

JN BANK UK LTD PRIVACY POLICY

We take your privacy very seriously. The effective management of all Personal Information, including its security and confidentiality, lies at the very heart of our business and underpins our practices and processes. Please read this Privacy Policy carefully as it contains important information on who we are and how and why we collect, store, use and share your Personal Information. It also explains your rights in relation to your Personal Information and how to contact us or supervisory authorities in the event you have a complaint.

We collect, use and are responsible for certain Personal Information about you. When we do so we are subject to data protection laws applicable in the United Kingdom and we are responsible as 'controller' of that Personal Information for the purposes of those laws.

1. KEY TERMS

Let's start by explaining some key terms used in this policy:

We, us, our	JN Bank UK Ltd, a company registered in England and Wales (under number 11734380) whose registered office is at 410 Brixton Road, London, United Kingdom, SW9 7AW United Kingdom and our group of companies
Our data protection officer	Dianne Augustin Email address: dataprotection@jnbank.co.uk
Personal Information	Any information relating to an identified or identifiable individual
Sensitive Personal Information	Personal Information revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership Genetic and biometric data Data concerning health, sex life or sexual orientation

2. PERSONAL INFORMATION WE COLLECT ABOUT YOU

We may collect and use the following Personal Information about you:

- your name, address, date of birth, and contact information, including email address, telephone number and information in respect of your social media accounts;
- details about your transactions with us including accounts you use;

- your contact with us, such as a note or recording of a call you make to one of our contact centres, an email or letter sent, contact in our branch, or other records of any contact with us;
- your account information, such as dates of payments owed or received, account numbers or other information related to your account;
- your employment details, financial position and information taken from identification documents like your passport or driving licence when we review your application for any of our products and/or services;
- information about your online activity; and
- your Sensitive Personal Information, but only in respect of: (i) your biometric data in relation to authenticating your identity when using our products and/or services; and (ii) your health data where you voluntarily disclose this to us in relation to the products and/or services that you are receiving.

This Personal Information is required to inform you about suitable products and/or services that we can or currently provide to you. Where you fail to provide that Personal Information when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with products and/or services). In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

3. HOW YOUR PERSONAL INFORMATION IS COLLECTED

We collect most of this Personal Information directly from you, by telephone, letter or email and/or via our website. However, we may also collect information:

- when you register and/or attend any of our events, webinars, or the conferences we host;
- from publicly accessible sources, e.g. Companies House or social media websites;
- directly from a third party, e.g.:
 - sanctions screening providers;
 - credit reference agencies;
 - customer due diligence providers;
- from a third party with your consent, e.g. another bank or building society;
- from cookies on our website – for more information on our use of cookies, please see our [Cookies Policy](#); and
- via our IT systems, e.g.:

- automated monitoring of our websites and other technical systems, such as our computer networks and connections;
- CCTV and access control systems, including in our branch;
- communications systems, such as call recordings; and
- email and instant messaging systems.

4. HOW AND WHY WE USE YOUR PERSONAL INFORMATION

Under data protection law, we can only use your Personal Information if we have a proper reason for doing so. In order to use your personal information, we rely on the following legal bases:

- processing is necessary for the performance of the products and/or services we provide to you (for example, opening an account, maintaining your account details and services connected with such account);
- processing is necessary for the purposes of the legitimate business interests pursued by us (including, for example, improving or offering suitable products and/or services);
- processing is necessary for compliance with a legal obligation to which we are subject (including undertaking screening for financial and other sanctions and conduct checks to identify you and verify your identity); and
- if we process your Sensitive Personal Information, we will only do so on the basis that we have obtained your explicit consent to carry out such processing.

Generally, we do not rely on consent as a legal basis for processing your Personal Information other than in relation to sending marketing communications to you (for example, via online banners, emails or text messages) and as set out in Section 4(iv) above. You have the right to withdraw consent to marketing at any time by contacting us (see **'How to contact us'** below).

We collect and process your Personal Information in order to:

- provide products and/or services to you;
- verify your identity and check credit with credit reference agencies;
- process and complete transactions, and send related information, including transaction confirmations and invoices;
- manage our customers' use of the products and/or services, respond to enquiries and comments and provide customer service and support;
- send customers technical alerts, updates, security notifications, and administrative communications;
- update customer records;
- prevent unauthorised access and modification to our systems;

- investigate and prevent fraudulent activities, unauthorised access to the products and/or services, and other illegal activities;
- undertake statistical analysis to help us manage our business, e.g. in relation to financial performance, customer base and work type; and
- for any other purposes about which we notify customers and users.

We may contact you via email to invite you to review any service and/or products you received from us in order to collect your feedback and improve our services and products (the “Feedback Purpose”).

We use an external company, Trustpilot A/S (“Trustpilot”), to collect your feedback which means that we will share your name, email address and reference number with Trustpilot for the Feedback Purpose.

We may also use such reviews in other promotional material & media for our advertising and promotional purposes.

If you want to read more about how Trustpilot process your data, you can find their Privacy Policy [here](#).

5. **WHO WE SHARE YOUR PERSONAL INFORMATION WITH**

We may share Personal Information, in the following limited circumstances, with:

- companies within the JN Bank UK Ltd company group;
- third parties we use to help deliver our products and/or services to you;
- other third parties we use to help us run our business, e.g. marketing agencies or website hosts;
- other banks and third parties where required by law to help recover funds that have entered your account as a result of a misdirected payment by such a third party;
- other banks to help trace funds where you are a victim of suspected financial crime and you have agreed for us to do so, or where we suspect funds have entered your account because of a financial crime;
- third parties approved by you;
- credit reference agencies;
- our insurers, brokers and other professional advisers;
- fraud prevention agencies if false or inaccurate information is provided and/or fraud is identified or suspected. Law enforcement agencies and other organisations may access and use this information; and

- in the event that any additional authorised users are added to your account, we may share information about the use of the account by any authorised user with all other authorised users.

We only allow our service providers to handle your Personal Information if we are satisfied they take appropriate measures to protect your Personal Information.

The Personal Information we have collected from you will be shared with fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance, or employment. Further details of how your information will be used by us and these fraud prevention agencies, and your data protection rights, can be found at <https://www.cifas.org.uk/fpn>.

We may disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations.

We may also need to share some Personal Information with other parties, such as potential buyers of some or all of our business or during a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations.

6. CREDIT REFERENCE AGENCIES

In order to process your application, we will perform credit and identity checks on you with one or more credit reference agencies (“**CRAs**”).

To do this, we will supply your Personal Information to CRAs and they will give us information about you. This will include information from your credit application and about your financial situation and financial history. CRAs will supply to us both public (including the electoral register) and shared credit, financial situation and financial history information and fraud prevention information.

We will use this information to:

- assess your creditworthiness and whether you can afford to take the product;
- verify the accuracy of the data you have provided to us;
- prevent criminal activity, fraud and money laundering;
- manage your account(s);
- trace and recover debts; and
- ensure any offers provided to you are appropriate to your circumstances.

We will continue to exchange information about you with CRAs while you have a relationship with us. We will also inform the CRAs about your settled accounts. If you borrow and do not repay in full and on time, CRAs will record the outstanding debt. This information may be supplied to other organisations by CRAs.

When CRAs receive a search from us they will place a footprint on your credit file. If this is an application search then it will be seen by other lenders; otherwise, it won't.

If you are making a joint application, or tell us that you have a spouse or financial associate, we will link your records together, so you should make sure you discuss this with them, and share with them this information, before lodging the application. CRAs will also link your records together and these links will remain on your and their files until such time as you or your partner successfully files for a disassociation with the CRAs to break that link.

The identities of the CRAs, their role also as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and your data protection rights with the CRAs are explained in more detail at <https://www.transunion.co.uk/crain>.

7. **HOW LONG YOUR PERSONAL INFORMATION WILL BE KEPT**

We will only retain your Personal Information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, accounting, or reporting requirements.

To determine the appropriate retention period for your Personal Information, we consider the amount, nature, and sensitivity of the Personal Information, the potential risk of harm from unauthorised use or disclosure of your Personal Information, the purposes for which we process your Personal Information and whether we can achieve those purposes through other means, and the applicable legal and regulatory requirements.

When it is no longer necessary to retain your Personal Information, we will delete or anonymise it.

8. **TRANSFERRING YOUR PERSONAL INFORMATION OUT OF THE EEA**

We may transfer Personal Information that we collect from you to our third party data processors, vendors or hosting partners acting on our behalf located in countries outside of the European Economic Area ("**EEA**") or to other entities in our group of companies in connection with the purposes set out above. We will only transfer your personal information outside the EEA where either the transfer is to a country which the EU Commission has decided ensures an adequate level of protection for your personal information, or we have put in place adequate safeguards as required by applicable data protection law. The adequate safeguards that we currently utilise are the relevant model clauses approved by the European Commission.

If you would like further information, please contact our Data Protection Officer (see '**How to contact us**' below).

9. **YOUR RIGHTS**

You have the following rights, which you can exercise free of charge:

Access	The right to be provided with a copy of your Personal Information (the right of access).
Rectification	The right to require us to correct any mistakes in your Personal Information.
Erasure	The right to require us to delete your Personal Information – in certain situations.
Restriction of processing	The right to require us to restrict processing of your Personal Information – in certain circumstances, e.g. if you contest the accuracy of the data.
Data portability	The right to receive the Personal Information you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party – in certain situations.
To object	The right to object: – at any time to your Personal Information being processed for marketing (including profiling and analytics); or – in certain other situations to our continued processing of your Personal Information, e.g. processing carried out for the purpose of our legitimate interests.
Not to be subject to automated individual decision-making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you.
Withdraw consent	The right to withdraw your consent to us processing your Personal Information at any time if our processing is based on your consent.

For further information on each of those rights, including the circumstances in which they apply, please contact us or see the [Guidance from the UK Information Commissioner's Office \(ICO\) on individuals' rights under the General Data Protection Regulation](#).

If you would like to exercise any of those rights, please:

- email, call or write to our Data Protection Officer – see below: **'How to contact us'**;

- let us have enough information to identify you (e.g. your full name, address and account number);
- let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and
- let us know what right you want to exercise and the information to which your request relates.

10. KEEPING YOUR PERSONAL INFORMATION SECURE

We have appropriate security measures to prevent Personal Information from being accidentally lost or used or accessed unlawfully. We also have procedures in place to deal with any data breach.

11. HOW TO COMPLAIN

We hope that our Data Protection Officer can resolve any query or concern you may raise about our use of your information.

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner who may be contacted at <https://ico.org.uk/concerns> or by telephone on 0303 123 1113.

12. CHANGES TO THIS PRIVACY POLICY

This privacy notice was published on 16/12/2019 and last updated on 05/02/2021.

We may change this privacy notice from time to time – when we do we will inform you via a notice on our website or via other means of contact such as email.

13. HOW TO CONTACT US

Please contact us and/or our Data Protection Officer by post, email or telephone if you have any questions about this Privacy Policy or the information we hold about you.

Our contact details are shown below:

Our contact details	Our Data Protection Officer's contact details
<p>JN Bank PO Box 76282 London SW9 1ET customerservice@jnbank.co.uk 0808 196 1945</p>	<p>Dianne Augustin 410 Brixton Road Brixton London SW9 7AW dataprotection@jnbank.co.uk</p>

PP05022021v2