Privacy Notice

ICBC (London) plc and Industrial and Commercial Bank of China Limited London Branch

Effective Date: April 2026

PUBLIC

Table of Contents

1 Introduction

ICBC (London) plc and Industrial and Commercial Bank of China Limited London Branch (collectively referred to as the 'Bank', 'us', 'our' or 'we') collect, hold and process personal data about individuals associated with our corporate customers, partners and counterparties which may directly or indirectly identify them. Wherever we have used 'you' or 'your', this means you, any authorised person on your account, or any other persons or entities relevant to the relationship you have with us.

The Bank primarily processes personal data to provide banking and financial services, maintain oversight and governance, and to comply with legal and regulatory obligations, including those relating to anti-money laundering and financial crime prevention.

We are committed to processing personal data lawfully, fairly, and transparently in accordance with applicable data protection laws, including UK General Data Protection (UK GDPR), Data Protection Act 2018 and Data (Use and Access) Act 2025.

This Privacy Notice outlines:

- What personal and special category of personal data we collect
- Where we obtain the personal data
- How and why we process personal data
- The lawful basis we rely upon for processing personal data
- How long we retain personal data
- With whom we share personal data
- Data protection rights and how to exercise them
- How to raise a complaint or contact us

2 Who are We

The Bank is a wholly-owned subsidiary and branch of Industrial and Commercial Bank of China Limited ('ICBC Limited' or 'ICBC Ltd' or 'the Parent Bank') with registered name of ICBC (London) plc and Industrial & Commercial Bank of China Limited, London Branch. Both entities are authorised by the Prudential Regulation Authority (PRA) and regulated by the Financial Conduct Authority (FCA) and the PRA.

The Bank is the Data Controller for the personal data it processes in connection with providing you with banking and financial services, meeting our legal, regulatory and contractual obligations and for any of our legitimate interests.

Who is a Data Controller?

The natural or legal person, public authority, agency or other body which, determines the purposes and means of the processing of personal data and is responsible for ensuring compliance with data protection laws.

In some circumstances, we may share your personal data with other external parties who use it for their own purposes and act as independent data controllers. Where this is the case, those organisations are responsible for providing you with information about how they use your personal data and complying with their own data protection obligations.

If you have any questions about this notice or how we handle personal data, please contact us using the details below:

Registered Office

81 King William Street,
London EC4N 7BG

ICO Registration Number

ICBC (London) plc: Z7924761
ICBC London Branch: ZA076926

Privacy Mailbox

privacy@ld.icbc.com.cn

3 Who This Notice Applies To

This notice applies to the personal data of any natural persons (individuals) connected to your business who could be a director, officer, key controller or employee, any substantial owner or ultimate beneficial owner, introducers, trustee, settlors, administrators, sponsors, protectors / enforcers, guarantors, payment remitters, payment beneficiaries, your representatives (for example, authorised signatories or individuals you nominate to attend any corporate event organised by us), agents, nominees, or any other persons or entities with whom you have a relationship that's relevant to your relationship with us. The notice will continue to apply even if your relationship with us ends as we will continue to hold personal data to meet our legal, regulatory, complaint handling and record keeping requirements.

This notice should be read in conjunction with our terms and conditions specific to the product or service you avail from us.

Before you (or anyone on your behalf) provide information about an individual connected to your business to us, you must make sure that you have an appropriate lawful purpose or an agreement with the relevant individual. You must also inform those individuals and ensure they've been provided a copy of this notice.

Part of this notice also applies to the Bank's retail customers. The Bank previously provided retail banking services to individual customers, but has ceased to provide this service now. This notice applies, on a limited basis, to those former retail customers solely because we continue to hold your personal data for record retention, legal, regulatory and complaint-handling purposes.

4 What Personal Data We Collect

What is Personal Data?

Personal Data refers to any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly.

The categories of personal data we collect are set out below. We only collect data that is relevant and necessary for the purpose for which it is being used. The categories below are referenced in Section 7 where we explain why we process personal data.

Categories of Personal Data	
General Personal Data	• Full Name • Date of Birth • Gender • Nationality • Place of Birth • Phone Number • Email Address • Country of Residence • Country of Domicile • Full Residential Address • Occupation Details
Data About Your Identity	• Passport • Ethnicity (incidentally) • Driver's License • National Insurance Number • National ID • Social Security Number • Signature • Bank Account Number and Statement • Utility Bill • Council Tax Bill
Financial Data	• Source of Wealth • Source of Income / Funds • Ownership Details • Bank Account Number and Customer Number • Tax ID and Residency • Customer ID (Retail Customers only) • Transaction Details and Balance (Retail Customers only) • Interest Received (Retail Customers only) • Tax Deductions (Retail Customers only)
Corporate Role and Biography	• Biography/Career History/CV • Directorship Information • Job Title and Designation • Corporate Phone Number • Corporate Email Address
Device and System Access Data	• User ID • Device ID • IP Address • Banking Platform Login Details (Date and time of login, web browser used, browser language, and data volume transmitted)

Communication and Surveillance Data	• CCTV Recordings • Chat Records • Telephone Recordings • Email Communications • Letter of Correspondence
PEP, Sanction Screening, and Criminal Records Data	• PEP Status • Global Fraud and Sanctions • Criminal Convictions and Offences • Adverse Media Reports • Sanction Check Conclusions and Rating
Gifts and Hospitality, and Corporate Event Data	• Travel Itinerary • Travel Preference • Flight Number • Gift and Hospitality Register • Dietary Preference

5 What Special Categories of Personal Data We Collect

What is Special Category of Personal Data?

Personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

To the extent permitted by law, we collect and process a limited amount of special category of personal data and data related to criminal convictions and offences in specific circumstances. Within this category, we collect and process information relating to,

- **Criminal Convictions and Offences:** For performing customer due diligence on prospective, new and existing customers, sanction screening, and management reporting on due-diligence.
- **Ethnicity Data (Incidental)**: We may in some circumstances, incidentally receive information that could reveal the ethnicity of an individual; for example, from a copy of your passport or other identification document provided to us. We do not use this information to make any decision about you.
- **Dietary Preference**: For corporate events, we process dietary requirements which may reveal health conditions, religious beliefs or philosophical views. This data is only processed for providing appropriate and safe catering and not used beyond these purposes.

6 Where We Obtain Your Personal Data

We collect personal data about you from various sources. In most cases, we obtain your personal data from the corporate entity (or any other persons or entities authorised to act on their behalf) you are associated with during account opening, periodic customer reviews, providing banking and financial services and when participating in corporate events such as conferences, hospitality events and roadshows.

We also receive data directly from you when you interact with us through our banking platforms (for example, Internet Banking, Mobile banking, or other apps issued by the Bank), call us, email us, write to us, chat with us, sign contracts, or attend corporate events such as conferences, hospitality events and roadshows.

We may also receive personal data about you from other sources when necessary as detailed below.

6.1 Personal Data We Receive from Indirect Sources

In some circumstances, we collect your personal data indirectly from external sources, as part of providing banking and financial services, combating fraud and money laundering and provide you secure banking platform, for example:

- ICBC Limited (Parent Bank)
- Screening Tools and Databases (for example, World-Check One, Dow Jones, Orbis, Banker Almanac etc.)
- PEP list, provided by our consultant or advisors
- Company Register (for example, UK Companies House)
- Official Government Sanction Lists and Regulatory Watchlists
- Public Domains and Registers such as corporate websites, regulatory websites, annual reports, etc.
- Deal Platforms (for example, Debtdomain, SyndTrak)
- Other Financial Institutions and Counterparties (for example, Correspondent Banks, Agent Banks, Lenders, Borrowers etc.)
- Professional Networks and Referrals (Primarily for relationship building and networking)
- Monitoring devices or other means (for example, CCTV system, mobile phone recordings, desk phone recordings, SMS logs, chat transcripts, Bloomberg chats, email logs, logs from banking platforms provided for your use) deployed by the Bank to meet information security, regulatory and physical security requirements of the Bank

7 Why We Process Your Data and What is Our Purpose

How to read this section?

This section explains, why we use personal data, which categories of data from Section 4 are involved, and the lawful basis we rely on. The three main lawful bases the Bank uses are: (1) Compliance and Legal Obligations - we must process the data to comply with the regulations and law; (2) Contract Requirements - processing is necessary to perform or enter into a contract; (3) Legitimate Interests - processing is necessary for our legitimate business interests, provided these are not overridden by rights and interests of individuals. We do NOT rely on Consent as a lawful basis for any processing, with the sole exception of dietary data collected as part of corporate events. You can withdraw your consent to process this information before the event by contacting us at ***privacy@ld.icbc.com.cn*** *or your point of contact for the event. If you chose not to provide dietary details, we will be unable to guarantee that a meal that meet your specific requirement will be available.*

7.1 Establish Customer Relationship, Customer Onboarding, Account Opening and Provide Banking Services

We process your personal data to open and manage banking accounts, establish and maintain our relationship with the corporate entity you are associated with, carry out your instructions, and to provide banking services, including a secure banking platform for your day-to-day banking needs.

Purpose of Processing	Categories of Personal Data	Lawful Basis (UK GDPR / DPA 2018)
Verifying the identity of individuals associated with a corporate customer to establishing and maintain banking relationship.	General Personal Data, Data About Your Identity, and Corporate Role and Biography	• Compliance and Legal Obligations
Setting up the customer accounts and users on our banking platforms (Core Banking System, Online Platforms, Mobile Banking etc,).	General Personal Data, Data About Your Identity, Corporate Role and Biography, and Device and System Access Data	• Legitimate Interest
Provide a secure banking platform for you to meet your banking needs.	Device and System Access Data	• Legitimate Interest
Enter into and perform the credit agreement, manage and administer credit.	General Personal Data, and Data About Your Identity	• Contractual Requirements
Customer complaints management and maintaining ongoing correspondence with customers.	General Personal Data, Financial Data, and Communication Data	• Compliance and Legal Obligations
Maintain records of the exited retail business for preserving audit trail, responding to customer complaints and maintaining accounts in suspended state if customers could not be reached for full closure. *Note: This process is applicable for the retail customers of the Bank*	General Personal Data, Financial Data, and Data About Your Identity	• Compliance and Legal Obligations

7.2 Due-Diligence, Financial Crime Prevention, AML and Regulatory Surveillance

We are required by law to take steps to prevent and detect money laundering, terrorist financing, fraud, bribery, corruption, and other financial crimes. This includes carrying out due diligence on all individuals associated with our customers, screening against sanctions and watchlists, and monitoring transactions and customer relationships on an ongoing basis.

Purpose of Processing	Categories of Personal Data	Lawful Basis (UK GDPR / DPA 2018)
Conduct due-diligence, financial crime review and anti-money laundering checks throughout customer engagement lifecycle.	General Personal Data, Data About Your Identity, Corporate Role and Biography, Financial Data, and PEP, Sanction Screening, and Criminal Records Data	• Compliance and Legal Obligations. • Criminal Convictions: DPA 2018 Schedule 1 (Preventing or detecting unlawful act, regulatory requirements relating to unlawful acts and dishonesty)
Assess the effectiveness and accuracy of the systems used for financial crime prevention and sanction screening	General Personal Data, Corporate Role and Biography, PEP, Sanction Screening, and Criminal Records Data	• Legitimate Interest

Purpose of Processing	Categories of Personal Data	Lawful Basis (UK GDPR / DPA 2018)
		• Criminal Convictions: DPA 2018 Schedule 1 (Preventing or detecting unlawful act, regulatory requirements relating to unlawful acts and dishonesty)
Assess gifts and hospitality register for preventing bribery and corruption.	General Personal Data, and Gifts and Hospitality and Corporate Event Data	• Compliance and Legal Obligations
Conduct surveillance of communication to detect fraud, insider training, market abuse, and misconduct.	General Personal Data, and Communication Data	• Compliance and Legal Obligations

7.3 Regulatory Reporting to Authorities

As an FCA and PRA-regulated bank, we are required to submit regular reports to a range of regulatory authorities. These reports may include personal data about individuals associated with our customers.

Purpose of Processing	Categories of Personal Data	Lawful Basis (UK GDPR / DPA 2018)
Provide regulatory reports for areas such as deposit guarantee scheme, financial crime, disqualified person, tax, interest paid to individuals as required by Bank of England (BoE), Home Office, PRA and HM Revenue and Customs (HMRC).	General Personal Data, Financial Data, and Data About Your Identity	• Compliance and Legal Obligations

7.4 Payments Processing

We process personal data in connection with the payment services we provide to corporate customers, including processing incoming and outgoing payments on behalf of our customers.

Purpose of Processing	Categories of Personal Data	Lawful Basis (UK GDPR / DPA 2018)
Process payments between parties to ensure the correct and timely exchange of funds.	General Personal Data, Financial Data, and Data About Your Identity	• Compliance and Legal Obligations

7.5 Business Development and Corporate Events

We process personal data to maintain and develop our customer relationships, market our banking services to existing and prospective customers, and manage participation in corporate events such as conference, office visits, hospitality events, roadshows and other customer-facing activities.

You have an absolute right to object to the Bank's use of your personal data for marketing and corporate events at any time. To exercise this right, you can notify your relationship manager or reach out to us using the contact details in Section 2.

Purpose of Processing	Categories of Personal Data	Lawful Basis (UK GDPR / DPA 2018)
Manage relationships, engage with potential customers, and identify and pursue future opportunities, including roadshows.	General Personal Data, and Corporate Role and Biography	• Legitimate Interest
Promote new syndications to potential lenders. The dietary details are collected to provide you will meals that meet your specific requirements when you attend business development or corporate events.	General Personal Data, Corporate Role and Biography, and Gifts and Hospitality and Corporate Event Data	• Contractual Requirements • Dietary Preference: Explicit Consent*
Support the delegations coming from ICBC Limited (Parent Bank) to comply with UK VISA requirements.	General Personal Data, and Data About Your Identity	• Legitimate Interest

*You can withdraw your consent to process this information before the event by contacting us at **privacy@ld.icbc.com.cn** or your point of contact for the event. If you chose not to provide dietary details, we will be unable to guarantee that a meal that meet your specific requirement will be available*

7.6 Internal Governance and Oversight, Group and Management Reporting, Risk Management, and Audit

We process personal data to fulfil our internal governance, management reporting, audit and risk management obligations, including ICBC Limited's (Parent Bank) oversight and reporting, and to maintain our business continuity capabilities.

Purpose of Processing	Categories of Personal Data	Lawful Basis (UK GDPR / DPA 2018)
Support Bank's internal governance and senior management oversight through reporting.	General Personal Data, PEP, Sanction Screening, and Criminal Records Data, and Financial Data	• Legitimate Interest • Criminal Convictions: DPA 2018 Schedule 1 (Preventing or detecting unlawful act, regulatory requirements relating to unlawful acts and dishonesty)
Support the Bank's internal audit plan.	General Personal Data, and Financial Data	• Compliance and Legal Obligations
Maintain Head Office oversight through reviews, reporting and audits.	General Personal Data, Data About Your Identity, Corporate Role and Biography, Financial Data, PEP, Sanction Screening, and Criminal Records Data	• Legitimate Interest
Facilitate IT systems for banking operations, customer user, and maintain a secure IT environment.	General Personal Data, Financial Data, Device and System Access Data, and Communication Data	• Legitimate Interest
Maintain key professional contacts of counterparties and other external stakeholders to coordinate during a business continuity scenario.	General Personal Data	• Legitimate Interest

7.7 Security Surveillance of the Premise

We process personal data to ensure the safety and security of the Bank's premise.

Purpose of Processing	Categories of Personal Data	Lawful Basis (UK GDPR / DPA 2018)
CCTV monitoring of the Bank's premise as the Bank has a legitimate interest to ensure safety and security of the staff, visitors and other individuals in the premise and also to restrict access of the premise to authorised individuals.	General Personal Data, and Communication and Surveillance Data	• Legitimate Interest

In many instances, the provision of your personal data is a legal or contractual requirement for providing you with banking services. If the required personal data is not provided, we may be unable to open your account, continue the business relationship with your corporate entity, execute the requested transaction, or provide you with the required banking services.

The above tables list the category of personal data used for each processing. For further information on the specific personal data used please contact us using the details provided in Section 2.

8 Keeping Your Information Secure

The Bank takes appropriate technical and organisational measures, to keep your information safe and secure, which may include data governance frameworks, information security and data security policies, data encryption, access controls, incident management, mandatory information and data protection trainings, IT security monitoring and other forms of data protection measures.

In the event of a personal data breach which is likely to result in a high risk to your rights and freedoms, the Bank will notify the relevant corporate entity without undue delay and also inform you directly.

9 How Long We Retain Your Personal Data

The Bank retains personal data only for as long as required to satisfy the purpose for which it was collected in line with the Bank's retention policy. The retention policy reflects our legal, regulatory and contractual obligations.

In general, we retain any personal data for a period of up to 6 years from the end of our relationship with you or your corporate entity or after the completion of the settlement. Personal data collected as part of due-diligence, sanction screening, transaction monitoring, and suspicious activity are however kept only for a period up to 5 years after the relationship has ended.

In certain cases, due to legal, regulatory, and Parent Bank obligations, we may need to retain the personal data for a longer period; for example, ongoing legal matters, disputes, investigations or any other legitimate interest of the Bank.

Where personal data is no longer needed for the purpose for which it was collected and there is no other legal or regulatory obligation, the Bank will securely delete personal data at the earliest practically possible opportunity.

10 Who We Share Your Personal Data With

The Bank may share personal data with ICBC Limited (Parent Bank) and external parties where this is necessary to operate the Bank's business, provide banking services, provide technology capability, meet legal and regulatory obligations, and protect the Bank, our assets, employees, and customers. The Bank only shares personal data where there is a lawful basis, and appropriate measures such as non-disclosure agreements, secure transfers, and confidentiality obligations are put in place as required.

10.1 Data Processors of the Bank

Who is a Data Processor?

A natural or legal person, public authority, agency, or other body that processes personal data on behalf or on the instruction of the Data Controller, in this case, the Bank.

The Bank has appointed a number of data processors and also shares with / receives from them personal data to the extent required for them to provide us the necessary services. The following are the categories where we use data processors:

- ICBC Limited (Parent Bank) who provides technology capability, IT systems, online banking and mobile banking platforms
- Deal platforms to facilitate sharing of KYC information as part of syndications
- KYC and AML screening platforms such as Dow Jones and World-Check One
- Consultants and advisors for reviewing the effectiveness of the systems used for financial crime prevention and sanction screening
- Preparing and submitting regulatory reports (for example, Regnology, Axiom)
- Data sharing service providers for disqualified person verification
- Electronic communication log management (for example, Bloomberg, BT and O2)
- Document archiving and shredding (for example, Restore Datashred)
- CCTV monitoring
- Building security pass administration
- Providing IT DR capability and data backup management
- Network and internet connectivity

The data processors appointed by the Bank are required to process the personal data in line with the data protection requirements of the Bank, which includes implementing appropriate technical and organisational measures. For any processing of personal data by the data processor to meet their legal and regulatory obligations, they will assume the role of an independent data controller.

10.2 Data Recipients (Independent Controllers)

The Bank shares personal data with organisations that receive and use it for their own purpose. In this scenario, the organisation we share your data with will act as independent data controllers and is responsible for providing you with information about their processing and complying with their own data protection obligations.

Examples of such data recipients are:

- ICBC Limited (Parent Bank)
- Bank's external auditors
- Other Financial Institutions and Counterparties (for example, SWIFT, Correspondent Banks, intermediary Banks, Agent Banks, Lenders, Borrowers etc.) as part of providing banking and financial services
- Government bodies, regulators, law enforcement agencies, courts and similar organisation such as BoE, PRA, FCA, HMRC, National Crime Authority, Home Office etc. as part of our legal, regulatory and public duty

In some circumstances, we may also share personal data upon having asked you or the individuals connected to your business for your permission to share it, and you (or they) have agreed, including with ICBC Group entities

11 Cross Border Data Transfers (Restricted Transfer)

What is Cross Border Data Transfer (Restricted Data Transfer)?

Any transfer of personal data to a separate organisation located outside the UK, which includes sending of personal data or making it accessible to a separate organisation outside the UK.

In the course of operating the Bank's business, providing banking services to customers, providing technology capabilities and meeting legal and regulatory obligations, the Bank may need to transfer your personal data outside of the UK, including to countries that may not have the same level of protection for personal data as in the UK.

Where this occurs, we ensure that appropriate safeguards are in place to protect your personal data in accordance with the UK data protection laws.

11.1 Transfer to Countries Within the EEA

Some of the Bank's data processors and data recipients are based in the European Economic Area (EEA). The UK government has recognised the EEA as providing an adequate level of protection to personal data. Transfers to these recipients are therefore permitted without additional safeguards. The data is transferred or made available as part of provisioning the KYC information to other ICBC entities, third party vendors who support in preparing and submitting regulatory reports.

11.2 Transfers to Countries Outside of the EEA

As a branch and subsidiary of ICBC Limited (Parent Bank), headquartered in China, the Bank may transfer certain personal data to the Parent Bank. This occurs where necessary for:

- Hosting and provisioning of IT systems, mobile banking and internet banking platforms from the Data Centre of ICBC Limited (Parent Bank)
- Meeting group-level compliance, reporting and oversight requirements
- Meeting the Group audit and risk management requirements

The categories of personal data shared or made available for access are General Personal Data, Data About Your Identity, Financial Data, Corporate Role and Biography, Device and System Access Data, PEP, Sanction Screening, and Criminal Records Data.

Some of the Bank's data processors maintain and store their data outside of the EEA, such as in the USA. The category of personal data shared is Bloomberg chats and any personal data stored in our deal platform. The Bank has put in place contractual measures for transfer to ICBC Limited (Parent Bank) in China

For transfer of personal data to countries which do not have full adequacy, the Bank ensures that appropriate safeguards (for example, data transfer agreements, UK-US Data Bridge) aligned with regulatory requirements are in place.

12 Your Data Protection Rights

Under the data protection law, you have the following rights in relation to your personal data. These are not absolute rights and may apply differently depending on the lawful basis for processing your personal data and any legal or regulatory obligations that apply to the Bank.

Data Subject Rights	What It Means	When It Applies and Exemptions
Right of Access	Access your personal data and receive a copy of the personal data the Bank hold about you, based on a reasonable and proportionate search.	Generally, applies for most processing. We may redact information that identifies other individuals, third parties or would prejudice legal proceedings.
Right to Rectification	Rectify any inaccurate personal data relating to you and also be able to have incomplete personal data completed based on the purposes for the processing. We will take reasonable steps to satisfy ourselves that the data is accurate and to rectify the data if necessary.	Generally, applies for most processing. May be limited where data accuracy is required for legal or regulatory compliance.
Right to Erasure	Erase your personal data in where the Bank have no lawful basis to continue processing it and there is no applicable exemption.	Exemption apply when the processing is required for • Compliance and Legal obligations • Establishment, exercise, defence of legal claims
Right to Restrict Processing	Restrict the processing of your personal data in certain circumstances, • Where you contest the accuracy of the personal data until we have taken sufficient steps to correct or verify its accuracy • Where the processing is unlawful but you do not want us to erase your personal data • We no longer require the personal data for the purposes of processing, but you require them to establish, exercise or defend a legal claim • Where you have objected to processing and we are determining the legitimate ground to continue processing	Exemption apply when the processing is required for • Establishment, exercise or defence of legal claims • Protection of the rights of another person or for public interest

Data Subject Rights	What It Means	When It Applies and Exemptions
	Where personal data is subjected to restriction, we will only process it with your consent or if an exemption applies.	
Right to Data Portability	You have the right to receive all personal data provided to us in structured, commonly used and machine-readable format and also to transmit to another controller where technically feasible.	The right applies where processing is based on consent or contract and carried out by automated means.

The Bank does not make solely automated decisions — all automated screening outputs (for example, carrying out fraud and money laundering checks) are reviewed by qualified human analysts with genuine authority to override any result.

Right to Object

You have them right to object to processing your personal data where we rely upon legitimate interests to process your personal data. If you object we will stop processing your personal data unless,

- We can either demonstrate compelling legitimate interests that override your interests, rights and freedoms; or
- We need to process the personal data for the establishment, exercise or defence of legal claims.

However, you have an absolute right to object to the Bank's use of your personal data for marketing and corporate events at any time; we will stop processing your data for these purposes immediately upon request without exception.

How to Exercise Your Rights

To exercise your rights, please submit a request via Bank's Privacy Email Box: ***privacy@ld.icbc.com.cn.*** *We will respond within one month of receiving a valid request, although this may be extended where requests are complex or numerous (we will notify you if an extension applies). The one-month period begins from the date we have verified your identity. We may pause the clock where we require further clarification about the request, we will notify you promptly if this applies.*

In some cases, we may be unable to fully comply with a request, for example, where:

- We must retain your personal data to comply with legal or regulatory obligations
- Disclosure would adversely affect the rights and freedom of other individuals
- An applicable exemption under UK data protection regulations exists

Where we would not be able to fully comply, we will explain the reasons and you have the right to complain.

13 How to Contact Our Data Protection Officer (DPO)

The Bank has appointed a Data Protection Officer (DPO) responsible for overseeing the Bank's personal data protection framework and ensuring compliance with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other applicable data protection laws.

You may contact the Bank's Data Protection Officer if you have concerns about the processing of your personal data, or any data protection issue which has not been addressed by the Bank.

The DPO's contact details and email address is as below:

Xiaoliang (Matthew) Zhang
Deputy General Manager &
Data Protection Officer (DPO)

Email: xiaoliang.zhang@ld.icbc.com.cn

DPO Mailbox

dpo@ld.icbc.com.cn

14 Your Right to Complain

If you have concerns about the Bank's use of personal data, you can first make a complaint to us using the contact details in Section 2, or escalate to the DPO. We will acknowledge complaints within 30 days and respond without undue delay.

You also have the right to lodge a complaint with the UK supervisory authority, Information Commissioner's Office (ICO) if you are not satisfied with the response or resolution provided by the Bank. ICO generally expects you to have raised your concerns with the Bank first.

The ICO contact details are as below:

Information Commissioners Office (ICO)

Make a Complaint Page:
https://ico.org.uk/make-a-complaint/

Helpline:
0303 123 1113

15 Notice of Changes to this Privacy Notice

The Bank may change or update this Privacy Notice from time to time to reflect changes in applicable data protection law, organisation structure, or new processing activities. Where changes are material, the Bank will take reasonable steps to inform and publish the updated Privacy Notice on our website. We would encourage you to visit our website regularly to stay informed of the purposes for which we process personal data and your rights to control how we process it. This Privacy Notice does not contractually bind us or any other parties.

This Privacy Notice was last reviewed and updated in March 2026 and is effective from April 2026.