TD Bank

Privacy Notice

May 2019

Contents

1. Introduction

The Privacy Notice applies to all persons with whom we have, wish to have, or used to have a direct or indirect relationship whose data is protected by TD Bank N.V. This includes the following legal entities:

- TD Bank N.V; and
- Elements of the TD Bank Group which process European personal information. The Group is headed by The Toronto- Dominion Bank, headquartered in Toronto, Canada.

In this Policy, the words "you" and "your" mean any data subject or individual customer. Any reference to "we", "us", "our" or "they" includes each of the entities listed above.

We have always regarded the need for the protection, privacy and confidentiality of the personal information (as defined in section 2 below) of our customers as an important and fundamental operating requirement. This Privacy Notice provides descriptions that support our obligations and your rights under the EU General Data Protection Regulation (the "GDPR") by explaining when and why we collect your personal information, how we use it, 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:

TD Bank N.V.
Data Protection Officer
60 Threadneedle
Street London
EC2R 8AP
United Kingdom
PrivacyEuropeandAsiaPacific@td.com

You have the right to make a complaint at any time if you feel the processing of your personal information infringes the GDPR. Please see section 3 below for the relevant regulators.

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 organization).

Examples of the categories of Personal Information we may process 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 give us by filling in forms or by communicating with us, whether face-to-face, by phone, email, online, or otherwise;
- information about you and your opinions expressed when participating in market research;
- your account information (for example account numbers, transaction history, passwords, and other (authentication) information relating to your use of our electronic networks, including our Secure Customer Portal and our TD Bank App); 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 collection, recording, organization, 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. Data Controllers

This Privacy Notice applies to the processing carried out by us:

- Regulated by the Dutch Data Protection Authority ('Autoriteit Persoonsgegevens'):

  TD Bank N.V.
  World Trade Centre, Tower A, 11th Floor
  Strawinskylaan 1103
  1077 XX Amsterdam
  Netherlands
  +31 20 301 84 10

We are a **data controller** in respect to the relationship between ourselves and you, as an individual whose Information we are processing. This means that we are responsible for deciding how we hold and use your Personal Information.

As data controller, we are accountable and have an obligation to ensure that we process your Personal Information in compliance with the GDPR. 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 without adequate protection.

Your relationship with us includes your application for financial services provided by us and the creation, administration and termination of the terms and conditions of these services. It includes the administration of legislative programs such as fulfilling regulatory requirements, tax and other statutory regulations.

4. How will we collect and what will be our legal ground for using your Personal Information?

During your relationship with us, we will collect and process your Personal Information as outlined in this Privacy Notice. We collect your Personal Information in a number of different ways, including the following:

- if you provide it when communicating with us (for example when registering for our services);
- if you order any of our products or services;
- if you make payments or modify your account details; and
- when you visit our websites (for example by cookies, please refer to section 6 below).

We record all service calls for quality and training purposes and to enable us to deal effectively with queries and complaints, in order to comply with our regulatory obligations. The use of Personal Information will also be justified on the basis of one or more legal

"processing grounds" that are provided for in the GDPR. The table below contains an explanation of the scope of the various legal processing grounds available under the GDPR for processing of Personal Information on which we rely:

(a) Contract performance: where we require your Personal Information in order to enter into a contract with you and provide our services to you.

(b) Legitimate interests: where we use your Personal Information to achieve a legitimate interest and our reasons for using it outweigh any prejudice to your data protection rights.

(c) Our legal obligations and rights: 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.

(d) Consent: where you have consented to our use of your Personal Information (in which case you will have been presented with a consent form in relation to any such use and you may withdraw your consent at any time by the method explained in the communication with you or, and in any event, by giving notice to our DPO).

Under limited circumstances, we will also process criminal personal data. We will only process criminal personal data when the processing is authorized 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.

You will be the primary source for your Personal Information. It may also be necessary to collect information from third parties such as reference checks (for example identification verification and financial crime checks). In this Privacy Notice, we explain how we intend to use your Personal Information and the legal ground for processing. For each type of processing where we are relying on our legitimate interests, we list out such interests. For processing requiring your consent, we provide you with details of the Personal Information we would like and the reason for collecting it, so that you can carefully consider whether you wish to consent.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your Personal Information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact us at CustomerService@tdbanknv.com. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose, or purposes, you originally agreed to, unless we have another legitimate basis for doing so in law.

We may process 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 the Information and collection is required to investigate a breach of the Guidelines of Conduct or contravention of European 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 the Information could be useful when investigating a contravention of a European 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:

- **To provide the financial products or services that you have requested:** the assessment and approval of you, the execution of agreements with you, the processing of your financial transactions including transfers and to liaise with appropriate third-party suppliers. The lawful bases are the preparation of and actual contract performance of our contract with you; legitimate interests to enable us to provide our services and sharing personal data between our branches and legal entities, where appropriate; and the preparation of and actual contract performance of our contracts with those appropriate third-party suppliers.
- **Secure Customer Portal, TD Bank App and 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 unauthorized 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.
- **Risk management:** preparing quotations and assess relevant risks for us and for you. We need your personal data for acceptance procedures, to prepare quotations and for risk-assessment of your and our risks. The lawful bases for using your information for this purpose are the preparation of and actual contract performance of our contract with you and our legitimate interests to help manage our and your risks.
- **To prevent and detect crime including, e.g. fraud, terrorist financing and money laundering:** conducting certain checks on you, such as know your customer (KYC) checks, anti-money laundering (AML) checks, and anti-fraud checks before we establish a relationship, and where required, during our relationship with you; complying with laws applicable to us as a financial institution (for instance by processing phone recordings or 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.
- **Banking operations support:** for undertaking business management and planning (including change of our business structure), 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 us to change our business structure. For criminal personal data, please refer to paragraph 4 above.
- **Marketing:** keeping our existing clients informed of our services and products. The lawful basis for this is our legitimate interests to enable us to promote our financial services and products. We may need your consent to communicate by certain channels and we'll make sure that we ask for this where we need to. You can change your mind on how to receive marketing messages or choose to stop receiving them at any time. To make that change, contact us in the usual way (as also indicated on each marketing communication).
- **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 purposes which justify our use of your Personal Information.

We will only use your Personal Information for the 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 notify you and explain the legal basis which allows us to do so.

Please note that we may process your Personal Information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. Cookies

A 'cookie' is a small text file containing information which is stored on your computer. Cookies are used for technical reasons and/or to facilitate your use of a website. A common type of cookie is the "session cookie". When you visit a website, session cookies are sent between your computer and the server to collect information. Session cookies are not saved once you close your web browser. For more information about how cookies work, please be referred to www.allaboutcookies.org.

We don't use permanent cookies on our website https://tdbanknv.com/ or the secure portal. The types of cookies that we use are saved during your session on our website or secure portal and are as follows:

- Consent (onetime session cookie) – This functional cookie is used on our website or secure portal to show you a cookie notification to accept or decline the use of cookies.
- Session cookie – This essential cookie refers to the piece of data that is used on our website or secure portal to identify a session:
- Anti-request forgery token of .Net (session cookie) – This essential cookie is used on our website or secure portal as an anti-forgery token that in turn is used to prevent a cross-site request forgery (CSRF) attack. It prevents anybody from forging a link between our site and your computer which could be subsequently activated by a powered user; and
- Time-out Cookie (TrxStsTrack or session cookie) – This essential cookie is used on our secure portal to show when a session is about to expire or has expired.

The cookies we use don't share or transmit information to any third parties.

If you do not wish to accept cookies you can change your web browser's settings to automatically deny the storage of cookies or to inform you when a website wants to store cookies on your computer. Previously stored cookies can also be deleted through the web browser (for more on this see below). Please note that certain areas and functions on this website require cookies and may not function if cookies are deleted or declined.

If you wish to remove the cookies that are already on your equipment, and you are using a PC and a newer browser, whilst in your browser you can press CTRL + SHIFT + DELETE simultaneously to access your cookie settings. If this shortcut does not work, you can find the support pages for the most commonly used browsers as well as a link to delete flash-cookies here:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Flash cookies

7. Sharing your Personal Information

We may share your Personal Information within TD Bank Group (as many of our processes are centralized) 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 is collected and 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:
  - Correspondent banks and settlement systems providers and similar third parties, who provide our banking operations support;
  - Third parties supplying and supporting our Secure Customer Portal, TD Bank App and Website;
  - Financial service providers supporting our IT infrastructure;
  - 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;
  - Agencies for marketing purposes;
  - Third parties in connection with potential or actual corporate restructuring, merger, acquisition or takeover, including any transfer or potential transfer of any of our rights or duties under our agreement with you; and
  - 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.

We may transfer your data to countries outside the European Economic Area ("EEA"), for example, if any of our servers are located in a country outside of the EEA, such as the USA. These countries may not have similar data protection laws to Europe. As we operate in various jurisdictions, the EEA operations regularly share data with 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 are used to protect your Personal Information, such as the European Commission's Standard Contractual Clauses. The standard contractual clauses can be found via the following link: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

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, 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).

8. Automated Decision Making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

9. 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, 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.

In some circumstances we may anonymize 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.

It is important that the Personal Information we hold about you is accurate and current. Please keep us informed if your Personal Information changes during your relationship with us, whether by informing your relationship manager or other key contact here.

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.

10. Your rights and contacting us

You have the following rights (unless exemptions apply), which can be exercised by contacting our Data Protection Officer using the details provided below.

The right:

- to ask us not to process your Personal Information for marketing purposes;
- 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 about the way in which your Personal Information is being shared with a supervisory authority.

Where we rely on your consent to use your Personal Information, you have the right to withdraw that consent at any time.

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.

You may at any time request rectification or erasure of your Personal Information. However, please note that deletion could mean that we cannot process your requests or that your account with us will expire.

11. Privacy Breaches

If you are aware of, or are the victim of, a suspected privacy breach in connection to your relationship with us, 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 your applicable data protection regulator, as listed above, if you believe there has been any breach of data protection law.

12. Changes to this Privacy Notice

We reserve the right to update this Privacy Notice at any time, and we will notify you, whether directly or indirectly, for example via our privacy notice webpage or email signatures, when we make any substantial updates. We may also notify you in other ways about the processing of your Personal Information, for example, in writing, by email, by messaging through the Personal Archive or telephone.

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