



Global Data Protection Policy




Target audience:	Group Companies	
Policy Owner (Responsible for the document)	CRO	
Units engaged in the implementation:	JSC TBC Bank Legal Department CEOs/Management team of Group Companies	
Reviewed by:	JSC TBC Bank Legal Department JSC TBC Bank Compliance Department JSC TBC Bank Information Security Department TBC Bank Group PLC Executive Committee JSC TBC Bank Corporate Secretary	
Approved by:	TBC Bank Group PLC Board of Directors  _____ Arne Berggren Chairman of the TBC Bank Group PLC Board of Directors	
Effective Date:	TBD	
Replaces	N/A	
In the event of any discrepancies between the English version of this Policy and a translated version, the English version shall prevail.		
Version		Date
Current version	5th	19.05.2025
Revision frequency	Annual	
Accessibility	Public	
Application and alteration	All Group Companies must adhere to this Policy in its entirety. If a Group Company wishes to adopt and modify its content, it may do so as long as the modifications do not contravene the intent of this Policy. Otherwise, any changes made require approval from TBC Bank Group PLC Board of Directors.	
Definitions	Terms written in capital letters that have not been defined in this Policy will carry the same meanings as stated in the Glossary approved by TBC Bank Group PLC Board of Directors	

Table of Contents

1. INTRODUCTION.....	4
2. SCOPE.....	4
3. APPLICABILITY OF DOMESTIC LAW AND POLICY	4
4. PERSONAL DATA PROTECTION PRINCIPLES	4
5. LAWFULNESS, FAIRNESS, TRANSPARENCY	5
6. CONSENT	5
7. TRANSPARENCY (NOTIFYING DATA SUBJECTS)	5
8. PURPOSE LIMITATION	6
9. DATA MINIMISATION	6
10. ACCURACY	6
11. STORAGE LIMITATION	6
12. SECURITY INTEGRITY AND CONFIDENTIALITY	7
13. REPORTING A PERSONAL DATA BREACH	7
14. TRANSFER LIMITATION	7
15. DATA SUBJECT'S RIGHTS AND REQUESTS.....	8
16. ACCOUNTABILITY	8
17. RECORD KEEPING.....	9
18. TRAINING AND AUDIT.....	9
19. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)	9
20. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING.....	10
21. DIRECT MARKETING	10
22. SHARING PERSONAL DATA	10
23. CHANGES TO THIS POLICY	11

1. INTRODUCTION

1.1 This **Policy** sets out how **TBC** handles the **Personal Data** of its customers, suppliers, **Employees**, workers and other third parties.

1.2 This **Policy** applies to all **Personal Data** **TBC** Process regardless of the media on which that data is stored or whether it relates to past or present **Employees**, workers, customers, clients or supplier contacts, shareholders, website users or any other **Data Subject**.

1.3 This **Policy** sets out what **TBC** expects from the **Staff** for the **TBC** to comply with applicable law. The **Staff** compliance with this **Policy** is mandatory. **Related Policies** are available to help **Staff** interpret and act in accordance with this **Policy**. The **Staff** must also comply with all such **Related Policies**. Any breach of this **Policy** may result in disciplinary action.

2. SCOPE

2.1 **TBC** recognizes that the correct and lawful treatment of **Personal Data** will maintain confidence in the organization and will provide for successful business operations. Protecting the confidentiality and integrity of **Personal Data** is a critical responsibility that **TBC** takes seriously at all times.

2.2 All **CEOs**, **Data Protection Executives**, head of units, departments, are responsible for ensuring all **TBC Staff** comply with this **Policy** and need to implement appropriate practices, processes, controls and training to ensure that compliance.

2.3 The **DPO** (where necessary) is responsible for overseeing this **Policy** and, as applicable, developing **Related Policies**.

3. APPLICABILITY OF DOMESTIC LAW AND POLICY

Data Subjects keep any rights and remedies they may have under applicable domestic law. This **Policy** shall apply only where it provides supplemental protection for **Personal Data**. Where applicable domestic law provides more protection than this **Policy**, domestic law shall apply. Where this **Policy** provides more protection than applicable domestic law or provides additional safeguards, rights or remedies for Individuals, this **Policy** shall apply.

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 **TBC** adheres to the principles relating to **Processing** of **Personal Data** which require **Personal Data** to be:

- (a) **Processed** lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- (b) collected only for specified, **Explicit** and legitimate purposes (Purpose Limitation);
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is **Processed** (Data Minimization);
- (d) accurate and where necessary kept up to date (Accuracy);
- (e) not kept in a form which permits identification of **Data Subjects** for longer than is necessary for the purposes for which the data is **Processed** (Storage Limitation);
- (f) **Processed** in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorized or unlawful **Processing** and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
- (g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
- (h) made available to **Data Subjects** and allow **Data Subjects** to exercise certain rights in relation to their **Personal Data** (**Data Subject's** Rights and Requests).
- (i) **TBC** is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 **Personal Data** must be **Processed** lawfully, fairly and in a transparent manner in relation to the **Data Subject**.

5.2 TBC only collects, **Process** and shares **Personal Data** fairly and lawfully and for specified purposes. TBC restricts its actions regarding **Personal Data** to specified lawful purposes. These restrictions are not intended to prevent **Processing** but ensure that TBC **Process Personal Data** fairly and without adversely affecting the **Data Subject**.

5.3 Some examples of allowed **Processing** for specific purposes are set out below:

- (a) the **Data Subject** has given his or her **Consent**;
- (b) the **Processing** is necessary for the performance of a contract with the **Data Subject**;
- (c) to meet our legal compliance obligations;
- (d) to protect the **Data Subject**'s vital interests;
- (e) to pursue our legitimate interests for purposes where they are not overridden because the **Processing** prejudices the interests or fundamental rights and freedoms of **Data Subjects**.

5.4 The purposes for which TBC **Process Personal Data** for legitimate interests need to be set out in applicable **Privacy Notices**; or the **Staff** must identify and document the legal ground being relied on for each **Processing** activity.

6. CONSENT

6.1 A **Controller** must only **Process Personal Data** on the basis of one or more of the lawful bases set out in this **Policy**, which include **Consent**.

6.2 A **Data Subject Consents** to **Processing** of their **Personal Data** if they indicate agreement clearly either by a statement or positive action to the **Processing**. **Consent** requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If **Consent** is given in a document which deals with other matters, then the **Consent** must be kept separate from those other matters.

6.3 **Data Subjects** must be easily able to withdraw **Consent** to **Processing** at any time and withdrawal must be promptly honored. **Consent** may need to be refreshed if TBC intends to **Process Personal Data** for a different and incompatible purpose which was not disclosed when the **Data Subject** first **Consented**.

6.4 When **Processing Special Category Data** or **Criminal Convictions Data**, TBC will usually rely on a legal basis for **Processing** other than **Explicit Consent** or **Consent** if possible. Where **Explicit Consent** is relied on, the TBC must issue a **Privacy Notice** to the **Data Subject** to capture **Explicit Consent**.

6.5 TBC will need to evidence **Consent** captured and keep records of all **Consents** in accordance with **Related Policies** so that the TBC can demonstrate compliance with **Consent** requirements.

7. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

7.1 **Data Controllers** shall provide detailed, specific information to **Data Subjects** depending on whether the information was collected directly from **Data Subjects** or from elsewhere. The information must be provided through appropriate **Privacy Notices** which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a **Data Subject** can easily understand them.

7.2 Whenever TBC collects **Personal Data** directly from **Data Subjects**, including for human resources or employment purposes, the **Staff** must provide the **Data Subject** sufficient information including the identity of the **Controller** and **DPO** or **Data Protection Executive**, how and why TBC will use, **Process**, disclose, protect and retain that **Personal Data** through a **Privacy Notice** which must be presented when the **Data Subject** first provides the **Personal Data**.

7.3 The **Staff** must check that the **Personal Data** was collected by the third party in

accordance with the law and on a basis which contemplates our proposed **Processing** of that **Personal Data**.

8. PURPOSE LIMITATION

8.1 **Personal Data** must be collected only for specified, **Explicit** and legitimate purposes. It must not be further **Processed** in any manner incompatible with those purposes.

8.2 **TBC** cannot use **Personal Data** for new, different or incompatible purposes from that disclosed when it was first obtained unless the **Staff** have informed the **Data Subject** of the new purposes and they have **Consented** where necessary.

9. DATA MINIMISATION

9.1 **Personal Data** must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is **Processed**.

9.2 The **Staff** may only **Process Personal Data** when performing their job duties requires it. The **Staff** cannot **Process Personal Data** for any reason unrelated to their job duties.

9.3 The **Staff** may only collect **Personal Data** required for their job duties: the **Staff** shall not collect excessive data and must ensure that any **Personal Data** collected is adequate and relevant for the intended purposes.

9.4 The **Staff** must ensure that when **Personal Data** is no longer needed for specified purposes, it is deleted or anonymized in accordance with the **TBC's** data retention guidelines.

9.5 The **Group Companies** will adopt and update, if necessary, procedures to ensure the best practices are maintained to achieve data minimization.

10. ACCURACY

10.1 **Personal Data** must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

10.2 The **Staff** will ensure that the **Personal Data** **TBC** uses and holds is accurate, complete, kept up to date and relevant to the purpose for which **TBC** collected it. The **Staff** must check the accuracy of any **Personal Data** at the point of collection and at regular intervals afterwards. The **Staff** must take all reasonable steps to destroy or amend inaccurate or out-of-date **Personal Data**.

10.3 The **Group Companies** will adopt and update, if necessary, procedures to ensure that data quality is maintained by regular check-ups, and the **Staff** can easily comprehend the principles that are to guide them with respect to data quality/accuracy.

11. STORAGE LIMITATION

11.1 **Personal Data** must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is **Processed**.

11.2 **Staff** must not keep **Personal Data** in a form which permits the identification of the **Data Subject** for longer than needed for the legitimate business purpose or purposes for which **TBC** originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

11.3 The **TBC** will maintain retention policies and procedures to ensure **Personal Data** is deleted after a reasonable time for the purposes for which it was being held unless a law requires that data to be kept for a minimum time.

11.4 **Staff** will take all reasonable steps to destroy or erase from our systems all **Personal Data** that **TBC** no longer require in accordance with all the **TBC's** applicable records, retention schedules and policies. This includes requiring third parties to delete that data where applicable.

11.5 **Staff** will ensure **Data Subjects** are informed of the period for which data is stored and how that period is determined in any applicable **Privacy Notice**.

12. SECURITY INTEGRITY AND CONFIDENTIALITY

12.1 **Personal Data** must be secured by appropriate technical and organizational measures against unauthorized or unlawful **Processing**, and against accidental loss, destruction or damage.

12.2 **TBC** will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of **Personal Data** that **TBC** owns or maintains on behalf of others and identified risks (including use of encryption and Pseudonymization where applicable). **TBC** will regularly evaluate and test the effectiveness of those safeguards to ensure security of our **Processing of Personal Data**. The **Staff** is responsible for protecting the **Personal Data** **TBC** holds. The **Staff** must implement reasonable and appropriate security measures against unlawful or unauthorized **Processing of Personal Data** and against the accidental loss of, or damage to, **Personal Data**. The **Staff** must exercise particular care in protecting **Special Categories of Personal Data** and **Criminal Convictions Data** from loss and unauthorized access, use or disclosure.

12.3 The **Staff** must follow all procedures and technologies **TBC** puts in place to maintain the security of all **Personal Data** from the point of collection to the point of destruction. The **Staff** may only transfer **Personal Data** to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

12.4 The **Staff** must maintain data security by protecting the confidentiality, integrity and availability of the **Personal Data**, defined as follows:

- (a) Confidentiality means that only people who have a need to know and are authorized to use the **Personal Data** can access it;
- (b) Integrity means that **Personal Data** is accurate and suitable for the purpose for which it is **Processed**; and
- (c) Availability means that authorized users are able to access the **Personal Data** when they need it for authorized purposes.

12.5 **Staff** must comply with and not attempt to circumvent the administrative, physical and technical safeguards **TBC** implements and maintains in accordance with the relevant standards to protect **Personal Data**.

13. REPORTING A PERSONAL DATA BREACH

13.1 **TBC** has put in place procedures to deal with any suspected **Personal Data Breach** and will notify **Data Subjects** or any applicable regulator where **TBC** are legally required to do so.

13.2 If **Staff** knows or suspects that a **Personal Data Breach** has occurred, they shall not attempt to investigate the matter and immediately contact the person or team designated as the key point of contact for **Personal Data Breaches**. The **Staff** should preserve all evidence relating to the potential **Personal Data Breach**.

14. TRANSFER LIMITATION

14.1 If **TBC** seeks to transfer **personal data** internationally, it will be executed in adherence to the regulations set forth by the applicable domestic law. Nevertheless, during such transfers, **TBC** will exert every effort to ensure that data is transferred securely and with complete confidentiality, fully complying with applicable domestic law.

Personal Data might be shared internationally under various circumstances, including:

- (a) The country receiving the information ensures adequate protection guarantees in line with applicable domestic law or the decision of the European Commission (only in case where **GDPR** is applicable)
- (b) In cases where applicable domestic law does not stipulate appropriate safeguards, or there is no relevant decision by the European Commission, **TBC** may transfer personal data to a third country or international organization only if **TBC** implements suitable measures stipulated by applicable domestic law or **GDPR** (if the latter is applicable).

14.2 If the applicable domestic law lacks appropriate provisions, or there is no decision by the European Commission or relevant guarantees, or there are no approved and applicable Binding Corporate Rules of European Commission, the transfer of personal data to a third country or international organization is carried out only in the following cases:

- (a) If the transfer is necessary for the conclusion or performance of a contract in alignment with the interests of the **data subject**;
- (b) If the transfer is necessary due to significant public interest;
- (c) If the transfer is necessary to comply with legal requirements or for protective purposes.
- (d) If the transfer is necessary to protect the vital interests of the **data subject** or other individuals, and the **data subject** is unable to provide consent.
- (e) In other circumstances stipulated by applicable domestic law or **GDPR** (only in case when **GDPR** is applicable).

15. DATA SUBJECT'S RIGHTS AND REQUESTS

15.1 **Data Subjects** have rights when it comes to how **TBC** handles their **Personal Data**. These include rights to:

- (a) withdraw **Consent** to **Processing** at any time;
- (b) receive certain information about the **Data Controller's Processing** activities;
- (c) request access to their **Personal Data** that **TBC** holds;
- (d) prevent our use of their **Personal Data** for direct marketing purposes;
- (e) ask us to erase **Personal Data** if it is no longer necessary in relation to the purposes for which it was collected or **Processed** or to rectify inaccurate data or to complete incomplete data;
- (f) restrict **Processing** in specific circumstances;
- (g) challenge **Processing** which has been justified on the basis of our legitimate interests or in the public interest;
- (h) request a copy of an agreement under which **Personal Data** is transferred to **Non-Adequate Country**;
- (i) object to decisions based solely on **Automated Processing**, including profiling (**ADM**);
- (j) prevent **Processing** that is likely to cause damage or distress to the **Data Subject** or anyone else;
- (k) be notified of a **Personal Data Breach** which is likely to result in high risk to their rights and freedoms;
- (l) make a complaint to the supervisory authority; and
- (m) in limited circumstances, receive or ask for their **Personal Data** to be transferred to a third party in a structured, commonly used and machine-readable format;

15.2 The **Staff** must verify the identity of an individual requesting data under any of the rights listed above (**Staff** shall not allow third parties to persuade them into disclosing **Personal Data** without proper authorization).

15.3 The **Staff** must immediately forward any **Data Subject** request they receive to **Data Protection Executive** or **DPO**.

16. ACCOUNTABILITY

16.1 **TBC** must implement appropriate technical and organizational measures in an effective manner, to ensure compliance with data protection principles. **TBC** is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 **TBC** must have adequate resources and controls in place to ensure and to document compliance with data protection principles including:

- (a) appointing a suitably qualified **DPO** (where necessary) and an executive accountable for data privacy;
- (b) implementing **Privacy by Design** when **Processing Personal Data** and completing **DPIAs** where **Processing** presents a high risk to rights and freedoms of **Data Subjects**;
- (c) integrating data protection into internal documents including this **Policy, Related Policies, or Privacy Notices**;
- (d) regularly training the **Staff** on the **GDPR** (where necessary), this **Policy, Related Policies** and data protection matters including, for example, **Data Subject's** rights, **Consent**, legal basis, **DPIA** and **Personal Data Breaches**. The **TBC** must maintain a record of training attendance by the **Staff**; and
- (e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. RECORD KEEPING

17.1 **Staff** must keep and maintain accurate corporate records reflecting our **Processing** including records of **Data Subjects' Consents** and procedures for obtaining **Consents**.

17.2 These records should include, at a minimum, the name and contact details of the **Controller** and the **DPO or Data Protection Executive**, clear descriptions of the **Personal Data** types, **Data Subject** types, **Processing** activities, **Processing** purposes, third-party recipients of the **Personal Data**, **Personal Data** storage locations, **Personal Data** transfers, the **Personal Data's** retention period and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

18. TRAINING AND AUDIT

18.1 **TBC** is required to ensure **Staff** have undergone adequate training to enable them to comply with data privacy laws. **TBC** must also regularly test its systems and processes to assess compliance.

18.2 The **Staff** must undergo all mandatory data privacy related training.

18.3 The **Staff** must regularly review all the systems and processes under their control to ensure they comply with this **Policy** and check that adequate governance controls and resources are in place to ensure proper use and protection of **Personal Data**.

19. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

19.1 **TBC** is required to implement **Privacy by Design** measures when **Processing Personal Data** by implementing appropriate technical and organizational measures (like Pseudonymization) in an effective manner, to ensure compliance with data privacy principles.

19.2 **Staff** must assess what **Privacy by Design** measures can be implemented on all programs, systems or processes that Process **Personal Data** by taking into account the following:

- (a) the state of the art;
- (b) the cost of implementation;
- (c) the nature, scope, context and purposes of **Processing**; and
- (d) the risks of varying likelihood and severity for rights and freedoms of **Data Subjects** posed by the **Processing**.

19.3 **Data Controllers** must also conduct **DPIAs** in respect to high-risk **Processing**.

19.4 The **Staff** should conduct a **DPIA** (and discuss their findings with the **DPO or Data Protection Executive**) when implementing major system or business change programs involving the **Processing** of **Personal Data** including:

- (a) use of new technologies (programs, systems or processes), or changing technologies

(programs, systems or processes);

(b) **Automated Processing** including profiling and ADM;

(c) large-scale **Processing** of **Special Categories of Personal Data** or **Criminal Convictions Data**; and

(d) large-scale, systematic monitoring of a publicly accessible area.

(e) A **DPIA** must include:

(f) a description of the **Processing**, its purposes and the **Data Controller's** legitimate interests if appropriate;

(g) an assessment of the necessity and proportionality of the **Processing** in relation to its purpose;

(h) an assessment of the risk to individuals; and

(i) the risk mitigation measures in place and demonstration of compliance.

20. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

20.1 Generally, **ADM** is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a **Data Subject** has **Explicitly Consented**;

(b) the **Processing** is authorized by law; or

(c) the **Processing** is necessary for the performance of or entering into a contract.

20.2 If certain types of **Special Categories of Personal Data** or **Criminal Convictions Data** are being processed, then grounds (b) or (c) will not be allowed but the **Special Categories of Personal Data** and **Criminal Convictions Data** can be **Processed** where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

20.3 If a decision is to be based solely on **Automated Processing** (including profiling), then **Data Subjects** must be informed when the **Staff** first communicate with them of their right to object. This right must be **Explicitly** brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the **Data Subject's** rights and freedoms and legitimate interests.

20.4 **Staff** must also inform the **Data Subject** of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the **Data Subject** the right to request human intervention, express their point of view or challenge the decision.

20.5 A **DPIA** must be carried out before any **Automated Processing** (including profiling) or **ADM** activities are undertaken.

21. DIRECT MARKETING

21.1 **TBC** is subject to certain rules and privacy laws when marketing to its customers.

21.2 For example, a **Data Subject's** prior **Consent** is required for electronic direct marketing (for example, by email, text or automated calls) unless otherwise stipulated by applicable domestic law.

21.3 The right to object to direct marketing must be explicitly offered to the **Data Subject** in an intelligible manner so that it is clearly distinguishable from other information.

21.4 A **Data Subject's** objection to direct marketing must be promptly honored. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

22. SHARING PERSONAL DATA

22.1 Generally, **TBC** are not allowed to share **Personal Data** with third parties unless certain safeguards and contractual arrangements have been put in place.

22.2 **Staff** may only share the **Personal Data** **TBC** holds with another **employee**, agent

or representative of our group (which includes our subsidiaries and our ultimate holding **TBC** along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

22.3 Staff may only share the **Personal Data** **TBC** holds with third parties, such as our service providers, if:

- (a) they have a need to know the information for the purposes of providing the contracted services;
- (b) sharing the **Personal Data** complies with the **Privacy Notice** provided to the **Data Subject** and, if required, the **Data Subject's Consent** has been obtained;
- (c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- (d) the transfer complies with any applicable cross-border transfer restrictions; and
- (e) a fully executed written contract that contains **GDPR**-approved third party clauses has been obtained.

23. CHANGES TO THIS POLICY

23.1 We keep this **Policy** under regular review. Historic versions (if any) can be obtained by contacting **Data Protection Executive** or **DPO** (where necessary).