Business Banking Data Privacy Notice.

TSB Business Banking

Contents

Your information.

We are TSB Bank,
20 Gresham Street,
London EC2V 7JE

TSB is committed to providing a real alternative in business banking in Britain. We want you to have trust and confidence in us and how we deal with your business information, and the personal information we collect during our relationship.

When providing Business Banking services, we manage personal information. This includes information relating to product parties and business parties. This personal information is protected by the UK's privacy laws. These privacy laws do not apply to information about Partnerships in Scotland, Limited Liability Partnerships or Limited Companies, but do apply to information relating to product parties, business parties or any other individual who we manage. We will, of course, treat your business information as private and confidential and make sure it is kept secure.

We have a dedicated team that looks after data privacy rights. We also have a Data Protection Officer ("DPO") to guide our business and oversee our use of your personal information. Please see below for their contact information and for more information on how we manage your personal information.

The Data Rights Team
TSB Bank
Ariel House
2138 Coventry Road
Sheldon
Birmingham
B26 3JW

You can also email **privacy@tsb.co.uk**

The Data Protection Officer
TSB Bank
Henry Duncan House
120 George Street
Edinburgh
EH2 4LH

When you apply for a product or service, and throughout our relationship, you will provide personal information to us, and we will gather certain personal information from other sources, some of which may be publicly available.

Whose data will we receive?	What type of data will we receive?	Who does the data come from?
Business parties, product parties	Data confirming their identity. Data relating to their credit history and status of that or any associated person. Data relating to any fraudulent activity or suspected fraudulent activity concerning business parties/product parties or any associated person. Data relating to Politically Exposed Persons (PEPs).	You. Credit Reference and Fraud Agencies. Further information is set out below. CIFAS, a not-for-profit fraud prevention membership organisation. For more information on CIFAS go to **www.cifas.org** or write to: Consumer Affairs, CIFAS, 6th Floor, Lynton House, 7–12 Tavistock Square, London WC1H 9LT
Guarantors, deposit providers, and similar	Where a person guarantees to pay TSB any sums that you may owe, or provides a deposit (for example, when you take out a mortgage), we will record sufficient details to allow us to contact them if/when required. Where they provide the deposit from their bank account, we will record the account details.	You.

Whose data will we receive?	What type of data will we receive?	Who does the data come from?
Employees and others associated with you	In some circumstances, you may provide us with employees' details such as name, address and payroll number.	You.
Providers of professional services	Business/trading name, address, contact details, internal reference, membership of professional bodies, levels of insurance (if any), identity of client and other information that is supplied to us for the professional services in question.	You, the person or entity which you are providing professional services, professional bodies and public sources.

We can't open or maintain an account or service if you don't give us certain information. For example, we will not be able to open an account unless you provide details about product parties and business parties.

02
Why we use your personal information

We use personal information so that we can deliver the banking service that business wants in the 21st century. This includes using personal information so that we can:

Provide you and/or business parties and/or product parties with services.

This is necessary to comply with our contractual obligations to you under our Terms and Conditions.

Identify products and services which might be suitable for you and/or business parties and/or product parties.

We need to do this to meet our legitimate business interests in providing our customers with products and services that they like. You are under no obligation to make use of these products or services.

Assess lending and insurance risks.

This is necessary for us to meet our legitimate interests in making sure we have an appropriate risk profile. Ensuring that we do not take excessive risks is in the public benefit, as we make sure your money is kept safe.

Recover debts, prevent, detect and prosecute fraud and other crimes.

This is necessary to meet our legitimate interests in exercising our rights and making sure that you and other customers are not subject to crime or fraudulent activity.

Manage our and any member of our Group's relationship with you and/or business parties and/or product parties.

We may need to do this to make sure we can meet our contractual obligations under our Terms and Conditions. It also lets us access your account details when you contact us.

Update our records about you and/or business parties and/or product parties.

This is necessary to meet our legitimate interests in keeping our records accurate and up to date, and to make sure that we do not use out of date information about you.

Improve our performance.

This includes testing new systems and checking upgrades to existing systems, training, undertaking transactional analysis, conducting audits, assessing lending and insurance risks. It also covers customer modelling, statistical and trend analysis with the aim of developing and improving products and services, and providing information to Regulators. We do this to meet our legitimate interests in giving our customers better services, and making sure commercial and personal information is appropriately protected.

Send direct marketing and promotional material.

We will offer you, product parties and business parties, an opportunity to receive direct marketing and promotional information. We will use your personal information to send marketing information as it's in our legitimate interests to market our products to our business customers. We will only send post, email, phone or SMS marketing if you let us know you want to receive it.

We value our relationship and do our best to send information which we think may be of interest, by post, email, phone or SMS. We respect your choices, and product parties and business parties can ask us to stop sending marketing to them at any time by contacting our Data Rights Team. Simply click 'unsubscribe' in any marketing email we send, or by following the instructions in our marketing SMS — and when this happens, we will stop.

Where product parties and business parties log in and use our online services, we will aim to give them a personal service, so that they easily see relevant information, including details of our products that we think are of interest.

They may also see TSB advertisements that we think may be of interest, when logged in to other secure websites.

Product parties and business parties can object to this, by contacting our Data Rights Team. This will mean that they view more general webpages. They won't see any fewer advertisements, but the pages and advertisements may be of less relevance.

Social Media.

If product parties and/or business parties engage with TSB through social media, we may use their information to interact with them. We only use this information if you actively engage with or publish a post about TSB through social media, on the basis that it is in our legitimate interests to engage and interact with you when you discuss TSB and/or connect with us.

To deliver the best customer experience, we partner with software providers that allow us to connect with them via online communities and blogs. These partners manage personal information only in accordance with our instructions. Personal information will not be stored or transferred outside the European Economic Area ("EEA") and TSB can instruct these partners to delete all personal information, or return it securely to TSB, at the end of our contract with them. For a list of EEA countries, **see page 13**.

Do what you ask us to do.

If you want particular services from us, or want to ask us a question, we will use product parties and/or business parties personal information to answer you. This is to meet our legitimate interests in making sure we can give you the best possible service.

Comply with legal obligations.

This might include providing information to HMRC, preventing money laundering and doing what our Regulators require. We only do this where strictly necessary to comply with these legal obligations.

To deliver better banking for Britain.

This includes using personal information to make sure we manage and develop customer relations; assess the suitability of existing and proposed products for our customers; pass information to Credit Reference Agencies (as described below); conduct internal or external reviews of our performance and quality.

We also instruct our internal or external legal teams; detect and prevent fraud and liaise with police and other anti-fraud agencies; engage with and interact on social media; and make sure we manage TSB as effectively and efficiently as possible.

We use personal information in this way as it is in our business interests to do so, and it allows us to defend our rights, provide a better service to our customers and understand what our customers want from us. Whenever we use personal information, we will always make sure we work to protect personal data interests and rights. We will not use personal information for any purpose which is contrary to those set out above. We will keep data appropriately secure, and tell customers when we use it for a new purpose.

03 Passing personal information to others

We treat personal information as private and confidential, but may disclose it outside TSB in some circumstances, to fulfil the purposes set out above (including sharing with partners with whom we provide services as described above). This may include sharing it with subcontractors, who will act only on our instructions or our behalf, and will use your information only for the purposes set out above.

We will disclose information to others:

To meet our contractual obligations to you in accordance with the Terms and Conditions, including where:

- Other product parties and/or business parties may be entitled to see your transactions
- It is needed by other parties connected with your account (including guarantors)
- We need to share information with other lenders who also hold a charge on your property

Where we must comply with legal obligations to which we are subject, including where:

- HMRC or other authorities require it
- The law, a regulatory body or the public interest requires it
- It is required as part of our duty to protect your accounts — for example we are required to disclose your information to the UK Financial Services Compensation Scheme (FSCS)
- It's required by us or others to detect, investigate or prevent crime or fraud
- Or where the person consents or asks us to. If they give their consent, they can withdraw it at any time and we'll stop disclosing the information in that way

Credit Reference Agencies.

In order to process your application for a product or service, we will perform credit and identity checks with one or more credit reference agencies ("CRAs"). Where you take banking services from us, we may also make periodic searches at CRAs to manage your account with us.

To do this, we will supply business and personal information relating to you, product parties and/or business parties to CRAs and they will give us information about you and these people. This will include information from your credit application and about your financial situation, and financial history, as well as that of the product parties and business parties. CRAs will supply us with public (including the electoral register) and shared credit, financial situation and financial history information as well as fraud prevention information.

We will use this information to:

- Consider 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
- Make sure any offers are appropriate to your circumstances

We will continue to exchange information 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 search footprint on your credit file and that of the product parties and business parties. These footprints may be seen by other lenders.

If you tell us that you have a spouse or financial associate, we will link your records together. You should make sure you discuss this with them, and share this information, before making 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 spouse, or financial associate successfully files for a disassociation with the CRAs to break that link.

The identities of the CRAs, their role as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and data protection rights with the CRAs are explained in more detail at www.experian.co.uk/crain. CRAIN is also accessible from each of the CRAs that TSB uses — visit any of these links to go to the same CRAIN document:

TransUnion www.transunion.co.uk/crain

Experian www.experian.co.uk/crain

Fraud Prevention Agencies.

The government also requires us to screen applications that are made to us, to make sure we are complying with the international fight against terrorism, money laundering, modern slavery and other criminal activities. So we may need to disclose information to government bodies and to fraud prevention agencies to meet these legal obligations.

We will study patterns of activity, check for unusual transactions and monitor devices used to access TSB's systems. Including Internet Protocol (IP) addresses and may include using widely available geographical mobile phone technology to assess the location.

General

Before we provide services, goods or financing to your business, we undertake checks for the purposes of preventing fraud and money laundering, and to verify the identity of the business, product parties and business parties. These checks require us to process personal data about these people.

The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and money laundering, and to verify your identity.

Details of the personal information that will be processed include, for example: name, address, date of birth, contact details, financial information, employment details, device identifiers including IP address and vehicle details of product parties and business parties.

We and fraud prevention agencies may also enable law enforcement agencies to access and use this personal data to detect, investigate and prevent crime.

We process this personal data on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the services or financing you have requested.

Fraud prevention agencies can hold this personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.

Consequences of processing

If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services or financing that has been requested, or we may stop providing existing services to you or your business.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you or the business. If you have any questions about this, please contact us on the details above.

Data transfers

Whenever fraud prevention agencies transfer personal data outside of the European Economic Area, they impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

If we or any other company in our Group wishes to sell or transfer all or part of its business and assets, or any associated rights or interests, or to acquire a business or enter into a merger, we/it may disclose your personal data and confidential business information to any potential buyer, transferee, merger partner or seller and its advisers and any other persons we/it may reasonably decide, provided that each person to whom information is disclosed promises to keep it confidential. If the sale or transfer is completed, the buyer, transferee or merger partner may continue to use and disclose the information, subject to the same provisions set out here.

04 Transferring personal information outside of the UK

The UK and other EEA countries* provide a high standard of data protection and privacy. We may run your accounts and provide other services from centres outside the UK and EEA, which are not considered by the European Commission to have a similar standard of legal protection for personal information. If so, we will require personal information to be protected to at least UK standards.

To do this, we make sure we only transfer personal information to countries which are regarded under EU law as providing an adequate level of protection for personal information, to companies in the USA which are certified as providing an adequate level of protection, or we will put in place contractual commitments which make sure they provide an adequate level of protection.

If you want to learn more about the specific countries to which we transfer personal data, or if you wish to obtain a copy of the safeguards we have in place for particular countries, please contact the Data Rights Team.

We may process payments through other financial institutions such as banks and the worldwide payments system operated by the SWIFT organisation if, for example, you make a CHAPS payment or a foreign payment. Those external organisations may process and store personal information abroad and may have to disclose it to foreign authorities to help them in their fight against crime and terrorism. If these are based outside the UK and the European Economic Area* ("EEA"), such personal information may not be protected to standards similar to those in the UK, but we will take steps, including through contractual commitments, to make sure that an adequate level of protection is provided.

*Countries that belong to the EEA: Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

05 How long will we keep personal information?

We will only keep personal information for as long as your application for an account or product, or for as long as you have accounts or products with us. We will also keep your personal information for a certain period after your application has ended or you have closed your accounts.

When working out how long this period will last, we take into account our legal obligations, the expectations of financial and data protection regulators, and the amount of time we may strictly need to hold your personal information to carry on our business or defend our rights.

For example, if you have an account with TSB, we will keep your information and details of the account, while the account is open. To meet our legal and regulatory requirements, we must keep a lot of this information for a number of years after the account is closed, even if you do not have another account with us. We will also keep your information in archived form in order to defend our legal rights (which may be for the period in which legal claims can be made under applicable law. In the UK, this is six years for contractual claims).

We have policies and procedures in place to make sure we delete information that is no longer needed for any of these purposes.

06 Personal information rights

People in the UK and across the EEA have certain rights over their personal information. These include the right to get a copy of their personal information or have some elements of it transmitted to themselves or another company in a common electric format. In certain circumstances, they can have their personal information corrected or erased, or have our use of their personal information restricted.

They also have the right to object to our uses of their personal information as described above.

Anyone who wishes to know more about their data rights should read our Data Privacy Notice, which can be found at: **www.tsb.co.uk/privacy**. They can also collect a copy at any TSB branch. We will generally not charge a person for exercising these rights.

We aim to work with you in relation to any request, complaint or question you have about your personal information. However, if you believe we have not adequately resolved a matter, you can complain to the Information Commissioner's Officer (the "ICO").

You have a right, at any time, to complain to the ICO, the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. You can follow this link to their website: **https://ico.org.uk** or ask for details from our Data Rights Team.

If you'd like this in another format such as large print, Braille or audio please ask in branch.

If you have a hearing or speech impairment you can contact us using Text Relay or Textphone on **0345 835 3843** (lines open from 7am to 11pm, 7 days a week).

Not all Telephone Banking services are available 24 hours, 7 days a week. Speak to a Partner for more information. Calls may be monitored or recorded.

If you need to call us from abroad, or prefer not to use our 0345 number, you can also call us on 0203 284 1575.

Information applies from May 2019.

Click **tsb.co.uk**
Visit **Drop into your local branch**

TSB Business Banking

TSB12732 (05/19)