Personal Information Protection Policy for Third Party Vendor

Date of Update: 9th May2026
Effective Date: 9th May 2026

This Personal Information Protection Policy ("**Policy**") applies to vendor-related personal information of an external third-party vendor ("**Vendor**" or "**Your Company**" or "**you**") in connection with the provision of services to the entities of HSBC Group in Mainland China ("**HSBC**" or "**we**" or "**us**") listed in Annex I. We will process the personal information of Your Company's relevant personal information subject ("**Connected Person**" or "**Personal Information Subject**") in accordance with this Policy. For the purposes of this Policy, a Connected Person or Personal Information Subject means any person who has a relationship with Your Company, including but not limited to any director, supervisor or employee of the company, partner or member of a partnership, shareholder, any substantial owner, controlling person, designated account holder, designated payee, representative, agent or nominee of Your Company, or any other individual who is relevant to Your Company's relationship with the HSBC Group.

Please read this Policy carefully before providing personal information to us, and please ensure that the relevant Personal Information Subject is aware of this Policy and should specifically inform the person how we will handle their personal information and obtain the relevant authorization and consent of such person. Your Company may remind the person to read this Policy in advance, or you may provide the person with a copy of this Policy.

IMPORTANT: Please do not submit Your Company's personal information if Your Company does not consent to the following provisions stated in this Policy. Please pay particular attention to the provisions that are bolded and underlined which we think have material impacts on the rights of Your Company/Connected Persons and/or deal with sensitive personal information of Your Company/Connected Persons.

Personal Information Protection Policy Overview

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

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

I. How We Protect Your Connected Person's Information

1. Information security is our top priority. We will always endeavour to safeguard your Connected Person's 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 Connected Person's information. We will take responsibility in accordance with the law if your Connected Person's information suffers from unauthorised access, public disclosure, erasure or damage for a reason attributable to us and so impairs the lawful rights and interests of Your Company and/or Connected Person.

2. Our website supports advanced encryption technology - an existing industry standard for encryption over the internet to protect your Connected Person's information. When Your Company provides 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.

3. We maintain strict security system to prevent unauthorised access to your Connected Person's information. We exercise strict management over our staff members who may have access to your Connected Person's 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 Connected Person's 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 Company or Connected Person' separate authorisation or consent. 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 Connected Person's information.

5. **For the security of your Connected Person's information, you take on the same responsibility as us. You shall properly take care of your Connected Person's information, including the documents, devices or other media that may record or otherwise relate to such information, and shall ensure such 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 Connected Person's information and/or relevant documents, devices or other media have been disclosed, lost or stolen, or any other circumstances may otherwise affect your Connected Person's information security have occurred, 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, a 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 laws and regulations, 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 is difficult to notify each vendor, we will post public notice in a reasonable and effective way. Please inform the relevant affected Connected Persons of the situation in accordance with applicable laws and regulations in a timely manner. Meanwhile, we will report such personal information security incident and our actions to the relevant authorities in accordance with applicable laws, regulations and requirements of the authorities.

II. How We Collect Your Connected Person's 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 includes name, birth date, ID certificate information (ID card, passport, etc.), personal biometrics recognition information, contact information, address, account information, property status, location, 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, etc.), personal biometrics recognition 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).

2. **Information We May Need to Collect**

a) When you apply to become our vendor, we may collect the following personal information about Your Company:

Purposes or Functions	Information We May Need to Collect
In order to communicate with Your Company, evaluate and manage vendor setup, conduct due diligence during the vendor on-boarding phase	(1) The name of the Vendor's legal representative. (2) Name, contact information (including fixed telephone number, mobile phone number, email address) and current position of the Vendor's contact person. (3) If the compliance risk rating of the procured services is high or very high after the completion of an internal inherent risk assessment, we need to further collect the name, date of birth, gender, nationality and identity **ID certificate information (including certificate type, number)** of the following individuals: ● the ultimate beneficial owner (natural person) of Your Company who has more than or equal to 10% equity, voting rights or property (including bearer stock, capital and profits) ; ● All senior management and executive directors of Your Company.

b) When Your Company becomes our vendor, we will use the personal information obtained during the above on-boarding process to further manage the conclusion and performance of the relevant agreement between Your Company and us. In addition, we may need to further collect the following related personal information about Your Company:

Purposes or Functions	Information We May Need to Collect
In order to conclude and perform the relevant contracts/ agreements between HSBC and Your Company	(1) Information about the staff assigned by Your Company to provide on-site services to HSBC • Name, nationality, gender, date of birth, **ID certificate information (including certificate type, number, date of expiry, issue**

	country/region), • As per the service nature, we may further collect background vetting information, including identity verification, working experience, current residential address, **criminal check (where legally permitted or required), any negative news available on public social media, credit reference check (only applicable when your staff have resided in the relevant country/territory for a period of six months or more within the last five years and we are legally permitted to do so),** confirmation of educational and other necessary qualification, **sanction check, any relationship with PEP and relevant information, whether you are subject to any legal or regulatory restriction which may affect your staff's provision of services, entries in local fraud databases (if any).** (2) Other staff and contact person's information provided by Your Company in the process of performing the agreement, including name, contact information (including fixed telephone number, mobile phone number, email address) and current position. (3) If the compliance risk rating of the procured services is high or very high after the completion of an internal inherent risk assessment, we need to further collect the name, date of birth, gender, nationality and **identification certificate information (including certificate type, number)** of the following individuals: • the ultimate beneficial owner (natural person) of Your Company who has more than or equal to 10% equity, voting rights or property (including bearer stock, capital and profits) ; • All senior management and executive directors of Your Company.

3. For the purposes described in this Policy, we may receive and keep the personal information proactively provided by Your Company/Connected Person, or, in

accordance with laws, regulations, regulatory provisions, or the authorisation or consent of Your Company/Connected Person, collect, enquire, and verify by proper methods your Connected Person's personal information from/with members of the HSBC Group or other third parties (including but not limited to credit reference agencies, information service providers, relevant authorities, contact persons and other entities/individuals). "HSBC Group" under this Policy means HSBC Holdings plc, and/or any of its affiliates, subsidiaries, associated entities and any of their branches and offices (together or individually), and "member of the HSBC Group" has the same meaning.

4. The personal information we collect may be in paper, electronic or any other forms.

III. How We Use Your Connected Person's information

1. We may use your Connected Person's information for the following purposes:

(1) to realize the purposes and functions mentioned in above Article II of this Policy "How We Collect Your Connected Person's information" and below Article VI of this Policy "Special Circumstances for Information Processing";
(2) to comply with any Applicable Laws ("Applicable Laws" refer to any applicable statute, law, regulation, ordinance, rule, judgment, decree, voluntary code, directive, sanctions regime, court order applicable to any member of the HSBC Group, agreement between any member of the HSBC Group and an authority, or agreement or treaty between authorities and applicable to HSBC or a member of the HSBC Group) and any order or requirement from any authority;
(3) to perform our and/or the HSBC Group's compliance obligations (including regulatory compliance, tax compliance and/or compliance with any Applicable Laws or requirements of any authority), or to implement any policy or procedure made by us and/or the HSBC Group for the performance of compliance obligations.
(4) for our third party risk management, business operations and management needs, including but not limited to monitoring and reviewing HSBC's supplier services procurement process, global operations, system or product development, audit, etc.;
(5) manage financial crime risk, prevent or prohibit illegal or non-compliant activities, control or reduce risks, detect, investigate and prevent any actual, suspected or potential financial criminal activities (including money laundering, terrorist financing, bribery, corruption, tax evasion, fraud, evasion of economic or trade sanctions, and any act or attempt to circumvent or violate any applicable norms relating to such matters) (including the possibility of further inquiries or confirmation of the identity and status of the relevant individuals or entities and whether they are subject to the sanctions regime)
(6) if applicable, collect from you any amounts due and unpaid;
(7) exercise or maintain our rights.

2. **The above information collection and use in this Policy shall not impact our use of your Connected Person's information for purposes as otherwise agreed between you and us.**

3. If we use your Connected Person's information for purposes other than the purposes as set forth in this Policy or in other agreement between you and us, we shall inform you how we use this information and obtain your consent before using your Connected Person's information for such additional purposes as per applicable laws and regulations.

IV. How We Store Your Connected Person's Information

Since we use global purchasing, account payable and risk management system which means that to the extent permitted by regulatory rules and applicable laws, your Connected Person's information may be transferred to and/or stored in the foreign jurisdictions, or be accessed from these jurisdictions. Up to now, the names and contact details of our overseas trustees are as follows: 1) HSBC Global Services (Hong Kong) Limited (contact: hkdpo.enquiry@hsbc.com.hk); 2) HSBC Global Services (UK) Limited (contact: ico.correspondence@hsbc.com). If we transfer your Connected Person's 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 Connected Person's information will be protected by a strict code of secrecy and security which we, other members of the HSBC Group and their staff, and third parties are subject to.

We comply with applicable laws and regulations on data storage and keep your Connected Person's information for the shortest time necessary to meet the purpose of information collection. For example, if we enter a contract with Your Company, any personal information we collect will be retained for 30 years from the expiration date of the contract with Your Company. We have a data retention policy that determines the specific retention period for each type of information based on different service scenarios and the nature of the service. At the end of the corresponding retention period specified in this Policy, we will destroy, delete or anonymize the relevant information. Alternatively, we will store your Connected Person's information in a safe and segregated way when it is impossible to destroy, delete or anonymize your Connected Person's personal information. **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 Your Company and us, or for record checks or enquiries from Your Company, regulators or other authorities.**

V. How We Entrust Processing, Share, Transfer and Publicly Disclose Your Connected Person's 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 Connected Person's 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 Connected Person's 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 or associated person of the HSBC Group (including their employees, directors and officers);**
(3) **any regulator of HSBC 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 your behalf according to your authorisation or in accordance with law (for example your legal advisers, contact persons);**
(5) **any party in connection with the transfer, reorganization, disposal, merger, spin-off or acquisition of business /assets involving us.**

Subject to applicable laws and regulations, we will seek separate consent from Your Company or your Connected Person (if legally required) and notify Your Company or your Connected Person of the data sharing/transferring arrangement, including the data receiver's identity, contact information, the purpose of processing, the method of processing, and the types of personal information.

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

2. Transfer

Without the separate consent of Your Company or Connected Person, we will not transfer your Connected Person's information to any other company, organization or individual, except **in the case of any business/asset transfer, restructure, disposal, merger, spin-off or acquisition transactions involving us where the transfer is necessary. In such circumstances, we will inform Your Company**

or Connected Person of the name and contact method of the data recipient as per applicable laws and regulations as well as request the personal information recipient to continue to protect your Connected Person's information as per applicable laws and regulations. If the personal information recipient changes the data usage purpose and processing method, it shall obtain separate consent from Your Company or Connected Person.

3. Public Disclosure

We will not disclose your Connected Person's information to the public unless we have separate consent from Your Company or Connected Person, except where we are mandatorily required to do so in accordance with applicable laws and regulations, judicial or legal proceedings, or mandatory administrative enforcement by the authorities.

VI. Special Circumstances for Information Processing

We will process your Connected Person's information (collection, storage, use, analysis, transfer, provision, disclosure) based on the consent of Your Company or Connected Person. To the extent allowed by laws and regulations, we may process your Connected Person's information without the consent from Your Company or Connected Person under the following circumstances:

(1) **where it is necessary for entering into a contract or the performance of a contract to which Connected Person is 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 Connected Person 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 the Connected Person;**
(6) **other circumstances stipulated by laws and regulations.**

VII. How We Use Cookies and Similar Technologies

1. Your Company or Connected Person visits, browses, uses of any of our website or mobile device applications may be recorded for analysis on the number of visitors to the site and/or applications, general use patterns and specific use patterns of Your Company/Connected Person and improving Your Company/Connected Person's 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 Company/Connected Person's device and store information about Your Company/Connected Person's use of website and/or applications so to provide continuous services to Your Company/Connected Person and to tailor the content of our website/applications to suit Your Company/Connected Person's interests. 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 and etc.

2. **Most local terminals are initially set to accept Cookies. Your Company or Connected Persons can manage or disable Cookies based on your/their own preference. Should Your Company or Connected Persons wish to disable the Cookies, you or they may do so by changing the setting on your or their local terminals. However, after changing the setting Your Company or Connected Persons may not be able to enjoy the convenience that Cookies bring, but Your Company or Connected Persons' normal use of other functions of your or their local terminals will not be affected.** Different local terminals offer different methods for setting changes, and Your Company or Connected Persons can find information on how to manage cookie settings on certain browsers via the following links.

   - Cookie settings in Chrome
   - Cookie settings in Firefox
   - Cookie settings in Microsoft Edge
   - Cookie settings in Safari

VIII. Your Connected Person's Rights Relating to Personal Information

1. Your Connected Persons have the right to request us to protect and secure their personal information in accordance with the provisions of the laws, regulations, and this Policy. They have the right to exercise their rights of individual granted by applicable laws and regulations.

2. Your Connected Persons have the right to check with us whether we hold their personal information as well as to access and copy their personal information.

3. Your Connected Persons have the right to change the scope of authorization or withdraw their consent, and exercise their right per the method listed in Article IX of this Policy "How to Contact Us". We will not further process the related information once Your Connected Persons change their authorization. Please note the withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

4. **Your Company has the right and obligation to update your Connected Person's information with us to ensure all information be accurate and up to date.** Your Connected Persons have the right to request us to provide convenience for them to update their personal information with us and to correct any of their personal information that is inaccurate.

5. Your Connected Persons have the right to request us to delete or otherwise properly dispose of their personal information that is beyond the retention period in accordance with the applicable laws and regulations, this Policy, and other agreement between you and us. If we cease our operation, we will stop collecting any personal information of your Connected Person's information in a timely manner, delete or anonymize all your Connected Person's information, and inform Your Company of such operation cessation via courier or public announcement, except as otherwise provided by laws and regulations or where the personal information deletion is technically impossible.

6. Nothing in this Policy shall limit the rights your Connected Person should have as a personal information subject under applicable laws and regulations.

IX. How to Contact Us

1. Requests for access to, copy, correction or deletion of personal information, for change/withdrawal of authorisation or disposal of personal information beyond retention period, or for a copy of this Policy, enquiries about our practices regarding personal information protection or exercising other rights you or your Connected Persons are granted by the laws and regulations, should be addressed to such contact person as listed out in Annex 1.

2. For security purposes, you Connected Persons may need to provide the request in written form via Your Company to prove their identity. We may request Your Company to verify your Connected Persons' identity before processing their request.

3. Upon the receipt of your Connected Persons' request, we will reply to them within 15 working days or shorter period as prescribed by laws and regulations (if any).

4. We will not charge fees for the processing of above-mentioned reasonable requests for checking, correcting or otherwise disposing of your Connected Person's information.

   Notwithstanding the foregoing, we may reject illegal, noncompliant, unnecessarily repeated request, request which needs excessive technical means (for example, the need to develop information systems or fundamentally change current practices) or brings risks to the legitimate rights and interests of others, or is unreasonable or technically impracticable.

Further, we may not be able to respond to part or all of your Connected Person's 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 Your Company or the Connected Person is intentionally malicious or abuses your/his/her rights;**
(6) **where the purpose is to protect the Connected Person or other individual's life, property and other substantial legal interests but it is difficult to acquire the consent of the Connected Person;**
(7) **where responses to Your Company's or the Connected Person's request will give rise to serious damage to the legal rights and interests of Your Company, the Connected Person or any other individual or organisation; or**
(8) **where the request involves any trade secret.**

5. Your company or Connected Person may supervise or make suggestions for our practices regarding personal information protection, and lodge complaints or demand compensation according to law against us or our staff for any infringement of the rights and interests in your Connected Person's information.

   If your company or Connected Person has any query, complaint, feedback, comment, suggestion, please contact us through the contact information listed in this Policy.

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

1. **The Policy is made by us and published on HSBC's relevant vendor management websites and/or applications and takes effect on the date of issuance.** This Policy may be amended and updated from time to time, in particular when the following material changes occur:

   (1) Material changes in our vendor management model or third-party staff information management model, such as changes to the purposes of processing personal information, the types of personal information processed, the manner in which personal information is used, etc.;
   (2) Material changes in our ownership structure, organisational structure, etc., such as changes as result of business adjustments, bankruptcy, mergers, etc.;

(3) Changes in the main recipients to whom personal information is shared, transferred or publicly disclosed;

(4) Material changes in the rights of your Connected Persons relating to personal information or in the methods to exercise such rights;

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

(6) other changes that may have a material impact on the personal information rights and interests of your Connected Persons.

We will post the changes to the Policy or the updated Policy through pop-ups or announcements, etc. on HSBC's relevant vendor management websites and/or applications. Changes to the Policy shall not diminish or limit the rights your Connected Person should have as a personal information subject under applicable laws and regulations.

2. If Your Company or Connected Person is also a customer of the HSBC Group, attention is drawn to the relevant personal information protection policy to customers.

3. Some links in our website may refer to websites of other companies, which may have their own privacy notices. The content may be different with ours. You need to make sure you are satisfied to their privacy notices when you are using other websites.

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

HSBC

Annex 1

List of HSBC Group Entities in the Mainland China and Contact Information

	Entity Name	Mailing Address	Zip Code	Contact Person	E-mail	Telephone
1.	HSBC Bank (China) Company Limited	HSBC Building, Shanghai IFC, 8 Century Avenue, Pudong, Shanghai, China	200120	Procurement Department	chn.sourcing@hsbc.com	021-38886325
2.	Beijing Miyun HSBC Rural Bank Company Limited	No.126-1, Xin Dong Road, Miyun, Beijing, China	101500	Procurement Department	chn.sourcing@hsbc.com	021-38886325
3.	Chongqing Dazu HSBC Rural Bank Company Limited	No.1 Beihuan Road(E) , Dazu, Chongqing, China	402360	Procurement Department	chn.sourcing@hsbc.com	021-38886325
4.	Chongqing Fengdu HSBC Rural Bank Company Limited	No.107, Pingdu Avenue(E), Sanhe Town, Fengdu, Chongqing, China	408200	Procurement Department	chn.sourcing@hsbc.com	021-38886325

5.	Chongqing Rongchang HSBC Rural Bank Company Limited	No. 3/5/7, Haitang Er Zhi Road, Changzhou Street, Rongchang, Chongqing, China	402460	Procurement Department	chn.sourcing@hsbc.com	021-38886325
6.	Dalian Pulandian HSBC Rural Bank Company Limited	1-2/F, No. 3 Nanshan Road, Pulandian, Dalian, Liaoning, China	116200	Procurement Department	chn.sourcing@hsbc.com	021-38886325
7.	Fujian Yong'an HSBC Rural Bank Company Limited	No.1211, Yan Jiang Road, Yong'an, Fu Jian, China	366000	Procurement Department	chn.sourcing@hsbc.com	021-38886325
8.	Guangdong Enping HSBC Rural Bank Company Limited	No.44, Xin Ping Middle Road, Enping, Guangdong, China	529400	Procurement Department	chn.sourcing@hsbc.com	021-38886325
9.	Hubei Macheng HSBC Rural Bank Company Limited	No.56 Yurong Street, Macheng, Hubei, China	438300	Procurement Department	chn.sourcing@hsbc.com	021-38886325

10.	Hubei Suizhou Cengdu HSBC Rural Bank Company Limited	No. 205, Lieshan Avenue, Ceng Du, Suizhou, Hubei China	441300	Procurement Department	chn.sourcing@hsbc.com	021-38886325
11.	Hubei Tianmen HSBC Rural Bank Company Limited	Building 3, Yin Zuo Di Jing Wan, Tianmen New City, Tianmen, Hubei, China	431700	Procurement Department	chn.sourcing@hsbc.com	021-38886325
12.	Hunan Pingjiang HSBC Rural Bank Company Limited	Room 101-102, 106, Commercial Pedestrian, Pingjiang, Yue Yang, Hunan, China	414500	Procurement Department	chn.sourcing@hsbc.com	021-38886325
13.	Shandong Rongcheng HSBC Rural Bank Company Limited	Room 2, No. 198, Chengshan Avenue (E), Rongcheng, Shandong, China	264300	Procurement Department	chn.sourcing@hsbc.com	021-38886325
14.	HSBC Electronic Data Processing (Guangdong) Limited	4-17/F, Office Tower 2 TaiKoo Hui, No. 381	510620	Procurement Department	chn.sourcing@hsbc.com	021-38886325

		Tianhe Road, Tianhe District, Guangzhou, Guangdong, China				
15.	HSBC Software Development (Guangdong) Limited	22/F, Office Tower 2, Taikoo Hui, No. 381 Tianhe Road, Tianhe District, Guangzhou, Guangdong, China	510620	Procurement Department	chn.sourcing@hsbc.com	021-38886325
16.	HSBC Life Insurance Company Limited	29th Floor, HSBC Building, No. 8 Century Avenue, China (Shanghai) Pilot Free Trade Zone Shanghai, China	200120	Procurement Department	chn.sourcing@hsbc.com	021-38886325
17.	HSBC FinTech Services (Shanghai) Company Limited	Room 406, No. 859-863, Huanhu West 1st Road,	200120	Procurement Department	chn.sourcing@hsbc.com	021-38886325

		Lingang New Area, Pilot Free Trade Zone, Shanghai, China				
18.	HSBC Insurance Brokerage Company Limited	Room 201, 2F, Tower 3, No.12 Anxiang Street, Shunyi, Beijing, China	101300	Procurement Department	chn.sourcing@hsbc.com	021-38886325
19.	HSBC Corporate Services (Shanghai) Limited	35/F HSBC Building, Shanghai IFC, 8 Century Avenue, Pudong, Shanghai, China	200120	Procurement Department	chn.sourcing@hsbc.com	021-38886325
20.	HSBC Qianhai Securities Limited	Unit 2201, 22/F, Qianhai Chow Tai Fook Finance Tower (Phase I), No. 66 Shu Niu Avenue,	518052	Procurement Department	chn.sourcing@hsbc.com	021-38886325

		Nanshan Subdistrict, Qianhai Shenzhen-Hong Kong Cooperation Zone, Shenzhen, China				
21.	HSBC Philanthropy Foundation Beijing	18/F Fortune Financial Center, No 5 Dongsanhuan Zhong Road, Chaoyang District, Beijing China	Procurement Department	chn.sourcing@hsbc.com	021-38886325	Procurement Department