HSBC Bank (China) Company Limited

Personal Information and Privacy Protection Policy for Corporate Digital Banking Services

Date of Update: 15 April 2024
Effective Date: 15 April 2024

HSBC Bank (China) Company Limited ("HSBC", "the Bank", "we" or "us") take personal information confidentiality and security very seriously, and strive at all times to protect personal information and privacy of our customers and other related personal information subjects ("you" or "Personal Information Subject") according to law. We therefore formulate this Personal Information and Privacy Protection Policy for Corporate Digital Banking Services (this "Policy") to help you understand the purposes, methods, and scope of personal information we collect and use, our practices regarding personal information and privacy protection, your rights and interests with regard to personal information and privacy and how to assert your rights and interests.

This Policy applies to your use of our corporate digital banking services (including internet banking (HSBCnet), client mobile app (HSBCnet), WeChat account, WeChat application).

The table of content of this Policy is set out as below:

Please read through this Policy carefully and pay particular attention to the provisions that are bolded and underlined which we think have material impacts on your interests and/or deal with your sensitive personal information. The key points of this Policy are summarized as below:

1. For your convenience to understand the purpose and category of personal information we collect when you sign up for our service, we therefore explain them under the particular service scenario.

2. When you sign up for some particular services, we will collect your sensitive personal information after you give us express consent if required by applicable laws and regulations. Refusal on providing consent might affect you use related service, but will not affect you use other services we provided.

3. To provide the service per your or relevant customers' request, we might need to share your personal information to a third party. We will carefully assess the legitimacy, propriety, and necessity of the data sharing with the third party. We will ask the relevant third party to take all data protection measures required pursuant to applicable laws and regulations.

We fully understand how important your personal information means to you, and we will exert our best effort to protect the security of your personal information. We have always been committed to maintain your trust and will stick to below principles to protect your personal information: Right and Responsibility Consistency, Explicit Purpose, Freely Given Consent, Minimum and Necessity, Assurance of Information Security, Participation, Fairness and Transparency. We are also committed to take appropriate security measures to protect your information.

We shall collect, use, store, disclose, and protect your and related parties' personal information in accordance with this Policy. **If there is any discrepancy between this Policy and the other agreements entered into or other terms and conditions agreed between you or relevant corporate business customers of which you are representative or with which you have a relationship ("Corporate Business Customers" or "Relevant Customers**") **and us, such other agreements or terms and conditions shall prevail.**

In the context of corporate business, we understand that you have agreed that Relevant Customers can use your personal information for the purpose described in this Policy, and therefore, we treat Relevant Customers as your authorized representatives related to your personal data processing activities.

I. How We Protect Your Personal Information

1. Information security is our top priority. We will endeavour at all times to safeguard your personal information against unauthorised or accidental access, processing or damage. We maintain this commitment to information security by implementing appropriate security and managerial measures to secure your personal information. We will take responsibility in accordance with the law if your information suffers from unauthorised access, public disclosure, erasure or damage for a reason attributable to us and so impairs your lawful rights and interests.

2. Our website supports advanced encryption technology - an existing industry standard for encryption over the Internet to protect your personal information. When you provide sensitive personal information through our website or applications, it will be automatically converted into codes so as to ensure secure transmission afterwards. Our web servers are protected behind "firewalls" and our systems are monitored to prevent any unauthorised access. Our mobile banking application software for corporate banking services has passed the software filing for financial client mobile application with National Internet Finance Association of China.

3. We maintain strict security system to prevent unauthorised access to your personal information. We exercise strict management over our staff members who may have access to your personal information, including but not limited to access control applied to different positions, contractual obligation of confidentiality agreed with relevant staff members, formulation and implementation of information security related policies and procedures, and information security related training offered to staff.

4. We will not disclose your personal information to any third party, unless the disclosure is made to comply with laws, regulations and regulatory requirements or according to this Policy or other agreement (if any), or based on your or Relevant Customers' separate consent or authorisation. When we use services provided by external service providers (entities or individuals), we also impose strict confidentiality obligations on them and request them to take all data protection measures required pursuant to applicable laws and regulations when processing your personal information.

5. **For the security of your personal information, you take on the same responsibility as us. You shall properly take care of your personal information, such as your identity verification information (e.g. user name, password, dynamic password, verification code, etc.), and all the documents, devices or other media that may record or otherwise relate to such information, and shall ensure your personal information and relevant documents, devices or other media are used only in a secured environment. You shall not, at any time, disclose to any other person or allow any other person to use such information and relevant documents, devices or other media. Once you think your personal information and/or relevant documents, devices or other media have been disclosed, lost or stolen, or may otherwise affect the security of use of our digital banking services by you or Relevant Customers, you shall notify us immediately so that we may take appropriate measures to prevent further loss from occurring.**

6. We will organize regular staff training and drills on emergency response so as to let the relevant staff be familiar with their job duties and emergency procedures. If unfortunately personal information security incident occurs, we will adopt emergency plan and take relevant actions and remediation measures to mitigate the severity and losses in connection therewith. Meanwhile, we will, following the applicable requirements set out in law and regulation, inform you or Relevant Customers of the basic information of the security incident and its possible impact, the actions and

measures we have taken or will take, suggestions for you to prevent and mitigate the risk, and applicable remediation measures. We will inform you or Relevant Customers about the security incident by email, mail, call, SMS, push notification or through other methods as appropriate in a timely manner. Where it is difficult to notify each Personal Information Subject, we will post public notice in a reasonable and effective way. Meanwhile, we will report such personal information security incident and our actions in accordance with applicable law, regulation and regulatory requirements.

II. How We Collect Your Personal Information

1. Personal information refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized. Personal information include name, birth date, ID certificate information (ID card, passport and etc.,), personal biometrics recognition information, contact information, address, account information, property status, location and etc., Sensitive personal information refers to personal or property information that, once leaked or illegally provided or misused, may harm personal or property safety and will easily lead to infringement of the personal reputation, human dignity, physical or psychological health, or discriminatory treatment. Such information mainly includes ID certificate information (ID card, passport and etc.,), personal biometrics recognition information, credit information, property information, transaction information, medical and health information, specific identity, financial account, individual location tracking etc. as well as any personal information of a minor under the age of 14 (i.e. child).

   The personal information we collect may be recorded in paper, electronic means (including but not limited to the information we collect via our self-service machine, website, online banking, client mobile app, WeChat account, WeChat application or other mobile device application, email, SMS or other channels) or any other means.

2. In order for us to provide Relevant Customers with digital banking services, fulfil the Bank's legal obligations and to ensure the safety of our digital banking services, you need to provide us, or allow us to collect from you or any third party upon your or Relevant Customers' consent or authorization, the following information necessary for the functions described in below table as well as under Article III of this Policy "How We Use Your Personal Information:

Functions	**Information We Need to Collect**	**Applicable Channel**
Registering digital banking service account	**Your personal name, date of birth, employer name, email/ fixed telephone number/mobile phone number for working purpose, employer's address**	Internet banking
Logging onto digital banking	**Your username/logon name, security question and answer, any password,**	Internet banking, client mobile app,

services or retrieving logon password.	**code, dynamic password, security code, verification code pre-set by you or created or sent via security device, mobile phone, email or other equipment or methods.**	WeChat account, WeChat application
Basic functions of digital banking services, including money receiving, payment or transfer, provision of bank statement/voucher, online trade services etc.	**Your personal name, email/fixed telephone number/ mobile phone number for working purpose, password** for the purposes of identity verification, approving and processing requests or instructions for payment or other financial product/service related transactions.	Internet banking, client mobile app,
Maintaining proper and secure operation of digital banking services, preventing and controlling digital banking services related risk	Your device type, operating system, device ID (applicable on client mobile app only), Mac address, unique device identifier (applicable on client mobile app only - iOS will collect UUID, Android OS will collect IMEI and Android ID)，the Open ID and Union ID associated with WeChat service account and mini programs (applicable on WeChat account, WeChat application only), software version, logon IP address, internet service provider (ISP), device accelerators (such as gravity sensing devices, etc.) **Technical information that may not be used to identify an individual's identity will not be treated as personal information. But if the information alone or in combination with other information may be used to identify your identity, we will treat it as your personal information and have it properly protected.**	Internet banking, client mobile app, WeChat account, WeChat application

We will only collect information that corresponds to the service that you trigger. If you refuse to provide those information, you or Relevant Customers will not be able to register or logon our digital banking service account, or will not be able to use our regular digital banking services in a safe and normal way.

3. You may decide, at your free choice, to provide us, or allow us to collect from you or any third partyupon your or Relevant Customers' consent or authorization, the following information for the functions described in below table as well as under Article III of this Policy "How We Use Your Personal Information:

Functions	**Information We Need to Collect**	**Applicable Channel**
WeChat account binding (Logon)	**Your user name, any password, code, dynamic password, security code, verification code pre-set by you or created or sent via security device, mobile phone, email or other equipment or methods , email for working purpose and user ID pre-set by you for HSBC corporate internet banking services.**	WeChat account, WeChat application
Fingerprint or facial biometrics recognition functions	**The operation system is carrying out direct interaction with you when you are using such function. We are notified only as to whether the authentication is successful or not. We do not collect nor access any fingerprint or facial biometric data.** The above function is used only for identity recognition, or verification of logon application.	Client mobile app
Message service functions	Device type, unique device identifier	Client mobile app
WeChat appointment for account opening	**Name, email/fixed telephone number/mobile phone number for working purpose, job position, WeChat open ID, WeChat name and profile photo of contact person, image of Legal Representative's ID certificate image in front and back side.**	WeChat account, WeChat application
To provide Relevant Customers with more accurate, tailor-made and convenient service and improve service experience	**Information you provide when raising your feedback, suggestion or complaint, information you input when participating in campaigns or surveys**. Meanwhile, to assure the service quality, we may record **the service call content. We will provide necessary hint before**	Internet banking

	recording to protect your right to be informed and the right of choice. **We will conduct analysis on that information and will contact you or provide you or Relevant Customers with relevant response, service or products based on that information.**	

We will only collect information that corresponds to the service that you trigger. If you refuse to provide the above information, you or Relevant Customers are not able to use or enjoy the relevant functions, but the use of other functions of our digital banking services will not be adversely affected.

4. Our client mobile applications may also invite your permissions for the following system functions relating to personal information and will collect and use the information for the permitted functions based on your permission:

Items	**Permitted Functions**	**Applicable Channel**
Fingerprint logon	Identity recognition, logon, and verification using fingerprint(s)	Client mobile app
Face ID	Identity recognition and logon using face ID (applicable to some type of Apple device)	Client mobile app
WeChat	Related functions on WeChat account and WeChat application service	WeChat account, WeChat application
Camera	Facial recognition and ID certificate/bill scanning	WeChat application
Location	Security verification	Client mobile app
Telephone	Dial the phone number of branches to enquire about banking business by one-touch	Client mobile app (Android)
Notifications	Push messages with alerts, sounds, and icon tags. To allow you to experience offline notification features, self-start functionality will be enabled in the mobile application when you agree to this Policy and grant permission for 'notifications' function. We will push notifications to you through your device's 'notification centre' as needed. You can enable or disable notification permissions in your device's 'Settings'. You can also manage and disable message push services in the mobile application under 'More >	Client mobile app

	Settings > Notifications'. After disabling this permission or service, the mobile application will be not self-started.	
Device Information	To ensure the normal connectivity of the mobile application, authorization is required for the use of network access information (iOS). Additionally, for push notification functionality, permission to access phone status is necessary (Android).	Client mobile app

You may, at your free choice, decide whether to additionally grant the above permission for the above functions on client mobile applications. **If you refuse to grant permission for a specific function, you or Relevant Customers are not able to use that specific function**, but use of other functions in our digital banking services will not be adversely affected.

5. **When you use the functions or services on our digital banking services, under some specific circumstances, we will use software development kit ("SDK") provided by third party service provider to serve you or Relevant Customers. For the purpose of providing the services, SDK of third party service providers will correspondingly collect the following information:**

SDK Name: AppDynamics SDK
Third-Party Service Provider: AppDynamics
Business Scenario: Throughout the utilization of the client mobile app
Usage Purpose: To systematically gauge and analyze the performance metrics of electronic banking channels
SDK User Information: Mobile phone IP, device manufacturer, phone model, network type, and access duration information
Applicable Channel: Client mobile app

SDK Name: OneSpan RASP SDK
Third-Party Service Provider: OneSpan
Business Scenario: Throughout the utilization of the client mobile app
Usage Purpose: To fortify the app and proactively deter users from running the client mobile app on devices with identified security vulnerabilities
SDK User Information: Inventory of installed software
Applicable Channel: Client mobile app

SDK Name: Tealium SDK
Third-Party Service Provider: Tealium
Business Scenario: Throughout the utilization of the client mobile app, WeChat official accounts, and WeChat mini-programs
Usage Purpose: To count page view volume and analyse customer behavioural patterns

SDK User Information: Mobile phone IP, browser type, pages you visit or click (applicable to client mobile app, WeChat official accounts, and WeChat mini-programs); device manufacturer, mobile phone model, network type, operating system version, operating system type (applicable to client mobile app only)
Applicable Channel: Client mobile app, WeChat official accounts, WeChat mini-programs

SDK Name: Transmit SDK
Third-Party Service Provider: Transmit Security
Business Scenario: Login and transaction operation
Usage Purpose: To deliver advanced login and authentication functionalities
SDK User Information: Mobile carrier information (country/region code), mobile phone IP, device manufacturer, mobile phone model, network type and operating system version.
Applicable Channel: Client mobile app

SDK Name: Baidu Cloud Push SDK (Integration of Baidu, Huawei, Xiaomi, OPPO, vivo, Meizu Push SDK and Meizu Cloud SDK. For users of Huawei, Xiaomi, OPPO, vivo, and Meizu brand phones, the corresponding SDK of the respective manufacturer will be seamlessly integrated; for users of other brand phones, Baidu Push SDK will be used.)
Third-Party Service Provider: Beijing Baidu Netcom Science and Technology Co., Ltd.
Business Scenario: Push notification services
Usage Purpose: To provide comprehensive push notification services
SDK User Information: IP address, device information permissions, OAID (Xiaomi, vivo, OPPO), Android ID, device model, operating system version, mobile phone carrier information (operator name, country/region code), network type, installed application information, currently running processes, IMEI, WIFI MAC address. To ensure the seamless operation of push notification services, the push SDK will periodically retrieve Android ID and mobile phone carrier information during instances when the application is not in a silent state.
Applicable Channel: Client mobile app (Android)

SDK Name: Baidu Maps SDK
Third-Party Service Provider: Beijing Baidu Netcom Science and Technology Co., Ltd.
Business Scenario: Trade transaction tracker
Usage Purpose: To facilitate trade transaction tracking functionality
SDK User Information: Network type, device identification information (Android ID, IDFV), system information (operating system version, device brand and model, device configuration), IMSI, WIFI MAC address, IMEI, currently running processes
Applicable Channel: Client mobile app (Android)

SDK Name: WeChat JS-SDK

Third-Party Service Provider: Tencent Corporation
Business Scenario: Enterprise account pre-application process
Usage Purpose: To deliver the capability of capturing images of the legal representative's ID card, company's business license, verifying and obtaining the applicant's mobile phone number and facilitating merchant's payment collection under the enterprise account pre-application functionality.
SDK User Information: To use your camera, photo album, mobile phone number quick verification component and WeChat scan functions. Your personal information will not be collected by the WeChat JS-SDK.
Applicable Channel: WeChat official accounts, WeChat mini-programs

If you do not agree the above information to be collected by SDK of third party service provider, you or Relevant Customers may not be able to use or enjoy relevant services or functions, but use of other functions in our digital banking services will not be adversely affected.

6. **Please understand that the digital banking services we provide are constantly evolving. If you or Relevant Customers choose to use any other service not listed above for which we have to collect your information, we will separately explain to you or Relevant Customers, the purposes, methods, and scope of personal information we collect etc., through reminders on pages, interaction with you/Relevant Customers, agreements entered into with you/Relevant Customers or other appropriate method, and obtain consent from you or Relevant Customers for that. We will use, store, disclose, and protect your information in accordance with this Policy and other agreements (if any) between you/Relevant Customers and us. If you or Relevant Customers choose not to provide certain information, you or Relevant Customers may be unable to use certain or part of the service, but the use of other services we provide will not be affected.**

III. How We Use Your Personal Information

1. We will use your information in the following circumstances:

   (1) To realize the purposes and functions mentioned in above Article II of this Policy "How We Collect Your Personal Information"; to contact you or Relevant Customers, or to approve, process, manage, execute or effect Relevant Customers' application or instruction for transactions;

   (2) To ensure safe and stable financial services, we will use your information for identity verification, safety precaution, fraud detection, prevention or prohibition of illegal or incompliant activities, control or reduction of risks, recording or filing purposes;

   (3) To comply with applicable laws and regulations or discharge of legal duties; to report to relevant regulators or other authorities according to laws, regulations or regulatory requirements;

(4) To maintain and improve digital banking service or any function thereof, develop new service or function;

(5) Subject to the authorisation granted by you or Relevant Customers, to promote the Bank's other products and services and to recommend the products or services that may interest Relevant Customers;

(6) To make statistics and analysis of the use of our business, products, services or functions; we may share such statistics to the public or third parties to present overall trend of relevant business, products, services or functions. But such statistics will not contain any of your personal identifiable information.

2. **The above content related to information collection and use in this Policy shall not impact our use of your information for the purposes as otherwise agreed between you/Relevant Customers and us separately.**

3. If we use your personal information for the purposes other than the purposes of information collection and use as set forth in this Policy or in other agreement between you or Relevant Customers and us, we shall inform you how we use this information and obtain consent from you or Relevant Customers before using your personal information for such additional purposes as per applicable laws and regulations.

IV. How We Store Your Personal Information

In principle, the personal information we collect and generate within the territory of the People's Republic of China will be stored in the territory of the People's Republic of China. Since we provide products or services through resources and servers across the world, which means that to the extent permitted by regulatory rules and applicable laws, your personal information may be transferred to the foreign jurisdiction, or be accessed from these jurisdictions. If we transfer your personal information overseas, we will comply with applicable laws and regulations related to cross border data sharing. Whether it is processed domestically or overseas, in accordance with applicable data protection legislation, your personal information will be protected by a strict code of secrecy and security which, the Bank, other members of the HSBC Group, their staff and third parties are subject to.

We comply with Chinese laws and regulations on data storage. When we collect or process your information, we will, according to applicable laws and regulations, regulatory, archival, accounting, auditing or reporting requirements, and the purposes as set forth in this Policy, store your information for a period as minimum as necessary to fulfill the purposes of information collection. For example, in accordance with *Administrative Measures for the Customer Identification Verification and Preservation of Customer Identification Material and Transaction Records of Financial Institutions*, *Administrative Rules on RMB Settlement Accounts* and relevant financial regulations as well as *Provisions on the Scope of Collection*

and Preservation Period in the Document Archiving of Enterprises, the customer materials shall be kept for at least 5 to 30 years or even longer, depending on the usage purpose and document nature of relevant material.

We have data retention policies. After the retention period expires under relevant data retention policy, we will destroy, delete or anonymise relevant information or where the destruction, deletion or anonymization is not possible, store your personal information securely or separate it from other data processing. **The exception is when the information needs to be retained according to applicable laws and regulations, regulatory, archival, accounting, auditing or reporting requirements, special agreement between you/Relevant Customers and us, or for settlement of indebtedness between you/Relevant Customers and us, or for record check or enquiry from you, Relevant Customers, regulators or other authorities.**

V. How We Share, Transfer and Publicly Disclose Your Personal Information

1. Entrusted Processing and Sharing

For the purposes set out above in this Policy, we may provide or disclose all or part of your personal information to the following recipients under the preconditions that such provision or disclosure is necessary and is made with proper protective measures (please refer to Article I of this Policy "How We Protect Your Personal Information" for details) and the recipients may also, for the aforesaid purposes, use, process or further disclose the information they receive provided that corresponding protective measures are adopted pursuant to the applicable laws or our requirements:

(1) any member of the HSBC Group;

(2) any contractor, subcontractor, agent, third party product or service provider, licensor, professional consultant, business partner, or associated person of the HSBC Group (including their employees, directors and officers);

(3) any regulator of the Bank or any member of the HSBC Group or any other authority, or any organisation or individual designated by such regulators or authorities;

(4) anyone acting on behalf of Relevant Customers according to the authorisation of Relevant Customers or according to law, payment recipients, beneficiaries, account nominees, intermediary, correspondent and agent banks (e.g. for CHAPS, BACS, SWIFT), clearing houses, clearing or settlement systems, market counterparts, upstream withholding agents, swap or trade repositories, stock exchanges, companies in which Relevant Customers have an interest in securities (where such securities are held by us for Relevant Customers), or anyone making any payment to Relevant Customers;

(5) any person or related party who has the right or obligation, acquires an interest or assumes risk, in or in connection with any product or service Relevant Customers receive from the Bank, or any business Relevant Customers handle at the Bank or any transaction Relevant Customers make with the Bank (for example, the person who provides or intends to provide any mortgage or other security for any of Relevant Customers' debt to the Bank);

(6) other financial institutions, industrial associations, credit rating agencies, credit reference agencies (including without limitation, the Basic Financial Credit Information Database) or information service providers;

(7) any third party fund manager providing Relevant Customers with asset management services through us;

(8) any third party to whom we provide referral, agency or intermediary service; and

(9) any party in connection with any business/asset transfer, restructure, disposal, merger, spin-off or acquisition transactions of the Bank.

Subject to applicable laws and regulations, we will seek separate consent (if legally required) from you or Relevant Customers and notify you of the data sharing with the third parties, including the data recipient's identity, contact information, purpose of processing, method of processing and the type of personal information.

In case of cross border personal data sharing, we will also conclude a data protection agreement with the offshore personal information recipient in the format of standard data protection clause issued by Cyberspace Administration of China as well as specify your relevant personal information subject's right in your capacity as a third party beneficiary under said agreement pursuant to applicable laws and regulations, for example the manner and method of exercising your right towards the offshore personal information recipient. If you want to know more details about aforesaid data protection agreement, you may contact us to raise such request via the method listed in Article IX of this Policy "How to Contact Us".

2. Transfer

Without separate consent from you or Relevant Customers, we will not transfer your personal information to any other company, organization or individual, except **in the case of business/asset transfer, restructure, disposal, merger, spin-off or acquisition transactions where the transfer is necessary. In such case, we will inform you or Relevant Customers of the identity and contact method of the personal information recipient as per applicable laws and regulations as well as request said recipient to comply with this Policy. If the personal information recipient changes the purpose**

and method of personal information processing activities under this Policy, they shall re-obtain the consent from you or Relevant Customers.

3. Public Disclosure

We will not disclose your personal information to the public unless we have your separate consent. If public disclosure is needed, we will inform you the purpose of such disclosure, the type(s) of information being disclosed, and any sensitive information involved.

VI. Special Circumstances for Information Processing

We will process your personal information (such as information collection, storage, use, analysis, transfer, provision, disclosure) based on your consent. To the extent allowed by laws and regulations, we may process your personal information without your consent under the following circumstances:

(1) where it is necessary for entering into a contract or the performance of a contract to which you are the party;

(2) where it is necessary for compliance with a legal obligation to which we are subject;

(3) where it is necessary in order to protect your or others' vital interests related to life and property in an emergency or respond to public health emergencies;

(4) where it is within reasonable limits in order to carry out news coverage or media supervision for the public interest;

(5) where it is within reasonable range according to law to process the information which has been legally made public or publicized by yourself;

(6) other circumstances stipulated by laws and regulations.

VII. How We Use Cookies and Similar Technologies

1. Your visit, browse, use of any of our website or digital banking service related applications may be recorded for analysis on the number of visitors to the site and/or applications, general use patterns and your personal use patterns and improving your experience. Some of this information will be gathered through the use of "Cookies" and similar technologies. Such technologies can enable our website or applications to recognise your device and store information about your use of website and/or applications so to provide continuous services to you and to tailor the content of our website/applications to suit your interests and, where permitted by you, to provide you

with promotional materials based on your use patterns. We will be able to access the information stored on the Cookies and similar technologies for aforesaid purposes.

The information collected by Cookies is anonymous aggregated data, and contains no personal information such as name, address, telephone, email etc.

2. **Most local terminals are initially set to accept Cookies. You can manage or disable Cookies based on your own preference. Should you wish to disable the Cookies, you may do so by changing the setting on your local terminals. However, after changing the setting you may not be able to enjoy the convenience that Cookies bring, but your normal use of other functions of the local terminals will not be affected.**

VIII. Your Rights Relating to Personal Information

1. You have the right to request us to protect and secure your personal information in accordance with the provisions of the law, regulation and this Policy. You have the right to exercise your rights of individual granted by applicable laws and regulations.

2. You have the right to inquire whether we hold your personal information, to access and copy your personal information. You can log in to online banking and go to "Click on your name in the upper right corner > Main details" to check your name, email/ fixed telephone number/mobile phone number for working purpose and work location details. You can also visit our local branch or contact us through the contact method specified in Article IX of this Policy to inquire or submit a request to copy your personal information.

3. You have the right to change the scope of authorization or withdraw your consent. We will not further process the related information once you change your authorization. Please note the withdrawal of consent will not affect the lawfulness of processing based on consent given by you or Relevant Customers before its withdrawal. You can modify or withdraw your device function authorizations by utilizing the permission management function within the operating system of the device itself, located under "Settings > HSBCnet," to manage permissions for features such as face ID, fingerprint recognition, notifications and other device functionalities.

4. **You have the right and obligation to update your personal information with us to ensure that all information is accurate and up-to-date.** You have the right to request us to provide convenience for you to update your personal information with us and to correct any of your information that is inaccurate. You can log in to online banking and navigate to “Click on your name in the upper right corner > Main details” to update your information such as your name, email/ fixed telephone number/mobile phone number for working purpose and work location details. Alternatively, you may visit our local branch or contact us through the contact method specified in Article IX of this Policy to initiate the process of updating your personal information.

5. In relation to personal guarantee, you have the right to request to be informed of your personal information that is disclosed to credit reference agencies by us, so as to enable your request to the relevant credit reference agencies for access to and correction of your information.

6. You have the right to request us to delete or otherwise properly dispose of your personal information that is beyond retention period in accordance with the applicable law and regulation, this Policy, and other agreement between you/Relevant Customers and us. If we cease our operation, we will stop collecting any personal data from you in a timely manner, delete or anonymize all your personal information, and inform Relevant Customers represented by you of such operation cessation via courier or public announcement, except as otherwise provided by laws and regulations or where the personal data deletion is technically not possible.

7. You have the right to uninstall digital banking services related applications. **Please note that to uninstall the applications will not close digital banking service account of Relevant Customers. Such digital banking service account closure shall be proceeded by Relevant Customers. Relevant Customers may request the closure of their electronic banking channel accounts by contacting their relationship managers, visiting a branch business outlet or calling the service hotline. After Relevant Customers close their digital banking service accounts, we will no longer collect your information through relevant channel, and will delete relevant personal information in accordance with the applicable law and regulation, this Policy, and other agreement between you/Relevant Customers and us, except for those we keep according to the applicable laws and regulations, regulatory, archival, accounting, auditing and reporting requirements, agreement between you/Relevant Customers and us, or for settlement of any indebtedness between you/Relevant Customers and us, or for record check or enquiry from you, Relevant Customers, regulators or other authorities, or where the personal data deletion is technically not possible.**

8. Responding to your request: in addition to the above-mentioned ways of exercising your rights, you may also make your request in the manner listed in Article IX of this Policy "How to Contact Us".

9. Nothing in this Policy shall limit the other rights you should have as a Personal Information Subject under applicable laws and regulations.

IX. How to Contact Us

Requests for access to, copy, correction or deletion of personal information, for change/withdrawal of authorisation or disposal of personal information beyond retention period, for a copy of this Policy, enquiries about our practices regarding personal information and privacy protection, or exercising other rights you are granted by the applicable laws and regulations should be addressed to:

Data Privacy Officer (DPO)
HSBC Bank (China) Company Limited
36/F HSBC Building, Shanghai IFC, 8 Century Avenue, Pudong, Shanghai, 200120
Tel: +86 400 821 8878 (8:30am - 5:30pm, Monday to Friday during the working days)

For the sake of security, you may need to raise your request in written form or use other methods to prove your identity. We may verify your identification before handling the request.

Upon the receipt of your request, we will reply to you within 15 working days or shorter period as prescribed by law and regulation (if any).

We will not charge fees for the processing of your above-mentioned reasonable requests for checking, correcting or otherwise disposing of your personal information.

Notwithstanding the foregoing, we may reject your request that is illegal, noncompliant, or unnecessarily repeated, needs excessive technical means (for example, the need to develop information systems or fundamentally change current practices), brings risks to the legitimate rights and interests of others, is unreasonable or technically impracticable. We may not be able to respond to your request under any of the following circumstances:

(1) **where the request is in relation to our legal and financial compliance obligation under laws and regulations;**

(2) **where the request is in direct relation to state security or national defence security;**

(3) **where the request is in direct relation to public security, public sanitation, or major public interests;**

(4) **where the request is in direct relation to criminal investigations, prosecutions, trials, execution of rulings, etc.;**

(5) **where there is sufficient evidence that you are intentionally malicious or abuse your rights;**

(6) **where the purpose is to protect you or other individual's life, property and other substantial legal interests but difficult to acquire your consent;**

(7) **where responses to your request will give rise to serious damage to your or any other individual or organisation's legal rights and interests; or**

(8) **where the request involves any trade secret.**

You may supervise or make suggestions for our practices regarding personal information and privacy protection, and lodge complaint or file a lawsuit with the competent Chinese court according to law against us or our staff for any infringement of your rights and interests in your personal information and privacy.

If you have any query, complaint, feedback, comment or suggestion, please **Contact HSBC.** You may contact us through the contact information listed in this Policy, by calling our hotline or visiting our branches or sub-branches. You may also visit our official website www.hsbc.com.cn to enquire the nearby branches or sub-branches, or other contact information of us suitable for you.

X. Protection of Minors' Personal Information

Our products, services and website related to corporate business are targeting Corporate Business Customers. The minors under the age of 18 (including children under the age of 14) cannot create business accounts at the Bank. But certain business (such as payment settlement service under corporate online banking channel) may collect minors' information. If, in the course of business, we notice that Relevant Customers fail to obtain consent from the minor's parents or guardians before providing relevant minors' information to us, we will request Relevant Customers to immediately stop further sharing such information with us and take other remediation actions.

XI. Formulation, Effectiveness, Update of this Policy and Others

1. **The Policy is made by us and published at our digital banking service related websites or applications and takes effect on the date of issuance.** The Policy may be amended or updated from time to time, particularly in the events of major changes as follows:

   (1) Major changes in our service model, such as changes in the purpose of processing personal information, changes in the types of personal information being processed, the use methods of personal information, etc.;

   (2) Major changes in our ownership structure, organisational structure, etc., such as changes as result of business adjustments, bankruptcy, mergers, etc.;

   (3) Changes in the main objects of personal information sharing, transfer or public disclosure;

   (4) Significant changes in your rights relating to personal information or in the methods to exercise such rights;

   (5) Changes of our contacts for personal information related requests/enquiries, changes of our contacts for complaint or feedback;

(6) Other major changes which may significantly impact your interests in personal information.

We will post the changes to the Policy or the updated Policy through push notifications, pop-ups, announcements etc., on our digital banking service related websites and/or applications. Changes to the Policy shall not diminish or limit the rights you should have as a Personal Information Subject under applicable Chinese law.

You may also check this Policy on our client mobile banking application via "i" button on the top of logon page or go to "More" – "Information" Page after logging.

2. **Where you provide to us personal information about another person, you should ensure that person acknowledges this Policy and, in particular, tell him/her how we may collect and use his/her personal information and obtain the consent/authorization of such person.** You should remind that person to read this Policy in advance and may also give him/her a copy of this Policy.

3. In case of discrepancy between the Chinese and English versions of this Policy, the Chinese version shall apply and prevail.