Data Privacy Policy

Approval Date: 10 June 2022
Version number: 2.0

Contents

Policy Details	
Policy name:	Data Privacy Policy
Date approved:	10 June 2022
Version number:	2.0

What is the policy objective?

This policy provides a framework for ensuring that TSB meets its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 18) and, where applicable, the EU GDPR and the Privacy and Electronic Communications Regulations. It applies to all processing of personal data carried out by, or on behalf of, TSB including processing carried out by suppliers, third parties and contractors.

Who does this policy apply to?

- All colleagues, in particular those in strategic roles responsible for deciding whether to use personal data, partners responsible for integrating data privacy into processing activities and business practices from the design stage right through the lifecycle and all partners involved in processing personal data.
- Contractors, third party suppliers and outsourcers.
- Joint Ventures and Partnerships.

Waivers

Waivers to this Policy are permitted in limited circumstances in accordance with the Waivers and Breaches Process.

Breaches

For any breaches identified please follow the incident process and guidance detailed in the Incident Manual. For further guidance and support please refer to the Incident and Breaches SharePoint site and / or Enterprise Assurance.

What must we do?	How do we check we are doing that? *(ie Monitoring of the control activity)*
All partners must comply with data protection legislation through ensuring that personal data is only processed in accordance with the Data Protection Principles: • processed fairly, lawfully and in a transparent manner. • used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.	**Processed in accordance with the Principles by:** • Complying with the Data Protection Principles Standard; • Maintaining and updating the Record of Processing (RoPA) document. The justification for the lawful basis relied upon for processing must be described in full, for example, if relying on 'legal obligations' there should be a document that outlines the legal obligation that the processing relates to. Multiple entries in the RoPA may link to the same description document if applicable. If relying on legitimate interests as the lawful basis, a legitimate interests assessment (LIA) must be undertaken and documented;

• adequate, relevant, and limited to what is necessary.
• accurate and, where necessary, up to date.
• not kept for longer than necessary; and
• kept safe and secure
	• When processing special category data the Data Privacy Policy Technical Standard: Special Category Data must be adhered to including ensuring a lawful basis, a condition and any sub conditions for processing this data are recorded and justified;
	• When processing criminal convictions and offences data a lawful basis, condition and any sub conditions for processing this data must be recorded and justified;
	• Complete Data Privacy Impact Assessments (DPIAs) in accordance with the Data privacy Impact Assessment Technical Standard and submit these to the DPO team for their view prior to processing being undertaken;
	• Successfully complete the mandatory data privacy core learning on an annual basis;
	• Where data subject requests are received, follow the data rights requests process on the Procedures Hub;
	• Have appropriate systems, methods and procedures in place to:
	  ○ change inaccurate information, add additional information to incomplete records or add a supplementary statement
	  ○ delete, suppress or otherwise stop processing personal data if required
	  ○ restrict processing
	  ○ securely move, copy or transfer personal to another organisation without affecting the data
	  ○ protect individual rights in relation to automated decision-making and profiling, particularly where processing is solely automated with legal or similarly significant effects
	  ○ recognise and respond to individuals' complaints about data protection and ensure individuals are made aware of their right to complain.
	• DPO must be notified immediately once a Personal Data Incident has been identified and incidents must be managed in accordance with the Personal Data Incidents Technical Standard;
	• When undertaking marketing or placing cookies meet the requirements set out in the Privacy and Electronic Communications Regulations (PECR) Technical Standards.
	• The Record Retention Schedule must be adhered to and records destroyed in accordance with this.

Senior Leaders must also demonstrate that appropriate technical and organisational measures have been implemented to meet the accountability principle.	• There is a clear governance structure for managing data protection with documented reporting lines and responsibilities supported by evidence including information flows between relevant groups, from the board

In addition, Senior Leaders must ensure that the Data Protection Officer does not take any direct operational decisions about the manner and purposes of processing personal data.	down and, where applicable, aligned to the SMCR Statements of Responsibility for senior managers; • Operational roles support the practical implementation of data protection and privacy, including the provision of a Data Privacy Notice; • Advice from the Data Protection Officer is sought in relation to potential or actual decisions to notify the regulator(s) of personal data security breaches. Those decisions must be taken by an Executive Member responsible for the area concerned and that notification made by the Data Protection Officer's team. The business must not notify the data protection regulator directly; • Training and awareness-raising provided for all partners, including role-specific training where appropriate; • Provide specialist training, managed by business areas, to meet the policy requirements, for all partners and contractors and maintain a record of the training undertaken and completion status; • Undertake training effectiveness reviews; • Business areas must ensure that the Data Privacy Notice accurately captures the purpose and processing of personal data undertaken by it; • Creating and keeping up to date a Record of Processing Activities document which is reviewed at least annually and when changes occur; • Ensure Data Privacy Impact Assessments (DPIAs) are carried out for uses and changes to the way personal data is processed that are likely to result in high risk to individuals' interests (according to the Bank's risk appetite, legislation and/or regulator) and/or as required by the Data Protection Officer. DPIAs must be reviewed by the business at least annually and/or where a change occurs; • Processes implemented to ensure a data protection by default approach is taken throughout the personal data lifecycle including when designing processes, systems, business practices and new products; • Ensure processes exist to identify and delete data in line with data retention schedules (including data held by third parties on behalf of TSB); • Ensure the Privacy and Electronic Communications Regulations (PECR) Technical Standards are adhered to when undertaking marketing or placing cookies.
The Data Rights Team must also ensure that individuals can exercise all of their rights and receive a response within the required timescales	• Ensure individuals are informed about their rights and all partners are made aware of how to identify and deal with both verbal and written requests; • All requests from individuals are uniquely referenced, logged and tracked to completion; • All requests must be managed in accordance with legal and regulatory requirements including: ○ Responses are provided within 30 days of receipt

	○ Searches are undertaken, for example of emails, complaints, records of other interactions with colleagues as well as product-related information; ○ Redactions are complete and an explanation for the redactions is provided to the individual; ○ The responses contain all of the supplementary information required by law; the information is provided in an accessible, concise, intelligible and secure format. • Undertake monitoring and use that information to make improvements.
The Data Protection Officer must ensure that they fulfil the DPO tasks set out in data protection legislation	• Remain independent and take no decisions in relation to the means and manner of processing; • Inform and advise TSB about its obligations to comply with the UK GDPR and other data protection laws; • Monitor compliance with the UK GDPR and other data protection laws, and with TSB's data privacy policy, including how it manages internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits; • Advise on, and monitor, data privacy impact assessments; • Be the first point of contact for the data protection regulator, the Information Commissioner (ICO) and for individuals whose data is processed (employees, customers etc). • Advise the business and notify the ICO, where required, of personal data security breaches.

Where to find out how to meet the requirements?

The key requirements documented in this policy apply to and are underpinned by the Data Privacy Technical Standards listed below. Each Technical Standard then has associated procedures designed and implemented by the business that are aligned with the stated expectations of the the Data Privacy regulator for the UK, the Information Commissioner (ICO). Further information is also available from the Policy Portal.

- Data Privacy Impact Assessment (DPIA) Technical Standards
- Data Privacy Policy Technical Standard - PECR Cookies and similar technologies v1.0 10 June 2022.pdf (sharepoint.com)
- Data Privacy Policy Technical Standard - PECR Direct Marketing v1.0 10 June 2022.pdf (sharepoint.com)
- Data Privacy Policy Technical Standard - Special Category Data v1.0 10 June 2022.pdf (sharepoint.com)
- Data Protection Principles Technical Standards
- Personal Data Incidents Technical Standards

- Procedures Hub: dsardatarightsfromcustomer (sharepoint.com)

In addition to the Data Privacy Policy and supporting Technical Standards, data privacy requirements and controls are also incorporated within the following L2 policies and technical standards:

- Information and Cyber Security Policy
- Risk Management Framework (RMF) Policy
- Technical Standard - Record Retention Schedule

Glossary	
Term:	**Definition:**
Controller	A controller is the main decision-maker that exercises control over the purposes and means of the processing of personal data, i.e., TSB.
Criminal convictions and offences	This covers a wide range of information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings and may also include personal data about unproven allegations and information relating to the absence of convictions. Information relating to criminal convictions and offences does not in itself make the data Special Category data.
Data Privacy Impact Assessment	A Data Protection Impact Assessment (DPIA) is a process to identify and minimise the data protection risks for an activity.
Data Privacy Notice	There are generally two types of Data Privacy Notice – one aimed internally and the other externally. These must contain the following: • Name and contact details of our organisation; • Name and contact details of our representative (if applicable); • Contact details of our data protection officer (if applicable); • Purposes of the processing; • Lawful basis for the processing; • Legitimate interests for the processing (if applicable); • Categories of personal data obtained (if the personal data is not obtained from the individual it relates to); • Recipients or categories of recipients of the personal data; • Details of transfers of the personal data to any third countries or international organisations (if applicable) • Retention periods for the personal data; • Rights available to individuals in respect of the processing; • Right to withdraw consent (where applicable); • Right to lodge a complaint with the regulator; • Source of the personal data (if the personal data is not obtained from the individual it relates to); • Details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to); • Details of the existence of automated decision-making, including profiling (if applicable).

Data Protection Act 2018 (DPA 18)	The DPA 2018 sets out the data protection framework in the UK, alongside the UK GDPR. It contains three separate data protection regimes: Part 2: sets out a general processing regime (the UK GDPR); Part 3: sets out a separate regime for law enforcement authorities; and Part 4: sets out a separate regime for the three intelligence services.
Data Protection by Design and by Default	In essence, this means you have to integrate or 'bake in' data protection into processing activities and business practices, from the design stage right through the lifecycle. 'Default' specifically refers to ensuring that the most privacy secure settings are in place by default, allowing the user to then open up access as they see fit.
Personal data	Any information relating to an identified or identifiable living individual. What identifies an individual could be as simple as an entry in a data field, a name or a number or could include other identifiers such as an IP address, a cookie identifier, the individual's unique way of walking caught on camera or data combined from other sources that together reveals something about an individual. The information must 'relate to' the individual in some way - it must concern them. It does not have to include the person's name. Pseudonymised data e.g., replacing names or other identifiers with, for example, a reference number is still personal data if it could be attributed to a person, or can be converted back using the relevant key by the bank. Permanently anonymised data with no names or indicators which could enable an individual to be identified is not personal data.
Privacy and Electronic Communications Regulations (PECR)	These give people specific privacy rights in relation to electronic communications. There are specific rules on: • Marketing calls, emails, texts and faxes; • Cookies (and similar technologies); • Keeping communications services secure; and • Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.
Processing	Means any operation or set of operations performed on personal data or sets of personal data such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying personal data.
Processor	A natural or legal person, agency or other body which processes personal data on behalf o the controller
Records of Processing Activity	These are documents, usually in the form of a register, that must contain: • The name and contact details of the organisation, other controllers, representative and the data protection officer. • The purposes of the processing. • A description of the categories of individuals and categories of personal data. • The categories of recipients of personal data. • Details of transfers to third countries including documenting the transfer mechanism safeguards in place. • Retention schedules. • A description of technical and organisational security measures.
Representative	This is an individual/organisation that acts for TSB where data protection legislation requires it.

Special Category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a living person's sex life or sexual orientation. It encompasses personal data revealing or concerning these types of data and that includes information where inferring or being able to guess details about someone in relation to the above areas is possible.
UK GDPR	UK General Data Protection Regulation. It came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies (that is contained in the DPA 18).

Appendix: Overview of Responsibilities

All colleagues (including temporary and contracted staff) have a responsibility to comply with this policy and to escalate any non-compliance or potential control weaknesses to senior management. Failure to comply with this policy may result in disciplinary action in accordance with HR policies. In addition, non-compliance with this policy may also result in prosecution.

Responsibilities applicable to all areas of the business:

- Design and maintain technical standards, processes, procedures and controls to ensure, and be able to evidence, compliance with this policy;
- Monitor and report on the effectiveness of controls, residual risks and areas of non-compliance to their Functional Risk Committees and the DPO;
- Breach identification, management and reporting; and
- Maintaining appropriate records demonstrating compliance including training records, record of processing activities and evidence of the application of privacy by design and by default (including data privacy impact assessments).

Each business area is responsible for ensuring that all of its activities and processes comply with data privacy law and for rectifying any breaches that are identified.

MRT Responsibilities (Operational Risk):

- Maintain this policy and ensure it is aligned to applicable privacy laws, regulatory requirements and Board risk appetite, advising of any material changes to the Board Risk Committee (BRC) and Board;
- Support the DPO and ensure effective implementation of this policy across TSB;
- Provide oversight and challenge to the first line of defence; and provide independent reporting on the aggregated TSB risk profile and policy compliance to Operational Risk and Resilience Committee and other internal forums as required
- Ensuring there is an appropriate data protection and privacy committee or other mechanism to co-ordinate the implementation and maintenance of this policy.

Data Protection Officer tasks include:

- Informing and advising TSB and its employees of their data protection obligations.
- Monitoring compliance with relevant data protection legislation and regulatory guidance and with TSB policies relating to the protection of personal data, including how TSB manages internal data protection activities; raising awareness of data protection issues, training staff and internal audits;
- Providing advice where requested relating to Data Privacy Impact Assessments and monitoring their performance;
- Being the first point of contact and cooperating with the Information Commissioner and other data protection regulators;
- Acting as a facilitator for individuals and upholding their rights

Data Protection Officer's team

- Provides expert advice and guidance about how responsibilities can be met, and the data privacy risks processing data can present.
- Undertake the DPO tasks above as required

Data Rights Team

- Manage requests from individuals in relation to their Data Subject Rights (inc. Right of Access ('DSAR'), Erasure, Portability etc)
- Provide advice and guidance to Business Areas in creating processes to support individuals in exercising their rights and identifying and transferring requests to the Data Rights Team