

HSBC Bank (China) Company Limited
Personal Information Protection Policy for Corporate
Digital Banking Services

Issuance Date: 5 December 2020

Effective Date: 5 December 2020

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 information subject (“you” or “Personal Information Subject”) according to law. We therefore formulate this Personal Information 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. **Please read through this Policy carefully and pay particular attention to the provisions that are bolded and/or underlined.**

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

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

- I. How We Protect Your Personal Information
- II. How We Collect Your Personal Information
- III. How We Use Your Personal Information
- IV. How We Store Your Personal Information
- V. To Whom We Disclose Your Personal Information
- VI. Special Circumstances for Information Collection, Use and Disclosure
- VII. How We Use Cookies
- VIII. Your Rights Relating to Personal Information
- IX. Protection of Minors’ Personal Information
- X. Formulation, Effectiveness and Update of this Policy and Others

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 customers of which you are representative or with which**

you have a relationship (“Relevant Customers”) and us, such other agreements or terms and conditions shall prevail.

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 physical, electronic 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. The secure area of our website supports the use of Secure Socket Layer (SSL) protocol and 128-bit encryption technology - an existing industry standard for encryption over the Internet to protect data. When you provide personal sensitive information through our website, 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.
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 Related Customers’ express 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 abide by our personal information protection policy and security standards when processing 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 your use of our digital banking services, you shall notify us immediately so that we may take appropriate measures to prevent further loss from occurring.

6. 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 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 about the security incident by email, mail, call, SMS, push notification or through other methods as appropriate in a timely manner. Where it's 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. In order for us to provide Relevant Customers with digital banking services 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 following purposes or functions:

| Purposes or Functions | Information We Need to Collect |
|--|---|
| Registering digital banking service account | Your name, birth day, employer name, email/telephone number/mobile phone number for working purpose, employer's address |
| Logging onto digital banking services or retrieving logon password. | Your user name/logon name, security question and answer, 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 |
| Basic functions of digital banking services, including money receiving, payment or transfer, | Your name, email/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. |

| | |
|---|---|
| provision of bank statement/voucher, online trade services etc. | |
| Maintaining proper and secure operation of digital banking services, preventing and controlling digital banking services related risk | <p>Your device type, operating system, unique device identifier, software version, logon IP address, internet service provider (ISP), device accelerators (such as gravity sensing devices, etc.)</p> <p>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.</p> |

The above information is the basic information we must collect to provide Relevant Customers with digital banking services and to comply with laws, regulations and regulatory requirements. If you refuse to provide those information, you or Relevant Customers will not be able to use our regular digital banking services.

- You may decide, at your free choice, 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 for the following purposes or functions:

| Purposes or Functions | Information We Collect |
|--|---|
| 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 |
| Fingerprint or facial biometrics recognition functions | <p>Your fingerprint and/or facial biometrics information</p> <p>The above information is used only for identity recognition, or verification of logon application, and we will not collect your original fingerprint or facial image.</p> |
| Message service functions | Device type, unique device identifier, geographic location information |

| | |
|---|--|
| WeChat appointment for account opening | Name, email/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 in front and back side |
| 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. <u>We will conduct analysis on those information and will contact you or provide you or Relevant Customers with relevant response, service or products based on those information.</u> |

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.

- 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 |
|--|---|
| Fingerprint logon | Identity recognition, logon, and verification using fingerprint(s) |
| Face ID | Identity recognition and logon using face ID (applicable to some type of Apple device) |
| WeChat | Related functions on WeChat account service |
| Camera | Facial recognition (applicable to some type of Apple device) |
| Location | Security verification, push messages |
| Telephone | Dial the phone number of branches to enquire about banking business by one-touch |
| Notifications | Push messages with alerts, sounds, and icon tags |
| Function of checking call status and mobile network information | Maintain proper and secure operation of digital banking services, prevent and control fraud risk, dial the phone number by one-touch, and access to network |

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.

4. **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 of third party service provider | Scope, function and purpose of information collection |
|--|---|
| AppDynamics SDK | In order to count and analyze the performance of digital banking services, we will use AppDynamics SDK to obtain your mobile phone IP, device manufacturer, mobile phone model, network type and visit period. |
| Tealium SDK | In order to count page view volume and analyze user’s behaviors, we will use Tealium SDK to obtain your mobile phone IP, device manufacturer, mobile phone model, network type and browser type. |

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.

5. **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, through reminders on pages, interaction with you/Relevant Customers or agreements entered into with you/Relevant Customers, and obtain consent from you or Relevant Customers for that. We will collect, 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 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 or execute 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 reduce of risks, recording or filing purposes;
 - (3) 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 personally 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 scope and 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 obtain consent from you or Relevant Customers before using your personal information for such additional purposes.

IV. How We Store Your Personal Information

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.

After the retention period expires, we will destroy, delete or anonymise relevant information, **except for the information that 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. To Whom We 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, 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, bank card organisations, credit rating agencies, credit reference agencies (including without limitation, the People's Bank of China's 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;
- (9) any party in connection with any business/asset transfer, restructure, disposal (including securitisation), merger, spin-off or acquisition transactions of the Bank.

Such provision or disclosure will involve cross border transmission of personal information, including information being transmitted to or being accessed from overseas only when the above recipient(s) is an overseas institution/person. 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.

2. Transfer

Without your express consent, we will not transfer your personal information to any other company, organization or individual, except in the case of business/asset transfer, restructure, disposal (including securitization), merger, spin-off or acquisition transactions where the transfer is necessary. Where any personal information is transferred, we will request the receiving company, organization or individual to comply with this Policy. Otherwise, they shall obtain separate consent from you.

3. Public Disclosure

We will not disclose your personal information to the public unless we have your explicit 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 Collection, Use and Disclosure

To the extent allowed by laws and regulations, we may collect, use or disclose your personal information without your consent under the following circumstances:

- (1) **where it directly relates to state security or national defence security;**
- (2) **where it directly relates to public security, public sanitation or major public interest;**
- (3) **where it directly relates to criminal investigation, prosecutions, trials or execution of rulings, etc.;**
- (4) **when it's urgently required to protect your or other's life, property or relevant material legal rights and interests while difficult to obtain your authorisation or consent;**
- (5) **where the information is made available to the public by yourself;**
- (6) **where the information is from the legitimate public sources, like the legitimate news report, information disclosure by government or other authorities;**
- (7) **where it's required by performance of obligations set out in laws or regulations, or of obligations for financial compliance; or**
- (8) **where it's necessary to enter into or perform the contracts at your request.**

VII. How We Use Cookies

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". Cookies are small bits of information automatically stored on your local terminal, which can be retrieved by your local terminal. Cookies can enable our website or applications to recognise your device and store information about your use of website and/or applications so to provide more useful features 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.

The information collected by us via above method is anonymous aggregated data, and contains no name or address information or any information that will enable anyone to contact you via telephone, email or any other means.

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.
2. You have the right to check with us whether we hold your personal formation and to check the personal information you have provided to us.
3. You have the right and obligation to update your personal information with us to ensure all information be 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.
4. In relation to personal credit or 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.
5. 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.
6. 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. 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.

7. **How to contact us**

Requests for access to, correction or deletion of personal information, for withdrawal of authorisation or disposal of personal information beyond retention period, for a copy of this Policy, or enquiries about our practices regarding personal information and privacy protection, should be addressed to:

Chief Data Officer

HSBC Bank (China) Company Limited

19/F HSBC Building, Shanghai IFC, 8 Century Avenue, Pudong, Shanghai, 200120

E-mail: hsbcaoc@hsbc.com.cn

Tel: +86 400-820-3090 (8:30am - 5:30pm, Monday to Friday during the working days)

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 illegal, noncompliant, unnecessarily repeated, unreasonable or technically impracticable requests. Due to the requirements of law and regulation, we may not be able to respond to your request under any of the following circumstances:

- (1) **where the request is in direct relation to state security or national defence security;**
- (2) **where the request is in direct relation to public security, public sanitation, or major public interests;**
- (3) **where the request is in direct relation to criminal investigations, prosecutions, trials, execution of rulings, etc.;**
- (4) **where there is sufficient evidence that you are intentionally malicious or abuse your rights;**
- (5) **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**
- (6) **where the request involves any trade secret.**

8. You may supervise or make suggestions for our practices regarding personal information and privacy protection, and lodge complaints or demand compensation 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, 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.

9. Nothing in this Policy shall limit the rights you should have as a Personal Information Subject under Chinese law.

IX. Protection of Minors' Personal Information

1. We pay particular attention to protection of the minors' personal information. We have no intention to collect any minors' personal information, unless it is agreed by their parents or guardians and it is necessary for the products or services offered to the minors (for example, the minors may be the holders of the Junior Account offered by us, the holders of supplementary card of certain credit cards issued by us, the beneficiaries of the insurance products that we distribute, the heirs of our customers, etc.).
2. **If you are under 18 years of age, it is suggested that your parents or guardians should carefully read this Policy and any of your personal information should be provided only after seeking consent from them. Meanwhile, it is suggested that your use of our products and services should be under the guidance of your parents or guardians. If they do not agree you to provide your personal information or to use any of our products or services, you should immediately stop providing the information or stop using our products and services. Please notify us of such event as soon as possible, so as to allow us to take appropriate measures accordingly.**
3. If you are under 18 years of age, for those personal information we collect with the consent of your parents or guardians, we will only use or disclose such information to the extent allowed by law and regulation or expressly consented by your parents or guardians or necessary for protection of the minors' interests.

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

1. **The Policy is made by us and published at our digital banking services related websites or applications and takes effect on the date of issue.** 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 services 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 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 use his/her information.** 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.