

Customer Privacy Notice

First issued: 18 May 2018
Revised Version: 19 October 2026

Who We Are?

National Bank of Kuwait (International) PLC "**we**", "**us**", and "**ours**" or "**NBKI**" or "**NBK UK**") is a company registered in England & Wales with Company Number 02773743 and registered with the UK Information Commissioner's Office (ICO) with registration number Z6471287.

This Privacy Notice is prepared for customers of NBKI and explains who we are, how we collect, share and use customers' personal information, and how you can exercise your privacy rights. If you have any questions or concerns about our use of your personal information, then please contact us using the contact details provided at the bottom of this Privacy Notice.

In some situations, we provide additional privacy information at the point your information is collected, for example where you use digital onboarding services, biometric identity verification services or our online services. These supplementary notices should be read alongside this Privacy Notice.

Contents

- What NBKI does
- Personal information we collect and where we collect it from
- How we use your personal information, including lawful bases
- Who we share your personal information with
- International transfers
- Data retention
- Automated decision-making and technology-assisted processing
- Your rights and complaints

What does NBKI do?

NBKI is a bank incorporated in the UK which mainly services clients of its Kuwaiti parent company when those clients want banking services in the UK. Corporate clients will generally have some nexus with the MENA region. NBKI is headquartered in the United Kingdom, but its parent, National Bank of Kuwait S.A.K.P., has branches, subsidiaries and representative offices in a number of countries, including most of the Gulf Cooperation Council (GCC) countries. A list of our group companies can be found at <https://www.nbk.com/nbk-group/about-nbk-group/our-network.html>. Our banking services include current and deposit accounts, FX services, property finance, trade finance and letters of credit and guarantees for corporate customers. Our Treasury department is also active in institutional banking, including accepting and making institutional deposits.

For more information about NBKI, please see our Website at <https://www.nbk.com/london>.

Our services are intended for adults and we do not knowingly collect personal information directly from children except where necessary in connection with products or services provided to a customer.

What personal information does NBKI collect and why?

NBKI is the 'data controller' of your personal information it collects and processes as set out in this Privacy Notice. This means we are responsible for how we hold and use your personal information about you. We are required to notify you of the information in this Privacy Notice and why we process your data.

Where we collect personal information from

We collect personal information from a number of sources depending on the products and services you use.

These sources include:

- information provided directly by you;
- information generated through your use of our products, services and mobile banking application;
- your employer or authorised representatives;
- NBK Group companies;
- identity verification, customer due diligence and fraud prevention providers;
- credit reference, sanctions screening and adverse media providers;
- public sources and public registers; and
- regulators, government bodies and law enforcement agencies.

Further details of the specific sources used for each processing activity are set out in the table below.

Categories of personal information we process

Depending on the products and services you use, we may process:

- identity and verification information;
- contact information;
- account and relationship information;
- transaction and financial information;
- customer due diligence, sanctions screening and financial crime information;
- device, technical and online information;
- communications, enquiries and correspondence;
- complaint, dispute and investigation information;
- biometric verification information (where applicable);

- information obtained from public sources and third-party providers.

The categories of information used for a particular purpose are explained in the table below.

Processing activities

The table below explains the main ways in which NBKI uses personal information, including the categories of personal information involved, where the information comes from, the purpose of the processing and the lawful basis relied upon.

Processing activity	Personal information processed	Source of information	Purpose	Lawful Basis
Account opening and customer onboarding	Name, date of birth, contact details, nationality, marital status, financial information, bank statements, identification documentation, account application information, age, employment information and salary information	Customer, employer, NBK Group companies, verification providers	Assess applications, open accounts, establish customer relationships and provide banking services	Contract, legal obligation
Identity verification and customer due diligence	Passport and identity document information, proof of address, verification results, source of wealth information, source of funds information, customer due diligence information	Customer, identity verification providers, public sources	Verify identity, satisfy KYC requirements and comply with regulatory obligations	Legal obligation
Remote onboarding and expatriate banking services	Identity documents, contact details, onboarding information, verification results, fraud indicators, biometric verification outcomes, audit records, source of funds information, source of wealth information	Customer, ComplyCube and other onboarding providers	Facilitate remote account opening, prevent fraud and support customer onboarding processes. More information is available via the onboarding process.	Legal obligation, legitimate interests
Management of banking products and services	Account information, transaction information, customer instructions, correspondence, contact information	Customer, authorised representatives	Operate and administer banking products and services, process transactions and	Contract

			manage customer relationships	
Mobile banking services	Device information, device identifiers, IP address, security information, app usage information, notification preferences, notification delivery information, messaging identifiers (where applicable), and location information where relevant.	Customer device, mobile banking application	Provide mobile banking functionality, administer customer notification preferences, deliver service-related notifications and alerts, secure customer accounts, detect fraud and unauthorised access, and support the operation and improvement of digital banking services.	Contract, legitimate interests
Customer communications	Contact information, correspondence records, enquiries, complaints, feedback, call recordings, communication preferences and records of communications exchanged through approved channels (including WhatsApp where used).	Customer	Respond to enquiries, manage customer relationships, provide service updates and administer accounts, including where customers choose to communicate with NBKI through approved communication channels such as telephone, email, online banking messaging services and WhatsApp (where available).	Contract, legitimate interests
Call recording and quality assurance	Call recordings, communication metadata	Customer	Comply with regulatory requirements,	Legal obligation, legitimate interests

	and associated customer information		monitor communications, investigate issues, staff training and quality assurance	
Anti-money laundering, sanctions and financial crime compliance	Identity information, transaction information, source of wealth, source of funds, adverse media information, sanctions screening results, politically exposed person information and risk indicators	Customer, public sources, screening providers, NBK Group companies	Prevent financial crime and comply with anti-money laundering, sanctions and counter-terrorist financing laws	Legal obligation
Ongoing customer due diligence and periodic reviews	Account information, transaction information, due diligence records, adverse media information and customer risk information	Customer, screening providers, public sources	Conduct ongoing monitoring and periodic customer reviews	Legal obligation
Technology-assisted customer monitoring (including WorkFusion)	customer information, transaction data, adverse media information, risk indicators and technology-assisted review outputs (including outputs generated by systems such as WorkFusion)	Customer, public sources, screening providers.	Support customer due diligence, adverse media screening and compliance review activities	Legal obligation, legitimate interests
Fraud prevention and security monitoring	Device information, authentication data, account activity, transaction information and security alerts	Customer, systems and service providers	Detect, investigate and prevent fraud, cyber threats and unauthorised access	Legitimate interests, legal obligation
Credit, risk and account management	Customer information, financial information, transaction information and account performance information	Customer, credit reference agencies, public sources	Evaluate risk, manage accounts and protect NBK's business interests	Legitimate interests, contract
Regulatory reporting and legal compliance	Customer information, transaction information, due diligence records and account information	Customer, regulators, NBK Group companies	Comply with legal, regulatory, tax, audit and reporting obligations	Legal obligation
Internal administration and business operations	Customer information, relationship information and operational records	Customer, NBK Group companies	Internal reporting, governance, audit, operational effectiveness and business administration	Legitimate interests

Complaints handling and dispute resolution	Correspondence, complaint information, account information, call recordings and investigation records	Customer, regulators and other third parties	Investigate complaints, resolve disputes and manage legal claims	Legal obligation, legitimate interests
Defence or establishment of legal claims	Customer information, transaction records, communications and evidence files	Customer and third parties	Exercise or defend legal rights and manage litigation	Legitimate interests, legal obligation
Information sharing within the NBK Group	Identity information, contact information, account information, transaction information and compliance records	Customer and NBK Group companies	Provide services, manage group systems, comply with regulatory requirements and support operational activities	Legitimate interests, legal obligation, contract
Website, cookies and online services	Technical information, website usage information, cookies, device information, IP address and online identifiers	Customer device, website and online services	To operate, secure, maintain and improve online services, analyse usage and manage website functionality. [Please see our cookie notice for more information: NBK Privacy Notices].	Legitimate interests, consent where required
Administration of deceased customers' accounts and probate matters	Death certificates, probate documents, details of executors, next of kin information, account information, transaction records and correspondence	Executors, personal representatives, family members, public registers and third parties acting on behalf of the deceased customer	To administer deceased customers' accounts, verify authority to act, comply with legal requirements and close or transfer accounts	Legal obligation, legitimate interests
Administration of mandates, powers of attorney, nominees and authorised representatives	Names, contact details, identification information, authority documentation, relationship information and correspondence	Customer, authorised representatives, attorneys, nominees, family members and other third parties acting on the customer's behalf	To administer accounts, verify authority to act on behalf of customers and provide requested products and services	Contract, legal obligation, legitimate interests

Joint account administration	Account information, transaction information, contact information, customer records, communications and account history	Joint account holders and NBKI records	To administer joint accounts, maintain accurate account records, retain appropriate records relating to current and former joint account holders, manage customer relationships and comply with legal and regulatory obligations.	Contract, legal obligation, legitimate interests
Payment and transaction services	Name, card details, transaction information, merchant information, authentication information and fraud indicators	Customer, card schemes, merchants and payment providers	To issue and administer payment cards, process card transactions, prevent fraud and comply with card scheme requirements	Contract, legal obligation, legitimate interests
Marketing and relationship management communications	Contact information, customer relationship information and communication preferences	Customer, NBKI records	To send information about NBKI products, services, events, business developments and relationship-management activities, to maintain customer relationships and to communicate with prospective and existing customers where permitted by applicable law.	Legitimate interests, consent where required

Please note: Where you use the NBK UK Mobile Banking App, NBKI may process information relating to your notification preferences and the delivery of notifications. Depending on your selected preferences, notifications may be delivered through email, SMS, in-app messaging or other communication channels made available by NBKI. You can manage your notification preferences through the mobile banking application or other preference management tools made available to you.

Use of messaging services

Where made available by NBKI, customers may choose to communicate with us through messaging services such as WhatsApp for certain types of enquiries and account-related communications. Messages exchanged through these channels may contain personal information provided by you and may be retained, monitored, reviewed and archived by NBKI and its service providers for customer service, security, fraud prevention, regulatory compliance, record-keeping and audit purposes. Please do not use messaging services to send information where we have asked you to use another communication channel instead. The scope of activities that may be conducted through messaging services may be limited and may be subject to separate terms, conditions or channel-specific guidance provided by NBKI.

What legal grounds do we rely on to process your personal information?

The table below explains the purposes for which we use your personal information and the legal grounds we rely on for each processing activity. Depending on the circumstances, we may rely on one or more of the following legal grounds under UK data protection law.

- **Providing services under a contract:** We may process your personal information where this is necessary to enter into, perform or administer a contract with you, or to take steps at your request before entering into a contract with us. For example, we rely on this legal ground when assessing applications for products and services, opening and managing accounts, processing transactions and customer instructions, communicating with you about your accounts and providing digital banking and related services.
- **Meeting a legal obligation:** We may process your personal information where this is necessary to comply with a legal or regulatory obligation that applies to NBKI. For example, we may process your personal information to verify your identity, conduct customer due diligence and "know your customer" checks, comply with anti-money laundering and sanctions requirements, fulfil regulatory reporting obligations and respond to requests from regulators, courts or law enforcement authorities.
- **Legitimate interests:** We may process your personal information where this is necessary for our legitimate interests or the legitimate interests of a third party, provided those interests are not overridden by your rights and freedoms. Before relying on legitimate interests, we consider the impact of the processing on individuals and ensure that the processing is proportionate and appropriately safeguarded. Examples of our legitimate interests include:
 - operating, managing and improving our products and services;
 - ensuring the security of our systems, networks and customer accounts;
 - preventing and detecting fraud and other unlawful activity;
 - managing customer relationships and communications;
 - conducting internal administration, governance and audit activities; and
 - establishing, exercising or defending legal rights.

You have the right to object to processing based on legitimate interests in certain circumstances. Further details of your rights are set out below.

- **Consent:** In limited circumstances, we may process your personal information where you have provided your consent for us to do so. For example, consent may be used where required for certain optional communications, notification preferences, cookies or similar technologies. Where we rely on consent, we will
 - explain this to you at the point consent is obtained;

- providing consent is generally voluntary; and
- you may withdraw your consent at any time.

The withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn.

In some cases, we need personal information in order to provide products and services, comply with legal obligations or enter into and perform our contract with you. If you fail to provide personal information when requested, we may not be able to provide some or all of our services, establish or maintain a banking relationship with you, open or operate your account, or comply with our legal and regulatory obligations, including customer due diligence requirements.

In limited circumstances, NBKI may process special category personal data where this is necessary for the provision of our services, to comply with legal or regulatory obligations, to prevent fraud or financial crime, or where you have provided such information to us. For example, this may include biometric information used as part of remote identity verification processes where customers choose to use digital onboarding services. Where we process special category personal data, we will do so in accordance with applicable data protection laws and, where appropriate, provide additional information at the point of collection.

Who does NBKI share my personal information with?

We may disclose your personal information to the following categories of recipients:

- to our **group companies**. A list of our current group companies is available here <https://www.nbk.com/nbk-group/about-nbk-group/our-network.html>.

We benefit from a centralised IT system, provided by our parent company, based in Kuwait. It allows us to access larger, more sophisticated systems to process your personal information. In order to protect your personal information in accordance with the UK's Data Protection laws we have put in place an agreement with our parent company through a set of standard contractual clauses. In respect of corporate customers, Group will have access to the personal details of individuals associated with the corporate, to enable relationship officers in Kuwait to access a consolidated view of the customer. It is not used by group companies for marketing purposes. Access is restricted and can only be viewed if the corporate customer has an account with Group.

Depending on the products and services provided, information accessible within the NBK Group may include identity information, contact details, account information, customer relationship information, transaction information and compliance-related information. Group access is restricted to authorised personnel with a legitimate business need and is not used for independent marketing purposes unless separately explained to you.

- to **third-party services providers and partners** that support the operation of our business, the provision of our products and services, customer onboarding and identity verification, financial crime prevention, payment processing, communications, notification services, information technology and operational activities. This may include providers that facilitate, secure, monitor, archive or retain communications

exchanged through approved communication channels, including messaging services where made available by NBKI.

- to **professional advisers**, including legal advisers, auditors and consultants.
- to **payment networks, card schemes and financial institutions** involved in processing transactions and providing banking services.
- to any **competent law enforcement body, regulatory, government agency, court or other third-party** where we believe disclosure is necessary (i) as a matter of applicable law or regulation including anti-bribery and corruption regulations and anti-money laundering laws, (ii) to exercise, establish or defend our legal rights, (iii) for fraud prevention purposes (iv) to protect your vital interests or those of any other person.
- to a **potential buyer** (and its agents and advisers) in connection with any proposed purchase, merger or acquisition of any part of our business, provided that we inform the buyer it must use your personal information only for the purposes disclosed in this Privacy Notice.
- to any **other person with your consent** to the disclosure.

A current list of our principal service provider categories is available on request.

How does NBKI keep my personal information secure?

We use appropriate technical and organisational measures to protect the personal information that we collect and process about you. The measures we use are designed to provide a level of security appropriate to the risk of processing your personal information. Specific measures we use include:

- physical access control systems
- a physical security presence
- logical access controls (such as passwords)
- perimeter security systems (such as firewalls)
- vulnerability management

International data transfers

Your personal information may be transferred to, and processed in, countries other than the country in which you are resident. These countries may have Data Protection laws that are different to the laws of your country (and, in some cases, may not be as protective).

Specifically, our servers are located in the UK, and our group companies and third-party service providers and partners operate around the world. This means that when we collect your personal information we may process it in any of these countries.

The main international transfers carried out by NBKI may include transfers to NBK Group entities, technology and operational service providers, identity verification providers, sanctions and adverse media screening providers, payment service providers and other third parties that support our banking, compliance and operational activities.

The categories of information transferred will depend on the service involved but may include identity and contact information, account information, transaction information, customer due diligence information, fraud prevention information, technical information and compliance-related records.

Where a transfer is not covered by UK adequacy regulations, NBKI uses appropriate safeguards, such as the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses or other permitted safeguards under Article 46 of the UK GDPR, as applicable to the transfer.

However, we have taken appropriate safeguards to require that your personal information will remain protected in accordance with this Privacy Notice. These include implementing the Standard Contractual Clauses for transfers of personal information between our group companies, which require all group companies to protect personal information they process in accordance with UK Data Protection law. These clauses are regularly reviewed to ensure they meet current legal requirements.

We have implemented similar appropriate safeguards with our third-party service providers and partners. Where our messaging service provider processes data outside the UK, we ensure that appropriate safeguards (such as Standard Contractual Clauses) are in place.

Data retention

We retain personal information we collect from you where we have an ongoing legitimate business need to do so (for example, to provide you with a service you have requested or to comply with applicable legal, tax or accounting requirements). This includes our specific obligations under the FCA rules.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymise it or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

We will keep transaction records for a minimum of seven years from the date of the relevant transaction, other information may be held for at least five years after the termination of our services.

Retention periods vary depending on the type of information and the reason it is held. For example, customer onboarding and due diligence records, anti-money laundering and sanctions records, transaction records, customer communications, call recordings and complaint records may be retained for different periods where required for regulatory, legal, audit, financial crime prevention, complaint handling or dispute resolution purposes.

Communications with NBKI, including telephone conversations, emails and approved messaging-channel communications, may be retained for regulatory, legal, audit, security, complaint-handling and record-keeping purposes.

Some records may need to be retained after an account has closed or after a particular service has ended, where this is required by law or regulation or where retention is necessary to establish, exercise or defend legal rights.

Automated decision-making

Automated decisions are decisions concerning you which are made automatically on the basis of a computer determination, without human review. We do not make decisions about customers solely by automated means

where those decisions produce legal effects or similarly significant effects. We may use technology tools and automated systems to support identity verification, fraud prevention, anti-money laundering checks, sanctions screening, customer due diligence and ongoing monitoring activities. These systems may generate alerts, verification results, confidence scores or risk indicators. However, decisions relating to account opening, customer risk assessments and account management continue to involve appropriate human review.

Your data protection rights

You have the following Data Protection rights:

- If you wish to **access, correct, update or request deletion** of your personal information, you can do so at any time by contacting us using the contact details provided under the "How to contact us" heading below.
- You may also have **the right to object** to certain processing, ask us to **restrict processing** of your personal information or **request portability** of personal information in certain circumstances. Where we rely on legitimate interests, you may ask us for more information about the balancing test we have carried out.
- You have the right to **opt-out of marketing communications** we send you at any time. Where permitted by law, NBKI may send you information about products, services, events and business developments that may be relevant to you. You can exercise your opt-out right by using any unsubscribe mechanism provided in the communication or by contacting us using the details set out under the "How to contact us" heading below. [Please note that account servicing communications, security alerts, fraud prevention messages, account statements, product administration communications, regulatory notices and other operational communications relating to your banking relationship are not marketing communications and may still be sent to you even if you have opted out of marketing].
- Similarly, if we have collected and process your personal information with your consent, then you can **withdraw your consent** at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.
- You also have the **right to raise a complaint with us** directly about how we handle your personal data. Please see the "Complaints Handling Process" section below for details.
- You have the **right to complain to a data protection authority** about our collection and use of your personal information. For more information, please contact your local Data Protection authority. The Data Protection authority in the UK is the Information Commissioner's Office (ICO).

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable Data Protection laws. If you wish to exercise any of the above rights, please contact the Data Protection Officer at the details listed below.

Complaints Handling Process

In accordance with Section 164A of the UK Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, NBKI is committed to maintaining a formal complaints process for all data-related concerns.

If you have a complaint about how your personal data is handled, you may submit it to our Data Protection Officer (DPO) using the contact details provided in the “How to contact us” section of this Privacy Notice. We will acknowledge your complaint within **30 days** of receipt and aim to investigate and respond without undue delay, typically within **three months**.

If you are not satisfied with our response, you may escalate your complaint to the **Information Commissioner’s Office (ICO)**, the UK supervisory authority for data protection matters. Contact details for the ICO are also provided in this Privacy Notice.

Updates to this Privacy Notice

We may update this Privacy Notice from time to time in response to changing legal, technical or business developments. When we update our Privacy Notice, we will take appropriate measures to inform you, consistent with the significance of the changes we make. This may be by posting a notice on the Website or notifying you. We encourage you to review this Notice to be informed of how NBKI is processing your personal information.

You can see when this Privacy Notice was last updated by checking the date displayed at the top of this Privacy Notice.

How to contact us

If you have any questions or concerns about our use of your personal information, please contact our Data Protection Officer (“DPO”) using the following details: DataProtection@nbki.com. OR

National Bank of Kuwait (International) PLC

13 George Street

London W1U 3QJ

Link to Website: <https://www.nbk.com/london/privacy-notice.html>

If you have concerns about our use of your personal information, please contact the DPO, but in the event you are not satisfied please contact the ICO, the UK Supervisory authority for Data Protection issues. Their address is:

ICO

Wycliffe House

Water Lane

Wilmslow, SK9 5AF

Website: <https://ico.org.uk/>