

Arab National Bank London Branch

Our Privacy Notice for Customers and Third Parties

The London branch of the Arab National Bank (referred to in this notice as the “ANBL”, “we” and “us”) is a limited company which forms a branch of Arab National Bank, registered at PO Box 56921, Riyadh 11564, in the Kingdom of Saudi Arabia under commercial registration number 1010027912.

ANBL is committed to protecting the privacy and security of your personal data. References to your “personal data” include any or all of your personal data, as the context requires, including “special categories of personal data”, which involves more sensitive information about you. This is most likely to include information about your racial or ethnic origin or health data. There are other categories of “special categories of personal data” which are less likely to be processed, but for a full definition, see Article 9 of the General Data Protection Regulation (“GDPR”).

This privacy notice describes how we are or will be processing personal data about you during your involvement with the branch, either as a client or otherwise. Please note that we have separate privacy notices for employees, workers, contractors and job applicants. By “processing”, we mean such actions as collecting, using, storing, disclosing, erasing or destroying your personal data.

We may update this notice at any time and without notifying you before we do so.

1. Identity and contact details of the data protection manager

ANBL is a “data controller”. This means that we are responsible for deciding how we hold and use personal data about you. ANBL is not obliged to appoint a statutory data protection officer, but your point of contact about any data protection issues is the Data Protection Team (“DPT”).

Email: DPT@anblondon.com

Tel: +44 (0) 207 297 4600

The DPT is responsible for overseeing compliance with this privacy notice and for handling any data protection queries or issues involving ANBL.

2. What information we collect

We collect and process the following personal information in relation to our customers:

- Name;
- Address;
- Email address;
- Telephone number(s);
- Date of Birth;
- Passport copies;
- National ID (if applicable);
- Employment status;
- Career history;
- Source of funds for a specific transaction;
- Source of wealth more generally;
- Details of jurisdictions where you may be liable for tax (FATCA and CRS reporting).

We collect the following information in relation to designated signatories for customer’s accounts:

- Name;

- Address;
- Contact Number;
- Copies of ID.

We collect names and contact details of individual suppliers and other third parties.

3. How do we collect your personal data?

We collect the data in relation to customers from our customers when they open an account and throughout our relationship with them including a mandate form.

We collect data in relation to designated signatories from the designated signatories themselves, and from customers who designate them.

We collect data about third party contacts from the contacts themselves.

4. Why do we collect your information

We collect data from our customers in order to facilitate the provision of our services to customers, and to ensure that we satisfy our regulatory and “know your client” anti-money laundering obligations. We collect data from designated signatories to provide an additional service to customers. We collect data about third parties in order to maintain communication with them.

5. What are the legal bases and the purposes for which we process your personal data?

We will only use your personal data as permitted by law. We may use your personal data in any of the following circumstances:

- Where we have your consent;
- Where we need to perform the contract;
- Where we need to comply with a legal obligation;
- Where processing is necessary to protect vital interests;
- Where processing is necessary in the public interest;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. We are required to specify what the legitimate interests are (see below for further details).

Please note that there is a separate section below that covers additional legal bases for processing more sensitive information about you.

Necessary for compliance with a legal obligation

We keep account and career information about our customers to comply with anti-money laundering legislation.

Necessary for the performance of a contract

We keep customer details in order to ensure that we can provide the account services that we have agreed with customers to provide as part of our terms of service.

Necessary for our legitimate interests and those of a third party

It is in our legitimate interests to use your personal information in such a way to ensure that we can continue providing the best account services to our customers. It is in our legitimate interests to be able to maintain contact details of suppliers and third party connections that provide insights and information about the market.

“Special categories” of personal data

“Special categories” of personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data. We may process special categories of personal data in limited circumstances, and we process copies of passports/ID where we are legally obliged to do so

6. Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so, before we start using it for that unrelated purpose. Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is permitted by law.

7. Sharing Data

We may share your data with third parties, including third-party service providers and any sub-contractors of those service providers where required by law, or where we have a legitimate interest in doing so. We require third parties to respect the security of your data and to ensure that adequate safeguards are in place to protect it, in line with applicable laws. As we are a branch of Arab National Bank, we share your name, account identifying details and account information as recorded in our customer files and systems with our Head Office in Riyadh, Kingdom of Saudi Arabia.

How secure is your information with third party service providers?

All our third party service providers are required to take appropriate security measures to protect your personal data in line with our policies. We do not allow our third party service providers to use your personal data for their own purposes unless they are data controllers in their own right in relation to your personal data. Where they operate as our “data processors” (i.e. they process your personal data on our behalf and acting only on our instructions), we only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about disclosure to other third parties?

We may share your personal data with other third parties, for example to external legal or other professional advisers, or to otherwise comply with the law.

What safeguards are in place in relation to the transfer of your personal data outside of the EU?

Aside from the transfer of data to the Head Office in Riyadh detailed above, we may also share personal data with other third parties in order to provide our services to you.

By transferring data to our Head Office in Riyadh, we are transferring your data outside the EU. We are therefore obliged to ensure that there are adequate safeguards in place in respect of your data, and we confirm that we have done so by entering into the model terms provided by the EU for such transfers. Where we transfer data to any other third party supplier outside the EU, we will ensure that adequate safeguards are in place for any such transfer.

Automatic Exchange of Information (FATCA and CRS)

We are required by law to collect and report certain information about customers and, where applicable, controlling persons for the purposes of compliance with the Foreign Account Tax Compliance Act (“FATCA”), the Common Reporting Standard (“CRS”) and related Automatic Exchange of Information (“AEOI”) regulations.

Where required, we will share relevant personal data (including identifying information, tax residency information, tax identification numbers and account details) with HM Revenue & Customs (“HMRC”). HMRC may then exchange this information with overseas tax authorities in accordance with applicable international agreements.

8. How long will we retain your personal data?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal data are available in our Retention Policy which is available from the DPT. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicabl

9. What are your rights and obligations as a data subject?

Your duty to inform us of changes

It is important that the personal data we hold about you is accurate and current. Please let us know of any changes. We will update your records promptly upon being notified of such changes.

Your rights in connection with personal data

Under certain circumstances, by law you have the right to:

- Request access to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it;
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground;
- Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it;
- Request the transfer of your personal data to another party.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact the DPT in writing.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances, as permitted by the GDPR.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

What are your rights to withdraw consent to processing?

Where you may have provided your consent to the processing of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, use our

unsubscribe buttons, or contact the DPT. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

10. Security

We have put in place measures to protect the security of your information. Details of these measures are available upon request but in brief, we secure the storage of your data on our servers, and restrict access to only those employees, agents, contractors and other third parties who have a business need to know. We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. We have implemented appropriate technical and organisational measures to protect your personal data.

11. Changes to this privacy notice

We reserve the right, from time to time, and at our sole discretion, to change or update this Privacy Policy. All changes to this Privacy Policy will be published on this page and on the applicable Site(s). Upon publication, each change will become effective and you will be deemed to be aware of and bound by it. You should therefore review this Privacy Policy regularly to ensure that you are up-to-date with the current terms of the Privacy Policy. If you have any questions about this privacy notice, please contact the DPT.

12. What are your rights to lodge a complaint about the way in which your personal data are being processed?

Firstly, we would urge you to contact the DPT in writing so that we can try to resolve your complaint to your satisfaction. If you are not satisfied with the DPT's response, you may contact the Information Commissioner's Office ("ICO") on 0303 123 1113.

You are free to contact the ICO at any time. However, the DPT may be able to answer your concerns or questions more quickly.