TBC BANK GROUP PLC

GLOBAL DATA PROTECTION POLICY

INFORMATION SHEET

Target audience:	All employees (temporary or permanent) of all majority owned TBC Bank Group PLC businesses (or business units).	
Department responsible for the document	Compliance Department Legal Department Information Security Department	
Corporate units engaged in the implementation	Compliance Department	
	Information Security Department	
	Legal Department	
Reviewed by	Compliance Department	
	Legal Department	
	Information Security Department	
Approved by	Subject to decision of the Board of Directors of TBC Bank Group PLC	
Effective Date	To be determined following the Board of Directors decision	
Replaces	This TBC Bank Group PLC Global Data Protection Policy ("Policy") supersedes all TBC Bank Group PLC data protection policies that exist on the Effective Date to the extent they address the same issues and are not consistent with this Policy.	
In the event of any discrepancies between the English version of this Policy and a translated version, the English version shall prevail.		
	Version	**Date**
Version I	V1	29 October 2021
Current Version	V1	29 October 2021

CONTENTS

1. INTRODUCTION

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

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.

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

TBC recognises that the correct and lawful treatment of Personal Data will maintain confidence in the organisation 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.

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.

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

3. APPLICABILITY OF LOCAL LAW AND POLICY

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

4. PERSONAL DATA PROTECTION PRINCIPLES

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 Minimisation);

(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 organisational measures to protect against unauthorised 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).

The Staff is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

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

The Staff 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.

The 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. 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

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.

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.

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

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 Staff must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

The Staff 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)

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.

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.

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

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.

The Staff 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

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

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.

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.

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

10. ACCURACY

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

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.

11. STORAGE LIMITATION

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

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.

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.

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.

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

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

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 Pseudonymisation 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 unauthorised 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 unauthorised access, use or disclosure.

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.

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 authorised 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 authorised users are able to access the Personal Data when they need it for authorised purposes.

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

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.

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

Staff may transfer Personal Data to a third party located in a Non-Adequate Country only if:

(a) The transfer is necessary for the performance of a contract with the Data Subject, for managing a contract with the Data Subject or to take necessary steps at the request of the Data Subject prior to entering into a contract, e.g., for processing orders; or

(b) A contract has been concluded between TBC and the relevant third party that provides for safeguards at a similar level of protection as that provided by this Policy or the contract shall conform to any model contract requirement under applicable local law, if any; or

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between TBC and a third party; or

(d) The third party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an “adequate” level of data protection; or

(e) The third party has implemented binding corporate rules or a similar transfer control mechanism which provide adequate safeguards under applicable law, a copy of the binding corporate rules or evidence of the transfer control mechanism must be provided to TBC prior to the transfer taking place;

or

(f) The transfer is necessary to protect a vital interest of the Data Subject; or

(g) The transfer is necessary in connection with legal proceedings, advice or rights; or

(h) The transfer is necessary to satisfy a pressing need to protect an important public interest; or

(i) The transfer is required by any law or regulation to which the relevant Group Company is subject; or

(j) The Data that will be transferred is included in a public register.

Items (h) and (j) above require:

(a) The prior approval of the appropriate Data Protection Executive; and

(b) That suitable measures are taken to safeguard the legitimate interests of the Data Subject (which may include consultation with relevant data protection authority).

If none of the grounds listed above exist or if applicable local law so requires TBC shall (also) seek either consent from the Data Subject or approval from a supervisory authority (whichever is required by applicable local law) for the transfer to a third party located in a Non-Adequate Country. Prior to asking for consent or approval, the Data Subject or supervisory authority shall be provided with the following information:

(a) The purpose of the transfer; and

(b) The identity of the transferring Group Company; and

(c) The identity or categories of third parties to which the Data will be transferred; and

(d) The categories of Data that will be transferred; and

(e) The country to which the Data will be transferred; and

(f) The fact that the Data will be transferred to a Non-Adequate Country.

15. DATA SUBJECT'S RIGHTS AND REQUESTS

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;

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 authorisation).

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

16. ACCOUNTABILITY

TBC must implement appropriate technical and organisational 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.

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

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

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

TBC are 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.

The Staff must undergo all mandatory data privacy related training.

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)

TBC are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Staff must assess what Privacy by Design measures can be implemented on all programmes, 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.

Data controllers must also conduct DPIAs in respect to high-risk Processing.

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.

A DPIA must include:

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

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

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

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

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

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 authorised by law; or

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

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.

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.

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.

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

21. DIRECT MARKETING

TBC are subject to certain rules and privacy laws when marketing to its customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

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.

A Data Subject's objection to direct marketing must be promptly honoured. 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

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

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.

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

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

24. DEFINITIONS

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Staff: all employees, workers, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. TBC are the Controller of all Personal Data relating to its Staff and Personal Data used in business for its own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom TBC holds Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Executive: DPO if it's required under GDPR or in any other case the person designated by each Group Company responsible for supervising general compliance with and for advice on the implementation and interpretation of the Policy throughout TBC;

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the TBC data privacy team with responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Group Companies: TBC Bank Group PLC, TBC Bank, and any company or legal entity, including branches and representative offices, of which TBC Bank Group PLC, directly or indirectly, owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint or remove the majority of the member of the board of directors or

equivalent governing body or cast the majority of votes at meetings of the board of directors or equivalent governing body.

Non-Adequate Country: a country that under applicable local law (such as Article 25 of the GDPR or Georgian Law on Personal Data Protection) is deemed not to provide an "adequate" level of data protection. For data transfers which falls within the scope of the GDPR a schedule of Adequate Countries is available on European Commission website (see *European Commission: Data protection*), for data transfers when Georgian Law applies a schedule of Adequate Countries is available on *Legislative Herald of Georgia* website. In all other cases, where there is a conflict between applicable local law and the Policy, the relevant manager of Employees or Staff raising the issue shall consult with the Bank Data Protection Executive.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that TBC can identify (directly or indirectly) from that data alone or in combination with other identifiers TBC possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that TBC or its third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data privacy principles.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the TBC collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the TBC's policies, operating procedures or processes related to this Privacy Standard and designed, developed and implemented to protect Personal Data.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.
TBC: TBC Bank Group PLC and its Group Companies.