. To specify:

1) Sign-up and login of FaceID account

In order to sign up a FaceID account and complete the login process, we will collect the user name, mobile phone number, email address (if you voluntarily fill in after the sign-up). **PLEASE note that the sign-up and login processes are one of the prerequisites for using this Platform. If you refuse to provide the aforementioned information, you will not be able to normally sign up, log in and/or use this Platform.**

In addition, if you choose to use a Face++ account or other MEGVII account to log in to this Platform, we will also collect your relevant Face++ account, password and mobile phone number to complete the identity verification of the login process.

2) Technical application of face image

In order to provide the capabilities of face image recognition related technology, we will further identify and extract **face key points and other facial recognition features** based on the original pictures, videos and other data actively provided by the Clients/Users. Such information would be used for specific functions such as face comparison, liveness detection, etc. **PLEASE note that this Platform is part of the open AI capabilities of MEGVII. If you refuse to provide original pictures, videos and other aforementioned data, it will NOT be feasible to implement the functional applications mentioned above.**

PLEASE note that, we mainly use advanced algorithms and models such as neural network algorithms to provide our Clients with the application of technical capabilities. The aforementioned functions may involve the processing of biometric information such as facial recognition features, which are personal sensitive information. Regarding the rules on how to collect and use biometric information under the specific products and/or services you directly use, we recommend that you should decide whether to consent to the processing after carefully understanding the relevant rules under the specific product and/or service scenario (usually explained to you by our Clients).

3) Application of ID information recognition technology

In order to provide the capabilities of ID information recognition related technology, we will also further identify and extract **ID information (such as photos and texts on ID card)** based on the original pictures and other data actively provided by the Clients. Such information would be used for specific functions such as recognition, and collection of identity information. **PLEASE note that, the function may involve the processing of personal identify information such as ID information, which is personal sensitive information. This Platform is part of the open AI capabilities of MEGVII. If you refuse to provide original pictures and other data, it will NOT be feasible to implement the aforementioned functional applications.**

Special Declaration on Cookie

Cookies are small files transmitted by a website, application or service and stored on your device. We use cookies like most websites on the Internet, the purposes mainly include:

1) to simplify your re-login steps, 2) to store your preferences, 3) help you confirm the security of the account or data, 4) automatically record certain information to analyze and manage our websites (such as IP address, type of browser, internet service provider, software version information of the equipment, number of page views, source site, date/time stamp, click stream). For more details about our use of cookies, please refer to the MEGVII Policy.

2. How we retain and disclose your personal information

Unless expressly required by applicable laws, regulations or regulatory provisions, we will retain your personal information for the shortest time required to achieve the processing purpose.

In this Platform, we mainly provide specific applications of technical capabilities. To ensure the normal use of the functions of this Platform, we will retain the equipment information you use during your use of this Platform and within a reasonable period thereafter. After the specific implementation of certain function, we will delete or anonymize original pictures, videos and other data provided by the Clients and the service results based on such original data as soon as possible.

In addition, in accordance with the Cybersecurity Law and other mandatory requirements in laws and regulations, we will keep network logs for no less than six months.

Unless the applicable laws, regulations or regulatory requirements clearly require, or there are other clear disclosure scenarios in the MEGVII Policy, we will not share or disclose personal information involved in the Platform to external third parties other than our Clients in any form and for any purpose.

3. How we protect your personal information

We have taken reasonable and feasible technical measures and management measures to protect personal information being processed and to deal with personal information security incidents. For more details about our measures, please refer to MEGVII Policy. Nevertheless, PLEASE note that although we have taken reasonable measures to protect your personal information, **NO WEBSITE, INTERNET TRANSMISSION, COMPUTER SYSTEM OR WIRELESS CONNECTION IS ABSOLUTELY SECURE**.

To specify, in this Platform, the major protection measures to protect your personal information include but are not limited to:

1) We will de-identify your personal information in a timely manner when feasible, to reduce the risk of other organizations or individuals re-identifying you.
2) We will regularly review the methods of personal information processing (including physical security measures), and continue to strengthen the security of technical tools such as API and SDK.
3) We will continually make efforts to ensure the security of your personal information, and implement encryption and other safeguards throughout the transmission to prevent your personal information from being accessed, used or disclosed without authorization.

4. How your personal information is transferred globally

Our servers are located in China and Canada. Due to the requirements of relevant laws and regulations, in principle, the personal information collected and generated in China will be processed within the territorial scope of China. For the business outside of China, our Client will choose the location of supporting servers on its own discretion, and your personal information will be transferred from your jurisdiction to servers located in Singapore or Indonesia or Japan for processing, depending on the choice of our Client.

If it is really necessary to transfer your personal information globally, we, together with our Client, will be committed to transfer your personal information under the premise of complying with the mandatory rules and requirements of the relevant jurisdictions.

5. Your rights to personal information

We highly respect your rights related to personal information in accordance with the law. Below we list your rights and how we will protect them. PLEASE note that for a specific request, for security reasons, we may need to verify your identity before processing your request.

1) Right to be informed: we are committed to improving the transparency of personal information processing, and will inform you how we process your personal information through the FaceID Policy and other relevant legal documents.
2) Right to access: you have the right to access your personal information we collect.
3) Right to rectification: you have the right to ask us to make rectifications, if you find that the personal information we process about you is wrong.
4) Right to deletion: you have the right to ask us to delete your personal information, if we have no legal basis to continue to retain and process your information.
5) Account cancellation: if you use related products or services by obtaining the account we provide through sign-up or any available method, you have the right to submit an application for cancellation through the account cancellation channel provided to you in specific scenarios, and we will review and process in a timely manner.
6) The right to refuse automatic decision-making: you have the right not to be subject to fully automatic processing of decisions, including user profiling. If these decisions significantly affect your lawful rights, you have the right to ask for an explanation.

For your reasonable request, we do not charge fees in principle, but for repeated requests that exceed reasonable limits, we will charge a certain cost depending on the circumstances. We may refuse those requests that a) are unreasonably repeated, b) require excessive technical means (for example, where it needs to develop new systems or fundamentally change existing business practices), c) bring risks to the legitimate rights and interests of others, or d) are very impractical (for example, involving information stored on backup tapes).

In general, we will response as soon as possible within 30 days or the time limit stipulated by laws and regulations, except in the following cases:

1) Where the request is related to fulfilling obligations under laws and regulations;
2) Where the request is directly related to national security and national defense;
3) Where the request is directly related to public security, public health and significant public interests;
4) Where the request is directly related to investigations into crimes, prosecutions, court trials, execution of rulings, etc.;
5) Where there is sufficient evidence that you may have subjective malice or abuse of rights;
6) Where refusing the request is to protect your or other individuals' life, property and other vital legal rights and interests, but it is difficult to obtain your or other individual's authorization and consent;
7) Where responding to your request will cause serious damage to the legitimate rights and interests of you or other individuals or organizations;
8) Where the request involves any trade secret.

6. How we process personal information of minors

Please note that all our products, websites and services are mainly for corporate Clients, and we will not actively collect or process personal information of minors. If any Client or User wants or intends to provide us with or request us to process the personal information of minors, please ensure that the prior consent and authorization of the minors' guardians has been obtained in strict accordance with the requirements of relevant laws and regulations such as the *Provisions on the Protection of Children's Personal Information Online* in China.

If we find that any Client or User has provided original data containing personal information of minors without the consent of their parents or guardians, we will immediately delete such original data and will not provide any services for such data. In avoidance of ambiguity, we treat anyone under the age of 14 as a minor.

In addition, we attach great importance to the security and control of personal information of minors. We have clearly listed children's personal information as the data type with the highest security level internally, and have effectively adopted technical and management measures such as encrypted storage and strict access control to provide additional security protection on personal information of minors.

7. How to contact us

If you have any need, we recommend that you directly make requests to the personal information controller (usually our Clients) under such specific business scenarios and they may forward such requests to us as appropriate. We will respond to your request as soon as possible. If needed, you may contact us directly by sending an email to business@megvii.com. To ensure that your request is clear and specific, please indicate in the aforementioned email that:

1) Your name and contact information;
2) Your specific request, suggestion and/or corresponding link.

8. How we update the FaceID Policy

We reserve the right to update or modify this FaceID Policy from time to time. Nevertheless, without your explicit consent, we will not reduce your rights in accordance with the FaceID Policy. You can view the latest version of FaceID Policy through this page. For material changes, we will provide more noticeable notifications (for example, for some services, we will send notifications by e-mail or other means, explaining the specific changes).

The “material changes" mentioned in this FaceID Policy include but are not limited to:

1) Where our service model has undergone material changes, such as the purpose of processing personal information, the type of personal information processed, the way of using personal information, etc.
2) Where our ownership structure, organizational structure or other aspects has undergone material changes, such as ownership transfer due to 1) business adjustments, 2) bankruptcy, 3) mergers, or 4) other possible reasons.
3) Where the main parties of sharing, transferring or public disclosing personal information have changed.
4) Where there is any material change on your rights to participate in personal information processing and how to exercise them.
5) Where there is any change on the department responsible for handling personal information security, our contact information or your complaint channel.
6) Where the report of personal information security impact assessment shows there is a high risk.