



# TD Bank Europe Limited Privacy Notice

## CONTENTS

1. INTRODUCTION	2
2. KEY DEFINITIONS	2
3. OBLIGATIONS OF THE DATA CONTROLLER	3
4. WHAT ARE OUR LEGAL GROUNDS FOR USING YOUR PERSONAL INFORMATION?	3
5. PURPOSES OF PROCESSING YOUR PERSONAL INFORMATION	4
6. SHARING YOUR PERSONAL INFORMATION	5
7. AUTOMATED DECISION MAKING	6
8. PROTECTION OF YOUR PERSONAL INFORMATION	6
9. YOUR RIGHTS AND CONTACTING US	6
10. PRIVACY BREACHES	7
11. CHANGES TO THIS PRIVACY NOTICE	7

## 1. Introduction

TD N.V., formerly known as TD Bank N.V., closed its retail operations on 30 October 2020. Following the closure, all customer records have been transferred to TD Bank Europe Limited ("**TDBEL**") in the U.K. for safekeeping and retention for regulatory purposes.

This Privacy Notice applies to all persons with whom TD N.V. used to have a direct or indirect relationship and whose data is now held by TDBEL.

TDBEL is now the **data controller** in respect to the information that TD N.V. previously held about its customers. This means that we are responsible for deciding how we hold and use your Personal Information.

In this Notice, the words "you" and "your" mean any data subject or individual customer. Any reference to "we", "us", "our" or "they" refers to TDBEL and other members of the TD Bank Group who may receive the personal information to which this Notice applies

This Privacy Notice describes your rights under the EU and UK General Data Protection Regulation (the "**GDPR**") and explains how we use your information, the conditions under which we may disclose it to others, and how we keep it secure.

We have appointed a Data Protection Officer (DPO) to oversee compliance with this Privacy Notice and GDPR generally. If you have any questions about this Privacy Notice or how we handle your Personal Information, please contact:

Data Protection Officer  
TDBEL  
60 Threadneedle Street  
London  
United Kingdom  
EC2R 8AP  
[PrivacyEuropeandAsiaPacific@td.com](mailto:PrivacyEuropeandAsiaPacific@td.com)

## 2. Key definitions

"**Personal Information**" means any personal data or details from which a living individual may be directly or indirectly identified whether on its own or in conjunction with any other information we may have or be able to access (e.g., from you directly and/or obtained from others within or outside our organisation).

Examples of the categories of Personal Information we may hold about you include:

- your contact details e.g. your name, address, telephone numbers and email address;
- your personal details, e.g. name, previous names, gender, date and place of birth, country of residence and employment status;
- information concerning your identity e.g. photo ID, passport information, National ID card, nationality and governmental identification number (for example Citizen Service Number ('BSN) or National Insurance Number) and utility bills;
- other information about you that you gave us by filling in forms or by communicating with us, whether face-to-face, by phone, email, online, or otherwise;
- your account information (for example account numbers, transaction history, passwords, and other (authentication) information relating to your previous use of

TDBEL is registered under Company No. 02734652 and Registration No. GB397103051.

©The TD logo and other trademarks the property of The Toronto-Dominion Bank.

- our electronic networks, including our former Secure Customer Portal and our former mobile application); and
- details of the third parties you have nominated, including their names and dates of birth.

**“Process” or “processing”** means any operation or set of operations which is performed on Personal Information (or sets of Personal Information), whether or not by automated means, such as organisation, structuring, storage, adaptation or alteration, obtaining, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**“Special categories of personal data”** means any personal data that provides information on persons’ religious or philosophical beliefs, race or ethnic origin, political opinions, health, genetics, biometrics, sexual life or orientation, or membership of trade unions.

**“Criminal personal data”** means any personal data that provides information on persons’ criminal convictions, offences, or related security measures.

### 3. **Obligations of the Data Controller**

This Privacy Notice applies to the processing carried out by TDBEL.

TDBEL  
60 Threadneedle Street  
London  
United Kingdom  
EC2R 8AP

As data controller, we are accountable and have an obligation to ensure that we process your Personal Information in compliance with the law. This means that your Personal Information must be:

- Processed fairly, lawfully and in a transparent way;
- Collected only for specified, explicit and legitimate purposes that are clearly explained to you and not used in any way that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary for the purposes for which they are processed;
- Accurate and up to date;
- Not kept for longer than is necessary for the purposes explained to you;
- Processed in line with your rights;
- Kept securely; and
- Not transferred to other countries outside the EEA or UK without adequate protection.

### 4. **What are our legal grounds for using your Personal Information?**

The table below explains the various legal processing grounds available under the GDPR which we rely on for processing your Personal Information:

(a) <b>Our legal obligations and rights:</b> where we are required to process your Personal Information under a statutory obligation, primarily as a result of our status as a regulated financial institution.
(b) <b>Legitimate interests:</b> where we use your Personal Information to achieve a legitimate business interest and our reasons for using it do not outweigh your data protection rights.

Under limited circumstances, we may also process criminal personal data. We will only process criminal personal data when the processing is authorised by applicable law that provides for appropriate safeguards for the rights and freedoms of data subjects. For example, where we participate in incident registers and alert systems for the financial sector, and as a result may process criminal data for that purpose. The purpose of an incident register or alert system is to protect the interests of financial institutions and their clients, for example by detecting fraud.

We may use your Personal Information on other grounds in exceptional and limited circumstances, in particular, without your knowledge or consent:

- Where we need to protect your interests (or someone else's interests);
- Where it is needed in the public interest or for official purposes;
- If knowledge would compromise the availability or accuracy of your information and it is required to investigate a breach of the Guidelines of Conduct or contravention of UK law;
- If it is publicly available (such as name, address and telephone number of a subscriber in a telephone directory);
- If we have reasonable grounds to believe your information could be useful when investigating a contravention of a European, UK or foreign law and the information is used for that investigation.

## 5. Purposes of processing your Personal Information

We will process your Personal Information, including disclosure to third parties or other entities within TD Bank Group, for any of the following purposes, on the associated supporting legal ground:

- **Compliance:** with legal and regulatory requirements relating to the retention of financial records and related information; the lawful basis is compliance with legal obligation;
- **Website:** for security purposes, including monitoring use of our information and communication systems to ensure compliance with our IT and equivalent policies, ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. The lawful bases are our legitimate interests to enable us to ensure the security of our systems and further improve our services.
- **To prevent and detect crime including, e.g. fraud, terrorist financing and money laundering:** we conducted certain checks on you, such as know your customer (KYC) checks, anti-money laundering (AML) checks, and anti-fraud checks during our relationship with you, where required; complying with laws applicable to us as a data controller (for instance by processing e-mails) and with laws and regulations regarding anti-money laundering, anti-terrorist financing, financial abuse, fraud and any other criminal activity, including cooperating with regulators, participating in internal and external investigations if any of these or any other suspicious activities are suspected. The lawful bases are our legal obligations and rights and legitimate interests to ensure the integrity and security of the financial sector. For criminal personal data, please refer to paragraph 4 above.
- **Operations support:** for undertaking business management, including accounting and auditing and for assisting with, managing and improving the operations, including security, of TD Bank Group enterprise-wide. The lawful bases are our

legitimate interests to enable the TD Bank Group to manage its business. For criminal personal data, please refer to paragraph 4 above.

- **Protecting our legal rights:** deal with legal disputes involving you, or other individuals including client representatives or customers. The lawful bases are our legitimate interests to enable us to cooperate with law enforcement and regulators and legal obligations and rights. For criminal personal data, please refer to paragraph 4 above.

Some of the above purposes for processing will overlap and there may be several lawful bases which justify our retention and use of your Personal Information.

However, we will only use your Personal Information for the original purposes for which it was collected, unless we reasonably consider that we need to use it for another purpose and that purpose is compatible with the original purpose. If we need to use your Personal Information for an unrelated purpose, we will make every effort to notify you and explain the legal basis which allows us to do so.

## 6. Sharing your Personal Information

We may share your Personal Information within TD Bank Group (as many of our processes are centralised) and with third parties, where it is necessary for the purpose for which it was collected or where we have another legitimate interest in doing so.

The Personal Information that was collected and is currently stored is exclusively used by us, except in the following cases where we may submit the data to recipient parties:

- When required by law; and/or
- To the following categories of third parties, including members of the TD Bank Group, but only to the extent they are necessary to provide services which support the following operations:
  - Law enforcement, government, courts, dispute resolution bodies, our regulators, auditors and any party appointed or requested by our regulators to carry out investigations or audits of our activities, or for the management of risks and disputes;
  - Financial crime prevention agencies, Competent Authorities and other Government Agencies for the prevention and detection of crime including, e.g. fraud, terrorist financing and money laundering;
  - Legal counsel and supporting third parties (e.g. investigators, forensic accountants, as applicable) for the protection of our legal rights.

We require third parties to respect the security of your Personal Information and to treat it in accordance with the law. We do not allow our third-party service providers to use your Personal Information for their own purposes. We only permit them to process your Personal Information for specified purposes and in accordance with our instructions. External third parties requiring access to any Personal Information within our control will have signed a confidentiality agreement and/or contract containing confidentiality and privacy wording with us. In these documents, the third party agrees to keep confidential any and all Personal Information they receive. They also agree not to collect, use or disclose it to any party other than as necessary to deliver the service in question to us.

Where we disclose personal data or criminal personal data in response to requests from regulators and law enforcement or security agencies, these regulators and law enforcement or security agencies

will be acting as a controller. We will always assess the legitimacy of such requests before disclosing any personal data and/or criminal personal data and only disclose the data required to comply with the request.

We will never rent or sell your Personal Information.

Your data may be transferred to countries outside the European Economic Area (“EEA”) or UK, for example, if any of our servers are located in a country outside of the EEA/UK. These countries may have different data protection laws. As we operate in various jurisdictions, we may share data with our central groups in Toronto, Canada under the European Commission’s 2002 Adequacy Finding. If the data is going to other jurisdictions – like the USA – other measures will be used to protect your Personal Information, such as the European Commission’s Standard Contractual Clauses.

By providing your Personal Information, you are acknowledging that this transfer, storing or processing may take place. If we transfer your information outside of the EEA/UK, we will take steps to help ensure that appropriate measures are taken to protect your privacy rights, as outlined in this Privacy Notice. You can request more information about any such measures taken from the DPO (please refer to section 1 above for contact details).

## **7. Automated Decision Making**

We do not envisage that any decisions would be taken about you using automated means, however, if this position changes we would take steps to notify you.

## **8. Protection of your Personal Information**

We have in place a number of appropriate technical and organization measures to protect our systems and your Personal Information. These include but are not limited to:

- Personal Information is only accessible by a limited number of relevant staff bound by duties of confidentiality;
- All electronic information is held on systems that incorporate firewalls, password-controlled access and virus protection procedures; and
- We audit our procedures and security measures regularly to help ensure that they are being properly administered and that they remain effective and appropriate to the sensitivity of the information.

We keep your Information for no longer than is necessary for the purpose(s) for which it was collected (including for the purposes of satisfying any legal, regulatory, accounting or reporting requirements). When we no longer require your Personal Information, we will securely destroy and/or delete it from our systems as far as is reasonably and technically possible.

We have put in place procedures to manage any suspected data security breach and will notify you, and any applicable regulator, where we are legally required to do so.

In some circumstances we may anonymise your Personal Information so that it can no longer be associated with you, in which case we may use such Information without further notice to you.

## **9. Your rights and contacting us**

You have the following rights which can be exercised by contacting our Data Protection Officer using the details provided above.

The right:

- to access personal information held about you and to obtain a copy of it;
- to prevent any processing of a record of Personal Information that is causing or is likely to cause unwarranted and substantial damage or distress to you or another individual;
- to obtain the rectification or completion of records of Personal Information which are inaccurate or incomplete;
- to restrict or object to the processing of your Personal Information and to request its erasure under certain circumstances. We will not be able to erase Personal Information where we have a legal obligation to retain such data for example the results of identity verification checks;
- in certain circumstances, to receive your Personal Information, which you have provided to us, in a structured, commonly-used and machine readable format and the right to transmit that data to another data controller without hindrance, or to have that Personal Information transmitted to another data controller, where technically feasible; and
- to lodge a complaint with the Information Commissioner about the way in which your Personal Information is being used or shared: <https://ico.org.uk>.

Please note some of these rights are qualified and may not always be applicable.

You will not have to pay a fee to access your Personal Information or to exercise any of the other rights, however, we may charge a reasonable fee if your request for access is clearly unfounded or excessive, in particular, in relation to repetitive requests. Alternatively, we may refuse to comply with the request in such circumstances.

We may ask you to specify your request for information to help us confirm your identity and ensure your right to access the Information or to exercise any of your other rights. This is another appropriate security measure to ensure that Personal Information is not disclosed to any person who has no right to receive it.

It is important that the Personal Information we hold about you is accurate and current. Please keep us informed if your Personal Information changes: [CustomerServiceTDNV@td.com](mailto:CustomerServiceTDNV@td.com)

## 10. Privacy Breaches

If you are aware of, or are the victim of, a suspected privacy breach in connection with the information that we hold about you, you should immediately contact the DPO (please refer to section 1 above for contact details). All suspected privacy breaches are appropriately investigated and applicable corrective action is taken.

In addition, as set out above, you have the right to make a complaint at any time to the data protection regulator, as listed above, if you believe there has been any breach of data protection law in relation to your information.

## 11. Changes to this Privacy Notice

We reserve the right to update this Privacy Notice at any time, and we will notify you, via our Privacy Notice webpage, when we make any substantial updates.

If you have any questions about this Privacy Notice, please contact the DPO (please refer to section 1 above for contact details).