Business Banking data privacy notice.

TSB

Business

What's inside?

1. Our Data Privacy Notice.

Your information will be held by TSB Bank plc ('TSB').

UK Data Protection Laws require us to manage all personal information in accordance with the Data Protection Principles. We're required to process your personal information fairly, lawfully and in a transparent manner. This means that you're entitled to know how we intend to use any information you provide. You can then decide whether you want to give it to us in order that we may provide the product or service that you require. All our employees are responsible for maintaining customer confidentiality. We provide training and education to all employees to remind them about their obligations. In addition, our policies and procedures are regularly audited and reviewed.

The TSB Business Mobile Banking App and Internet Banking

We monitor how you use the TSB App. We also collect information on all the other apps installed on your device, to help us detect malware and potential fraud. This safeguards us all against financial crime.

If we detect suspicious activity or notice that your device is unsafe, we might block your account and your access to the TSB Mobile Banking App and Internet Banking.

2. Your information.

We're TSB Bank, 8 Bishopsgate, London, EC2N 4BQ

We want you to have trust and confidence in the way we deal with your information.

The UK is a world leader in data protection and privacy. 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.

All our employees are responsible for maintaining customer confidentiality. We provide training and education to all employees, and we regularly review our policies and procedures. Our aim is to make sure that you have confidence in TSB and feel comfortable about giving us your information. We think that safely looking after your information and processing it fairly is a key part of our relationship.

We have a dedicated team that looks after data privacy rights. We also have a Data Protection Officer ('DPO') to guide the business and oversee our use of your information.

The Data Rights Team
TSB Bank
Ingenuity House
Elmdon Trading Estate
Bickenhill Lane
Birmingham
B37 7HQ

You can also contact our team by emailing **privacy@tsb.co.uk**

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

You can see a copy of this Customer Data Privacy Notice at **tsb.co.uk/privacy**

3. Why and how we manage your information.

Providing our products and services.

When you apply for a product or service, and throughout our relationship, you'll provide personal information to us.

We'll also collect certain information about you from others, including people who may be acting on your behalf. We'll gather and process the type and amount of personal information that is relevant and required. We use this personal information to do the things you would expect us to do under your terms and conditions or to comply with law.

This includes:

- checking your identity and confirming that it's you
- managing your relationship with us
- providing you with products and services
- checking your credit record and that you can afford products and services
- recording money in and out of your accounts
- telling you about important changes or developments to the features and operation of these products and services
- updating, consolidating and improving the accuracy of our records
- crime detection, prevention and prosecution
- carrying out financial reviews
- responding to your enquiries and complaints
- administering offers, competitions and promotions
- arrears and debt recovery activities
- reporting to regulators
- testing systems and processes, including using your information in secure test environments, even if your application is unsuccessful.

We won't be able to open or maintain a product or service if you fail to provide certain information.

Occasionally we receive names and addresses (including email addresses) of non-customers who it's thought may be interested in our products and services.

In these circumstances, where we have your consent, we'll let you know by email or post of the products or services we believe may be of interest. If we don't already have your consent, we'll tell you about our products and services by post in accordance with our legitimate interests to promote our business. You have the right to opt out of this marketing at any time, by following a link on the email or by contacting our Data Rights Team.

3. Why and how we manage your information.

Who else will we receive your information from?	What type of data will we receive?
Credit Reference and Fraud Agencies. See more information below. **CIFAS, a not-for-profit fraud prevention membership organisation.** **For more information on CIFAS go to cifas.org or write to:** **Consumer Affairs, CIFAS 6th Floor Lynton House 7-12 Tavistock Square London WC1H 9LT**	Data confirming your identity. Data relating to credit history and status of you or any associated person. Data relating to any fraudulent activity or suspected fraudulent activity concerning you or any associated person. Data relating to Politically Exposed Persons (PEPs).
Joint Business Accounts	Where one person opens a joint account (e.g. partnership, Limited Company or Limited Liability Partnership), or adds an additional party to an account, they'll provide us with the name and address of those additional parties, who will also become a TSB customer.
A TSB customer, where you act as a guarantor for them or where you pay their deposit	If you guarantee to pay TSB any sums that a TSB customer may owe or provide a deposit (for example when a TSB customer takes out a mortgage), we'll record enough details to let us contact you if/when needed. Where you provide the deposit from your bank account, we'll record the account details.
Your professional advisers	Name or Business/trading name, address, contact details, internal reference and other information provided to us in the course of delivering the professional services in question.

Providing products with other service providers.

As well as our core banking services, we combine with others to provide additional services. We do this where we believe it's in your interests and ours, or where it's necessary to deliver the service you've asked for. This involves passing some of your personal information to our business partners who help provide these products. We only pass the minimum information needed to these business partners. And we always make sure that your information remains protected as required under UK law, including laws regulating the sending of marketing messages to you.

Where you apply for a product or service that's delivered with a business partner, we'll collect your personal information and use it to process your application and provide these services in the ways described in this notice.

4. Special Category and Criminal Offence Information.

Special category information

We process sensitive information (also known as "special category data").

This includes:

a) racial or ethnic origin.

b) political opinions.

c) religious or philosophical beliefs.

d) trade union membership.

e) genetic information.

f) biometric information.

g) health information; and

h) information concerning a person's sex life or sexual orientation.

We'll only process special category data if:

(i) One or more of the following lawful bases apply: consent, legitimate interest, legal obligation, performance of contract, public task or vital interest; and

(ii) One or more of the following applies:

- We have your explicit consent for example where we process biometric data for identification and verification purposes or where we have your consent to record vulnerable customer information.
- The processing is necessary for employment and social security, and social protection. For example, where we need to retain customer information (including CCTV) in relation to an investigation, or complaint around employee conduct.
- The processing is necessary to protect the vital interests of an individual where they are incapable of giving consent. For example where they need emergency medical services but are incapable of giving their consent
- The processing relates to personal data made public by the individual.
- The processing is necessary for the establishment, exercise or defence of legal claims. For example any legal proceedings in relation to collections and recoveries.
- The processing is necessary for reasons of substantial public interest. For example where we seek or receive information as part of a fraud investigation.
- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.

and

(iii) The following applies:

Where the processing is necessary for the purposes of carrying out obligations and rights in connection with employment and social security and social protection, one of the following conditions applies:

Processing is necessary for:

- Employment and social security and social protection.
- Reasons of public interest in the area of public health.

Where the processing is necessary for reasons of **substantial public interest**, one of the following conditions applies:

Processing is necessary for:

- Complying with a legal requirement, for example money laundering regulations.
- Equality of opportunity or treatment, for example in relation to accessibility and equality monitoring.
- Preventing or detecting unlawful acts, for example fraud detection, crime prevention and money laundering.
- Protecting the public against dishonesty, for example investigating fraud.
- Regulatory requirements relating to unlawful acts and dishonesty, for example fraud detection, crime prevention and money laundering.
- Preventing fraud, for example sharing information with fraud prevention agencies.
- Suspicion of fraud and terrorist financing or money laundering.
- Safeguarding children and individuals at risk.
- Safeguarding of economic well-being of certain individuals, for example to protect customers in financial difficulty and vulnerable customers.
- Insurance.
- Disclosure to elected representatives.

Criminal offence information

We also process information about criminal convictions, including allegations, investigations and proceedings (also known as “criminal offence information”) for example where we have suspicion of fraudulent activity on an account.

We'll only process criminal offence information if:

- One or more of the following lawful bases apply: consent, legitimate interest, legal obligation, performance of contract, public task or vital interest; and
- One of the following conditions applies:
  - Preventing or detecting unlawful acts
  - Protecting the public against dishonesty
  - Regulatory requirements relating to unlawful acts and dishonesty
  - Preventing fraud
  - Suspicion of terrorist financing or money laundering
  - Safeguarding of children and individuals at risk
  - Safeguarding of economic well-being of certain individuals
  - Insurance
  - Consent
  - Protecting the life of an individual
  - Information is made public by the individual
  - In relation to legal claims or to obtain legal advice
  - In connection with providing information to a court

We have the following procedures in place for complying with the principles for processing information under The General Data Protection Regulation ("GDPR"):

- **Lawful, fairness and transparency** – We:
  - provide clear and transparent information about what special category and criminal offence information we process and why we process it
  - identify our lawful basis and conditions for processing special category or criminal offence information
  - don't mislead people when we collect their information, and we don't use their information in a way they wouldn't reasonably expect.
- **Purpose limitation** – We only process special category and criminal offence information for purposes that are compatible with the purpose for which it was collected.
- **Data minimisation** – We only collect and process the minimum amount of special category and criminal offence information that is necessary and proportionate for our specified purpose. We erase any information that isn't relevant to our purpose.

- **Accuracy** – We:
  - have processes to make sure special category and criminal offence information is accurate and up to date
  - take reasonable steps to make sure that any inaccurate special category and criminal offence information is rectified or deleted without delay.
- **Storage limitation** – We only keep special category and criminal offence information for as long as we need it and for the defined periods set out in our retention schedule, which is based on our legal obligations and business needs. We review our retention schedule regularly and update it when required.
- **Integrity and confidentiality** – We:
  - have appropriate measures in place to protect special category and criminal offence information from unauthorised or unlawful processing or accidental loss or damage
  - only process electronic special category and criminal offence information within our secure network and paper records in line with our security procedures
  - use appropriate access controls so that our employees only have access to the special category and criminal offence information they need to carry out their duties.
- **Accountability** – We:
  - have an appointed Data Privacy Officer who reports to the highest level of management
  - take a 'data protection by design and default' approach to our processing
  - maintain a record of our processing activities
  - have appropriate data privacy policies and standards in place
  - implement appropriate security measures
  - provide mandatory training to all our employees
  - record (and if required) report personal data breaches
  - carry out data protection impact assessments for any high-risk processing of special category and criminal offence information.

Our retention periods for special category and criminal convictions and offences information are as set out in **Section 8**.

5. Why we use your information.

We use your information so we can deliver the banking service that meets your needs. This is so that we can:

Determine your eligibility

Like all banks, when you apply for products or services, we use automated processes to carry out financial reviews and make faster decisions (for example determining your eligibility for an account or loan). But we want to make sure this works for you and us.

We'll use automated processes to help decide whether you're eligible for a particular product, the appropriate amount of credit that we should provide, and to carry out credit and fraud prevention checks. Due to the sheer amount of information involved and the volume of applications, routine human involvement is impractical or impossible. So, to allow us to provide banking services, we need to do this work in an automated way. Some fraud checks that we carry out are necessary to meet our legal obligations.

Based on the information you provide us; we'll compare this against different metrics to determine whether you meet the eligibility criteria for an account. Or to determine whether you'll be able to make repayments on a product.

We work hard to make sure we make the right decision. Sometimes this means saying no to offering you an account or product. In making these decisions, we'll pass information to, and receive information from, Credit Reference Agencies.

If we make an automated decision on something important to you, we'll always allow you to contest the decision, give your views and make sure there's proper human involvement. If you want to exercise this right, please contact our Data Rights Team using the details shown on **Section 2**. Where possible you should provide any additional relevant information, you'd like us to consider. The logic and outcomes of this decision-making are tested regularly to make sure they're fair.

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

To meet our legitimate business interests, we'll:

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

We do this so we can provide our customers with products and services that they need. You don't have to use these products or services.

Assess lending and insurance risks

We do this to make sure we don't take excessive risks. This in the public benefit and means your money is kept safe.

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

We do this to exercise our rights our rights and make sure that you and other customers aren't subject to crime or fraudulent activity.

Manage our relationship with you and/or business and product parties

We may need to do this to make sure we 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 and product parties

We do this to keep our records accurate and up to date, and to make sure that we don't use out of date information about you.

Improve our performance

We'll use your information to make sure we give you and other customers the best possible service.

This includes testing new systems, checking processes, checking upgrades to existing systems, training, undertaking transactional analysis, conducting audits and assessing lending and insurance risks. It also involves customer modelling, statistical and trend analysis aimed at developing and improving products and services, as well as providing information to Regulators. We do this to meet our legitimate interests in providing better services to our customers and making sure your information is appropriately protected.

To undertake consumer experience research, we may pass your contact details to our trusted third-party market research companies, who may contact you on our behalf to conduct surveys and provide us with the results of your customer experience. We'll use this information to develop products, services and process improvements. You'll be given the opportunity to opt-out of these.

Improve security and combat fraud

We use biometric data analysis to combat fraudsters. When you use a debit or credit card to purchase goods or services online, we'll ask you to enter your email address, as well as a one-time password sent to your phone at the point of payment.

Although we won't store or check your email, we'll use biometric data analysis to assess the unique way you type your email and the one-time password as part of our identity verification. So should anyone else try to use your credit card or debit card to make an online purchase, we'll be alerted to it because of the way they enter your details. We also analyse how you use the App to keep your accounts safe. The lawful basis for this is the substantial public interest of combatting fraud.

Using CCTV

We use CCTV Systems (comprising static cameras and body worn video (BWV)) to record images to keep our customers, employees and property safe. Where used, BWV will capture audio as well as video imagery.

Processing personal data in this way is in our legitimate interests to:

- maintain public safety
- maintain the security of our property
- assist in the prevention of crime
- reduce the fear of crime and offer reassurance to colleagues and customers; and
- apprehend and prosecute offenders in relation to crime.

When we collect your personal data in this way, we:

- Only use carefully selected specialist service providers, where necessary.
- Will only hold your information in this way for as long as is needed.
- Will only share it in very limited circumstances, such as when we're permitted or required to comply with a legal or statutory requirement or where we need to investigate a suspected crime.

You have the right to object to us processing your information in this way. You can find out more about this, and your other rights, in **Section 9**.

Send Direct Marketing and Promotional Material

We take great care to make sure that information you receive from us is likely to be of interest to you. We do this by comparing a range of products and services provided by us and partners we work with, with what we know about your needs and interests. We may 'profile' our customers to allow us to identify relevant opportunities to promote our services and the services of partners we work with to individual customers or prospective customers. This may include reviewing historic and current data about which account or services you hold, the way you operate your accounts, your account balances and the transactions on your TSB accounts. This could include analysis of individual payments in and out of your accounts.

The profiling we carry out will aim to ensure the marketing of products and services is likely to be of interest to you. We'll do this through TSB channels, such as our branches, websites, mobile apps, telephone service; or through non-TSB channels, such as social media, websites, radio or TV advertising.

The lawful basis for the profiling we do, and any tailored marketing through these channels, is our legitimate interests. This means we have a legitimate interest in carrying out these activities to promote our business and to help ensure that our customers only receive useful information likely to be of interest to them. You can object to this by contacting our Data Rights Team. This means you'll see more general marketing, and the pages and ads may be less relevant to you; the number of advertisements will generally remain the same.

We value our relationship, so we do our best to only send you information we think may be of interest to you personally. You decide if you want to receive direct marketing from us, whether by post, email, phone or text message.

We'll only send direct marketing to TSB customers in this way if you've consented to receive it. And don't worry, you can withdraw your consent at any time. Simply contact our Data Rights Team, click 'unsubscribe' in any marketing email we send you, or follow the instructions in our marketing text messages.

From time to time, we use QR codes to direct you to a page on our website or to make it easier for you to download the mobile app. When you scan a TSB QR code, no personal information is collected, stored, or tracked by TSB.

Make the most of social media

We may share limited personal information (such as your email address) with advertising and social media platforms so they can help us show you relevant adverts and measure how effective our marketing is.

Before we share this information, we take steps to protect it by converting it into a coded form using a secure, one way process (sometimes called "hashing"). This means the information cannot be read or used in its original form.

These platforms use the same process to compare this coded information with their own records in order to recognise users across their services. They cannot see your original details as a result of this process.

We sometimes also share this coded information to help us find similar 'lookalike' audiences within our partners' userbases to help us more effectively target our advertising, and exclude customers from marketing.

We only share this information in line with applicable data protection laws and our agreements with these providers, and we don't allow it to be used for unrelated purposes.

Do what you ask us to do

If you request particular services from us, or ask a question, we'll use your personal information to respond. This is to make sure we can provide the best possible service.

Comply with legal obligations

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

Delivering better banking

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
- 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
- make sure we manage TSB as effectively and efficiently as possible.

We use your personal information in this way as it's in our business interests. It also allows us to defend our rights, provide a better service to our customers and understand what our customers want from us. Whenever we use your personal information, we'll always make sure we work to protect your interests and rights. We won't use your personal information for any purpose incompatible with those set out above.

We'll keep your data appropriately secure and let you know if we use it for a new purpose.

Occasionally we'll ask for your specific consent to use your personal information. This might be when we want to record sensitive information, such as details about your health or ethnicity.

Asking for your consent gives you control over how this information is used. You can withdraw this consent at any time.

6. Passing your information to others.

We treat your personal information as private and confidential. In some instances, we may disclose it outside TSB for the purposes set out above (including sharing information with partners who help us provide services). This may include sharing it with subcontractors. They'll act solely on our instructions or behalf and will only use your information for the purposes set out above.

We may also share your information with third parties who provide tracing services. We'll do this for the purpose of verifying and updating your contact details.

We'll 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's needed by other parties connected with your account (including guarantors)
- we need to share information with other parties who also hold a charge on your property.

We'll also disclose information where strictly necessary to comply with our legal obligations, including where:

- HMRC or other authorities require it
- the law, a regulatory body or the public interest requires it
- it's required as part of our duty to protect your accounts. For example, we're required to disclose your information to the UK Financial Services Compensation Service (FSCS)
- it's required by us or others to detect, investigate or prevent crime or fraud.

Information can also be made available where you consent or ask us to. If you give your consent, you can withdraw it at any time, and we'll stop disclosing the information in that way.

Debt Collection Agencies

As part of our debt recovery processes, we may place your account with a debt collection agency. To support this process, we'll share your information such as, account number, name and address to support the tracing and recovery of debt.

Credit Reference Agencies

In order to process your application for a product or service, we'll perform credit and identity checks on you with one or more credit reference agencies ('CRAs'). If you use our banking services, we may also make periodic searches at CRAs to help manage your account.

To do this, we'll supply your personal information to CRAs, and they'll give us information about you. This will include information from your credit application and about your financial situation and history. CRAs will supply us with public data (including the electoral register) as well as shared credit, financial situation, financial history and fraud prevention information. We'll use this information to:

- assess your creditworthiness and whether you can afford to take out a product
- verify the accuracy of the data you've provided
- prevent criminal activity, fraud and money laundering
- manage your account(s)
- trace and recover debts
- make sure any offers provided to you are appropriate to your circumstances.

We'll continue to exchange information about you with CRAs while you have a relationship with us. We'll also inform them about your settled accounts. If you borrow and don't 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'll place a search footprint on your credit file that may be seen by other lenders.

If you tell us that you have a spouse or financial associate, we'll link your records together. So make sure you discuss and share this information with them before sending the application. CRAs will also link your records together. These links will remain on both your files until such time as you or your partner successfully files for a disassociation with the CRAs to break that link.

The identities of 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 your data protection rights with CRAs are explained in detail at **experian.co.uk/crain**

Fraud Prevention Agencies

To make sure we help in the international fight against terrorism, money laundering, modern slavery and other criminal activities, the government requires us to screen applications made to us. As a result, we'll disclose information to fraud prevention agencies and to government bodies. If we think there is a risk of fraud, we may block access or stop activity on an account.

We'll study patterns of activity, check for unusual transactions and monitor devices used to access our systems, including Internet Protocol (IP) addresses and this may include using widely available geographical mobile phone or other technology to assess the location where you or any devices may be located.

TAKE FIVE TO STOP FRAUD™

Data-sharing with our parent company

TSB Bank plc is owned by Santander UK plc (Santander UK) whose ultimate parent company is Banco Santander S.A. (Banco Santander).

We'll share your personal data with Santander UK and Banco Santander and other companies in the Santander group for essential purposes, including:

- meeting legal and regulatory requirements
- preventing and detecting fraud and financial crime
- preparing and testing new banking systems
- communicating with you about your accounts.

We do this because we're required to by law or because it's in our legitimate business interests to ensure your banking services continue to run smoothly and securely.

The data shared will be within the EEA* and is therefore protected to a similar standard to when it's in the UK.

You have the same rights with regards to Santander UK and Banco Santander's processing as you do when TSB is processing/using your personal data and these rights are explained in **Section 9**. Should you wish to exercise rights in relation to Santander UK's and/or Banco Santander's processing, please contact the dedicated data rights teams at Santander UK: Santander, Sunderland, SR43 4GP and Banco Santander: C/ Juan Ignacio Luca de Tena, 11, 28027 Madrid.

The personal data shared will be held by them for as long as is necessary (i) to deal with queries and claims (ii) to comply with legal and regulatory obligations and (iii) for the purposes of their legitimate interests.

* 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.

If you have a problem accessing the information you're concerned about, or the way that Banco Santander has handled your information then, in addition to complaining to the ICO, you can also complain to the Spanish data protection regulator Agencia Española de Protección de Datos (AEPD): **aepd.es/en**.

Further information about Banco Santander's processing can be found here: **bancosantander.es/en/informacion-proteccion-datos** and about Santander UK's processing can be found here: **santander.co.uk/personal/support/customer-support/legal-information**.

Data sharing with our previous owner

We may need to share your personal data with our previous owner, Banco de Sabadell S.A. in order to comply with our legal or regulatory obligations or where it is in our legitimate interests to do so. We'll only share information that is necessary and it will be protected in line with data protection law.

Data sharing on transfer of duties

We may transfer some or all of our rights and duties under our agreement(s) with you, to another provider in the future. If we do this, we may need to share your information with them and/or their professional advisers.

We'll only share information that is necessary, and we'll make sure this is done under strict confidentiality. The processing of your information for these purposes is our legitimate interests to enable the transfer of some or all of our rights and duties to another provider.

General

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

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.

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

We process your personal data on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify your identity, 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 your personal data for different periods of time, and if you're 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 you have requested, or to employ you, or we may stop providing existing services to you.

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. If you have any questions about this, please contact us using the details in **Section 2**.

Data transfers

Fraud prevention agencies may allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards, but if the transfer is to another type of country, then the fraud prevention agencies will ensure your data continues to be protected by ensuring appropriate safeguards are in place.

7. Transferring your information outside the UK.

The UK and EEA countries* provide a high standard of data protection and privacy. However, we may run your accounts and provide other services from centres outside the UK and EEA that don't have a similar standard of data protection laws. If so, we'll require your personal information to be protected to at least UK standards. So, we only transfer personal information to:

- countries that have been confirmed as protecting personal information to UK and EEA standards
- companies in the USA certified as providing an adequate level of protection.

In other instances, we'll put contractual commitments in place which make sure personal information is protected to UK and EEA standards.

If you want to learn more about the specific countries to which we transfer personal data or need a copy of the safeguards we have in place for particular countries, 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. For instance, this can happen if you make a CHAPS or foreign payment. These external organisations may process and store your 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 EEA, your personal information may not be protected to standards similar to those in the UK. However, we'll take steps, including using 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.

8. How long we'll keep your information.

We'll keep your information for as long as your account or product application takes. And for as long as you have accounts or products with us. We'll also keep your personal information for a certain period after your application has ended, or you've closed your accounts.

When determining 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 need to hold your personal information to carry on our business for redress purposes or defend our rights. For example, if you have an account with TSB, we'll keep your information and account details while the account is open. To meet our legal and regulatory requirements, we must keep much of this information for a number of years after the account is closed – even if you don't have another account with us.

We'll also need to keep your information in order to defend our legal rights. This may be for the period during which legal claims can be made under applicable law. In the UK this is six years for contractual claims. Where possible, we'll delete information no longer needed for any of these purposes.

Where we're not able to completely delete, destroy or anonymise your personal information because, for example, there are inter-dependencies between IT systems, we'll limit access to your personal information or put it beyond use wherever possible.

9. Your rights.

You have certain rights over your personal information.

We generally won't charge you to exercise these rights:

Informed

You have a right to be informed about how we collect and use your personal data. This includes our purposes for processing your personal data, how long we'll keep it for, and who it will be shared with.

Access

You have a right to ask TSB if we have your personal information. If we do, you have a right to know:

- why we have it
- what type of information we possess
- whether we have or will send it to others, especially outside the European Economic Area (for a list of EEA countries, see **Section 7**)
- how long we'll keep it
- where we got it from
- details of any automated decision-making.

If you want, you can ask for a copy of your information.

Rectification

Where any of your information is incorrect, you have a right to tell us to correct it promptly. Please tell us as quickly as possible if you change your address or other contact details. If your information is incomplete, you can ask us to correct this too.

Object

Depending on the legal basis for which we're using your information, you may be entitled to object. For example, where we're using your information connected with marketing, we'll stop if you object. However, if we're using your information to meet certain legal obligations, we may continue to do so even if you object.

Erasure

You may have a right to have some or all of the information we hold about you deleted. However, you should be aware that, as a bank, we're required to retain many records even after you close your account. Please see **Section 8** for further information.

Portability

In certain circumstances you're entitled to receive some of your information from us electronically. We can either pass the information to you, or to another person or business if you want.

Restriction

You might also be entitled to ask us to restrict our use of your information – for example if you think the information we hold on you is incorrect.

Automated decision-making

If we make an automated decision on something important to you, we'll always allow you to contest the decision, give your views and make sure there's proper human involvement. The logic and outcomes of our decision-making are tested regularly to make sure they're fair.

Consent

If you consent to us using your information, you have the right to withdraw that consent at any time.

You can exercise these rights by contacting the Data Rights Team using the details shown on **page 2**.

Complaints

We'll work with you on any request, complaint or question you have about your personal information.

However, if you believe we haven't adequately resolved a matter, you have the right to complain to the Information Commissioner's Office (ICO), the UK's independent information rights regulator. You can visit their website at **ico.org.uk/make-a-complaint** for further information or ask for details from our Data Rights Team.

Changes to this data privacy notice

From time to time, we may make changes to this notice to reflect changes to how we process your data. If we do this, we'll post a copy of the updated privacy notice on our website. We recommend you check our website regularly for updates. If we make any significant changes to the way we process your data, we'll tell you directly before the changes are made.

Need some extra help to do your banking? This might be due to physical or mental wellbeing or a life event. We're here to support you. Let us know what you need by calling **0345 835 3858**, chat to us in the Mobile Banking App, or visit us in branch. This information is available in large print, braille and audio. Ask in branch or call us on **0345 835 3858** (lines are open Monday to Friday 8am to 6pm, Saturday 9am to 2pm).

If you have a hearing or speech impairment you can call us using the Relay UK service. Type '**18001**' before entering our telephone number. A member of the Royal National Institute for Deaf People will join the call to speak with us as you send and receive text messages. Please visit www.relayuk.bt.com to read how they manage your data.

tsb.co.uk/business

Our lost and stolen card and fraud reporting lines are open 24/7. Not all Telephone Banking services are available 24 hours, 7 days a week. Speak to a TSB colleague for more information.

If you need to call us from abroad, or prefer not to use our **0345** number, you can also call us on **+44 203 284 1576**. Calls may be monitored or recorded.

TSB Bank plc Registered Office: Henry Duncan House, 120 George Street, Edinburgh EH2 4LH. Registered in Scotland No. SC95237. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Registration No. 191240.

TSB

Business

Information correct as at August 2026
TSB17334 (08/26)