

Privacy Notice

Effective: 24 April 2022

Navigating this Notice

If you are viewing this Notice online or on PDF, you can click on the below links to jump to the relevant section:

1. [Introduction & scope of this Privacy Notice](#)
2. [The Personal Data we collect and process](#)
3. [The purposes of processing](#) as well as the legal basis for processing
4. [How we collect and process your Personal Data](#)
5. [Sharing Your Personal Data](#)
6. [Transfer of Personal Data to third countries or international organisations](#)
7. [Your Rights as a Data Subject](#)
8. [Retention of Personal Data](#)
9. [Existence of automated decision-making](#)
10. [How we secure your information](#)
11. [Data Breaches](#)
12. [Changes to this Privacy Notice](#)
13. [Our details](#)

To access this notice online, please visit: <https://trustednovusbank.gi/privacy>

1. Introduction & scope of this Privacy Notice

- 1.1 Trusted Novus Bank (“TNB”, “we”, or “us”) is committed to protecting the privacy of our customers and stakeholders, and we take our data protection responsibilities with the utmost seriousness. For Trusted Novus Bank it is essential to protect any data you entrust us with and to ensure confidentiality of this data.
- 1.2 This Privacy Notice applies to all Personal Data processing activities carried out by TNB. We ensure compliance with the Data Protection Legislation, which requires us to provide you with certain information when Personal Data relating to you is either collected from you directly or from other sources. Moreover, we do not collect, use or process personal data without an appropriate legal basis, as required under the Data Protection Legislation.
- 1.3 The purpose of this privacy notice is to explain how we process your Personal Data in connection with our business (if you are a customer), or your use of our website (if you are a prospective customer, stakeholder or just browsing). We may supplement this notice with other privacy notices as appropriate; for example, if you attend one of our events or you are one of our employees.
- 1.4 To the extent that you are a customer or user of our services, this Privacy Notice applies together with any terms of business and other contractual documents, including but not limited to any agreements we may have with you.
- 1.5 If you are using our website, we have designed this so that you may navigate and use it without having to provide Personal Data, subject only to certain data that may be collected via the use of cookies. This notice should therefore be read together with our Cookie Policy, which provides further details on our use of cookies on this website. A link to our Cookie Policy can be found in the bottom of the page: www.trustednovusbank.gi

Some important terms used in this notice

- 1.6 TNB offers its services in or from within Gibraltar, which is no longer part of the EU. Gibraltar has its own data protection laws that apply certain EU laws. This is referred to as the “Data Protection Legislation”, and includes:
 - The Data Protection Act 2004 (as amended), and regulations made under that Act; and
 - The “Gibraltar GDPR”, which is essentially the EU’s General Data Protection Regulation or (Regulation (EU) 2016/679, or the “EU GDPR”) as it forms part of Gibraltar law. This basically means it is read slightly

differently to the EU GDPR but still offers privacy protections and guarantees in a similar manner. If you live or work outside of Gibraltar, other laws, including the EU GDPR, may be applicable to your individual circumstances

17. For the purposes of this Privacy Notice, **“Personal Data”** means any information relating to you as an identified or identifiable natural person (**“Data Subject”**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an online identifier or to one or more factors specific to your physical, physiological, genetic, mental, economic, cultural or social identity.
18. In this notice, **“processing”** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
19. TNB is a **“controller”** (sometimes referred to as **“data controller”**) when it determines the purposes and means of processing of your Personal Data. We may also act as **“processors”** (sometimes referred to as **“data processor”**) when we process your data, and may use other data processors who act on our instructions.

2. The Personal Data we collect and process

- 2.1 We collect and process various categories of Personal Data at the commencement of and for the duration of our relationship with you. The collection and processing of Personal Data is limited to that which is necessary to achieve one or more of the legitimate purposes identified in the notice.
- 2.2 Personal Data which we may collect and process may include:
 - (i) basic personal information, such as name and address, contact details, marital status, tax information, residency status and date of birth;
 - (ii) financial history and information, such as transactional and account information;
 - (iii) information regarding your financial circumstances, such as proof of income, sources of wealth, assets and liabilities, credit and borrowing history, details of expenditure and other outgoings;
 - (iv) information regarding your financial needs and requirements;
 - (v) information about the purposes and scope of your expected relationship with TNB;
 - (vi) basic information about your family, partners and dependants;
 - (vii) employment and education history;
 - (viii) personal identification documents, such as copies of passports, driving licences and/or identity cards;
 - (ix) other official documents allowing us to have independently verifiable information as to your source of funds/wealth, your residence and tax status (e.g. utility bills, tax filing information)
 - (x) CCTV images containing your Personal Data where you visit any of our premises (warning signage will be used to inform you at the time of collection).
 - (xi) Our interactions with you (for example by email, telephone, post, SMS or via our website), which may include basic personal information together with enquiries, reviews, follow-up comments or complaints lodged by or against you and disputes with you.
 - (xii) (Subject to our Cookie Policy referred to above) Online profile and social media information obtained as a result of use of TNB’s websites, platforms and applications, such as the browser types and versions used, the date and time of access to our website, platforms and applications, the Internet protocol address (“IP address”), the Internet service provider of the accessing system; and any other similar data and information that may be used in the event of attacks on our information technology systems.
 - (xiii) When we send marketing emails to you, we may use certain technologies (e.g. “web beacons”) to collect information about when you open the email, your IP address and browser or email client type, and other similar information. We do this as necessary for our legitimate interests in reviewing and considering our direct marketing activities. Further information on your rights in relation to direct marketing appears below.
- 2.3 Additionally, TNB may also collect and process certain special categories of Personal Data or Personal Data relating to criminal convictions and offences, which for convenience we refer to as “sensitive data”. Personal

Data that falls under these categories are those that reveal any of the following:

- (i) your racial or ethnic origin;
- (ii) your political opinions;
- (iii) your religious or philosophical beliefs;
- (iv) your trade union membership;
- (v) your genetic data or biometric data for the purpose of uniquely identifying you;
- (vi) your health;
- (vii) your sex life or sexual orientation;
- (viii) criminal convictions and offences (including the alleged commission of offences, proceedings in relation to such offences or alleged commission of offences or the disposal of such proceedings, including sentencing);

2.4. TNB will not necessarily process any sensitive data in relation to you, and the extent of processing will depend on your relationship with us. This data would only be collected and processed where TNB is lawfully permitted to do so (including where you manifestly make that data public) and only for limited purposes such as fraud prevention, prevention of money laundering, financial crime and terrorist financing, bribery and corruption. Where none of these limited purposes can be made out, but special category Personal Data is required to be processed by us (such as in connection with our services to you as our customer), we may need to rely on your explicit consent. This essentially means we will ask you to confirm in writing and after you are provided with full information so you can exercise a free and informed choice. Further information about providing and withdrawing your consent appears below under information regarding your right as a Data Subject.

3. The purposes of processing as well as the legal basis for processing

3.1. We will only use and share your information where it is necessary and lawful for us to do so. Where the Data Protection Legislation allows us, we will inform you, to the extent you do not already have this information, of the processing purposes as well as the legal basis for processing. We may also need to further process the Personal Data for a purpose other than that for which the Personal Data were collected

3.2. Any of the information we collect from you may be used for one or more of the following purposes:

- (i) To provide services to you;
- (ii) To manage your relationship with TNB and any transactions;
- (iii) To meet Compliance and or Regulatory obligations;
- (iv) To perform financial crime risk management, including reporting suspicious activity to relevant authorities;
- (v) To collect money, you owe us;
- (vi) To enforce/defend the rights of Trusted Novus Bank
- (vii) To meet our internal policy requirements;
- (viii) To market our services/products to you

3.3. As referred to above, we only process Personal Data, including any sensitive data, where we have a valid lawful basis to do so. Some of the more common lawful bases we rely on are as follows:

- (i) **Contractual necessity** – your Personal Data will be processed where it is necessary for performance of any contract with you for the provision of our services, or to take steps at you request prior to entering into such a contract. Our information gathering and applications forms will contain information about whether the provision of Personal Data is a statutory or contractual (or pre-contractual) requirement and of the possible consequences for not providing such Personal Data (e.g. we may not be able to provide our services to you);
- (ii) **Legal Obligation** – TNB may be required to collect and process certain Personal Data in order to comply with relevant legislation, which may extend beyond the Data Protection Legislation (e.g. Anti-Money Laundering obligations);
- (iii) **Legitimate interests of TNB** – we may collect and process your Personal Data where it is in our legitimate interests to do so and without prejudicing your interests or fundamental rights or freedoms. In this

particular case, we will provide you with further details of those legitimate interests (e.g. our marketing communications will include this information).

34. In rarer cases, we may rely on other lawful bases:

- (i) **Consent** – this may apply where no other lawful basis can be relied on (e.g. for the use of our website by persons who are not our customers, in respect of certain cookies that are not essential – see our Cookie Notice for further information)
- (ii) **Vital interests** – we may need to process Personal Data to protect your vital interests or those of another person (e.g. in life-threatening situations)
- (iii) When processing more “sensitive” types of Personal Data (as noted above at paragraph 2.3), we will rely on one of the above lawful bases together with additional safeguards and lawful bases required in respect of this data. We will inform you of these as appropriate.

4. How we collect and process your Personal Data

4.1. Other than information you provide to us directly when using our services and/or website, attending our offices or our events, or requesting information from us, information is also collected from other sources, which include:

- (i) Information we receive from third parties, either as arranged by you or otherwise when there is a lawful basis. This may include other entities affiliated with TNB or its subsidiary and related undertakings within any part of TNB’s corporate group, third party service providers, credit reference agencies and resources, government and quasi-government agencies, other banks and regulatory authorities, or Personal Data obtained from sources and records accessible to the general public. At the time of collection of this information we shall, to the extent allowed under Data Protection Legislation, provide you with information about the source of the Personal Data;
- (ii) Information acquired and generated by us during our relationship with you, such as the use of our services, accounts, payment services, enquiries, credit or payment cards, Netbank or other kinds of payment services. In such cases, TNB will obtain information from you, shops and merchants, financial institutions and others;
- (iii) Information collected through the use of TNB’s websites, platforms and applications;

4.2. Information is also collected via the recording of telephone conversations for training, monitoring or other legal/regulatory purposes. Financial services legislation under which we are regulated requires us to record certain telephone conversations and keep these records for minimum periods of 5-7 years. Further information is provided at the time of recording and also within relevant customer information as part of any relevant services where such call recording is required.

4.3. Information may also be collected directly from you or other third parties when you apply for a job at TNB, or if you are an existing employee. We will supplement this Privacy Notice with further privacy notices directed at our employees / prospective job applicants as appropriate.

5. Sharing Your Personal Data

5.1. In certain cases, we may access, preserve, and disclose to third parties’ information about you if we believe disclosure is in accordance with, or required by, any contractual relationship with you, applicable law, regulation or legal process. Personal Data may be processed by us internally (including within our corporate group) and/or shared with third parties for the purposes specified above, where you have consented to this, or if otherwise lawfully required.

5.2. Such third parties may include our affiliates, agents, vendors, consultants or suppliers, as well as any other third-party service providers who are performing certain services on our behalf (as data processors), such as external counsel, correspondent banks and other financial institutions, investment managers or other service providers.

5.3. Where lawfully required, we may disclose Personal Data to relevant regulatory, law enforcement and/or

other competent authorities. We may also need to share your information in order to enforce or apply our legal rights under any agreed terms of business, including establishing, exercising or defending legal claims, or in compliance with a legal, regulatory or other administrative/judicial process (such as a court order).

54. If TNB enters into a sale, reorganisation, transfer, asset disposal or joint venture with or is merged with another business entity, your Personal Data may be disclosed to our new business partners or purchasers. In such cases, we will take steps to ensure that your privacy rights continue to be protected.
55. TNB will not share your Personal Data with third parties for their own marketing purposes without your permission.

6. Transfer of Personal Data to third countries or international organisations

6.1 In connection with TNB's (i) IT development, hosting and support (ii) payment service provision to its customers; (iii) human resources/talent acquisition; and (iv) general compliance functions, Personal Data is transferred to data processors within and outside of the EEA (the EEA includes countries in the European Union as well as Iceland, Lichtenstein and Norway). Under Gibraltar GDPR, all transfers outside of Gibraltar are treated as transfers to a "third country" as that expression means a country or territory outside of Gibraltar. In cases where we intend to transfer personal data to third countries or international organisations outside of Gibraltar, we are required to confirm to you whether it has been determined by under Gibraltar GDPR that the country or organisation we are sharing your Personal data with will protect your information adequately. Specifically, we need to confirm the existence or absence of a decision based on an adequacy regulation as set out in Article 45(1) of the Gibraltar GDPR (known as a "adequacy regulations" made by the United Kingdom).

6.2 A transfer of Personal Data to a third country or an international organisation may take place if:

- (i) it is a transfer to the United Kingdom;
- (ii) it is a transfer based on adequacy regulations;
- (iii) we or our processors have provided "appropriate safeguards" (see paragraph 6.5 below);
- (iv) (where none of the above items (i) to (iii) apply) we rely on specific derogations provided for under the Data Protection Legislation (see paragraph 6.6 below).

6.3 We transfer Personal Data to the following countries/international organisations which are deemed adequate and subject to adequacy regulations for the purposes of Gibraltar GDPR and/or the Data Protection Legislation at the date of this Notice:

- (i) Denmark
- (ii) Ireland
- (iii) Israel
- (iv) Italy
- (v) Netherlands
- (vi) Spain
- (vii) Switzerland
- (viii) United Kingdom
- (ix) Israel

6.4 We also transfer Personal Data to the following countries/international organisations which are not deemed adequate at the date of this Notice:

- (i) India
- (ii) Vietnam
- (iii) United States of America

6.5 In the absence of an adequacy decision, we rely on "appropriate safeguards" as provided for in the Data Protection Legislation. In this regard, we use a number of legal mechanisms to ensure that your rights and protection level follow your data, including (a) standard data protection clauses specified in Gibraltar regulations, issued by the Information Commissioner, or approved by the EU Commission as standard contractual clauses and given effect under Gibraltar law; (b) approved codes of conduct; (c) certification mechanisms; or (d) binding corporate rules.

- 6.6. Certain third country transfers are exempted transfers, meaning that they are allowed under the specific derogations in the law and are used where “appropriate safeguards” above are not available. We may rely on these exemptions in order to transfer data to third countries:
- (i) with your explicit consent
 - (ii) where necessary for the performance of a contract, or for pre-contractual steps taken at your request;
 - (iii) where necessary for the conclusion of a contract between us and a third party which is in your interest;
 - (iv) where necessary for important reasons of public interest;
 - (v) where necessary for the establishment, exercise or defence of legal claims; or
 - (vi) where necessary to protect your vital interests (or those of another), if you are physically or legally incapable of giving consent
- 6.7. As a measure of last resort, we may also make a third country transfer where we cannot rely on any of the above reasons, but only if the transfer fulfils the following criteria:
- (i) the transfer must not be repetitive;
 - (ii) the transfer must concern only a limited number of data subjects;
 - (iii) the transfer must be necessary for compelling legitimate interests we pursue which are not overridden by your interests and freedoms (as well as those of affected data subjects);
 - (iv) we must have assessed all the circumstances and provided suitable safeguards (e.g. encryption measures) to protect the Personal Data;
 - (v) we inform the relevant supervisory authority of the transfer; and
 - (vi) we provide you with (i) confirmation of the transfer, (ii) the information in this Privacy Notice, and (iii) the compelling legitimate interests we seek to rely on.
- 6.8. You may request further information on appropriate or suitable safeguards we rely on using the details contained in this Notice.

7. Yours Rights as a Data Subject

- 7.1. Under the Data Protection Legislation, we are required to inform you about the existence of the right to request from TNB access to and rectification or erasure of Personal Data or restriction of processing concerning you as a Data Subject, as well as your rights to object to processing, your right to data portability, and your right to lodge a complaint with a supervisory authority.
- 7.2. We have provided all this information in the Schedule to this Notice below for your ease of reference, as well as other privacy rights available to you.
- 7.3. If you wish to exercise any of these rights, please contact our data protection officer (“DPO”) or (in the DPO’s absence) the Data Protection Steering Group directly (see ‘Our details’ below at paragraph 13). We may need to request specific information from you to help us understand the nature of your request, to confirm your identity and to ensure that Personal Data is not disclosed to any person who has no right to receive it. Requests will be processed within one month of receipt, but this might be extended by two further months in case of a complex request, where you have made a number of requests, or if the identity of the requestor cannot be verified.
- 7.4. You will not ordinarily 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 one or more of your requests for access/other rights are clearly unfounded or excessive, in particular because any repetitive character in such requests. Alternatively, we may refuse to comply with such requests in such circumstances. Please also note that there are certain exemptions or derogations from, and restrictions and adaptations of the application of, rules of the Data Protection Legislation. These exemptions may impact on your rights, and restrict them entirely or partially in certain cases. The rights themselves are also qualified and may not always apply.
- 7.5. Depending on your particular circumstances, you may also have additional rights if you live or work outside of Gibraltar. For example, the EU GDPR may apply to you if you are based in the EEA, and also depending on whether we are seen to be offering goods or services or monitoring the behaviour of persons in the EEA. You can find out more about the EU GDPR and your rights (if any) by accessing the European Commission’s

website: <https://ec.europa.eu>.

8. Retention of Personal Data

- 8.1. We retain your information only for as long as is necessary for the purposes for which we process the information as set out in this notice. Records can be held on a variety of media (physical or electronic) and formats.
- 8.2. Retention periods are determined based on the type of record, the nature of the record and activity and the legal or regulatory requirements that apply to those records. TNB will, in the normal course of events, keep client records for up to 10 years after the termination of the relationship.
- 8.3. However, we may retain your Personal Data for a longer period of time where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.
- 8.4. 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. Existence of automated decision-making

We do not use automatic decision-making or profiling when processing Personal Data. Were we to decide to do so, we would confirm this to you and provide meaningful information about the logic involved, as well as the significance and the envisaged consequences for you.

10. How we secure your information

- 10.1. We are committed to taking appropriate measures designed to keep your Personal Data secure. Our technical, administrative and physical procedures are designed to protect Personal Data and non-personal data from loss, theft, misuse and accidental, unlawful or unauthorised access, disclosure, alteration, use and destruction. We follow generally accepted standards to protect the Personal Data submitted to us, both during transmission and once it is received.
- 10.2. To prevent unauthorised access, we follow strict security procedures in the storage and disclosure of information, which you have given us. Our security procedures mean that we may request proof of identity before we are able to disclose Personal Data to you following a request from you for us to do so. We implement security measures across TNB to ensure our clients' data is protected within secured and encrypted servers we control. We may also keep hard copy records of this Personal Data in physical storage facilities with access restricted solely to our personnel. We also take steps to monitor access to and modification of your information by our contractors, advisers, consultants and staff members, and ensure that they are aware of and properly trained in their obligations for managing your privacy.
- 10.3. We update and test our security technology on an ongoing basis. We restrict access to your Personal Data to those employees who need to know that information to provide benefits or services to you. In addition, we train our employees about the importance of confidentiality and maintaining the privacy and security of your information. We commit to taking appropriate disciplinary measures to enforce our employees' privacy responsibilities.
- 10.4. Our website does not collect your personal information and you may browse anonymously. More information is found in our Cookie Policy in the bottom of the page at www.trustednovusbank.gi

11. Data Breaches

A loss of Personal Data is known as a data breach. The GDPR imposes requirements on businesses to identify, assess and report breaches in a timely manner (within 72 hours). We undertake to inform you if your Personal Data is compromised and there is a high risk to your rights and freedoms as a result.

12. Changes to this Privacy Notice

We may update this notice from time to time by publishing a new version on our website and will also update the “Last updated” field at the top of this notice. If you do not have a business relationship with us, you are encouraged to review our website regularly in order to remain informed about how we process Personal Data. If you have a business relationship with us, we reserve the right to inform you of changes to this notice from time to time either through our website or via other means of communication.

13. Our details

Trusted Novus Bank Limited is a company incorporated in Gibraltar with registered number 3936 and registered office situated at 76 Main Street, Gibraltar. We are also regulated by the Gibraltar Financial Services Commission and further details appear in our general Terms and Conditions. If there are any questions regarding this notice, you wish to exercise any of the rights described in this notice, or if you are concerned about the way we have handled your Personal Data you may contact our DPO or (in the DPO's absence) the Data Protection Steering Group using the details below:

Data Protection Officer / Data Protection Steering Group

Trusted Novus Bank

76 Main Street

GX11 1AA

Gibraltar

Telephone: +350 2000 3000

Website: www.trustednovusbank.gi

Email: DPOmailbox@trustednovusbank.gi / dataprotection@trustednovusbank.com

SCHEDULE – INFORMATION ABOUT YOUR RIGHTS AS A DATA SUBJECT

As outlined in our Privacy Notice, you have the following rights under the Data Protection Legislation, which can be exercised by contacting our Data Protection Officer (contact details below under 'Our details'):

The right to confirmation and access

You have the right to ask us to confirm to you whether or not we collect, process or store your Personal Data. Where we collect process or store your Personal Data, you are entitled to access to your Personal Data and you further have the right to be informed about:

- the purposes of the processing;
- the categories of Personal Data concerned;
- the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from us rectification or erasure of Personal Data, or restriction of processing of Personal Data concerning you as a Data Subject, or to object to such processing
- the existence of the right to lodge a complaint with a supervisory authority;
- where the Personal Data is not collected from you, any available information as to its source;
- the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for you; and
- whether your Personal Data is transferred to a third country and if so of the appropriate safeguards relating to the transfer

Note that most of this information is already contained within our Privacy Notice. Exercising this right is also referred to as submitting a "data subject access request" or "DSAR".

The right to information

You have a right to be informed about the processing of your Personal Data (and if you did not give it to us, information as to the source) and this Notice intends to provide the required information. Note that your right to information is limited in certain cases, and the requirements to give information do not apply insofar as:

- The provision of information to you proves impossible or would require disproportionate effort on our part in order to provide. This is provided that we take appropriate steps as controller to protect your rights as a Data Subject, your freedoms and your legitimate interests, including by making information publicly available (as this Notice intends to do)
- obtaining information or disclosure is expressly laid down by Gibraltar law which we are subject and which provides appropriate measures to protect your legitimate interests;
- the personal data must remain confidential subject to an obligation of professional secrecy regulated by Gibraltar law (such as statutory obligations of secrecy); or
- you already have the information.

The right to rectification

You have the right to have any inaccurate Personal Data about you rectified and to have any incomplete Personal Data about you completed. You may also request that we restrict the processing of that data until rectified. If you ask TNB to restrict processing your Personal Data or parts thereof, TNB may have to suspend the operation of your accounts, products or services that are provided to you. It is important that the Personal Data we hold about you is accurate and current. Any terms of business which we may have with you will also require you to inform us if your Personal Data changes during your relationship with us. If we do hold Personal Data and you believe it is incorrect, you may submit a request to us to correct any alleged mistakes. We shall communicate any rectification of Personal Data to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort, and shall inform you about such recipients if you request this information.

The right to erasure (right to be 'forgotten')

You have the general right to request the erasure of your Personal Data. This right can be exercised if one of

the following applies:

- the Personal Data is no longer necessary for the purpose it was collected it for;
- you withdraw your consent to consent based processing and no other legal justification for processing applies;
- you object to processing for direct marketing purposes;
- we unlawfully processed your Personal Data; and/or
- erasure is required to comply with a legal obligation that applies to us;

Once you have requested erasure of your Personal Data for one of the reasons above, we will proceed to comply without delay unless continued retention is necessary for:

- exercising the right of freedom of expression and information;
- complying with a legal obligation under EU or other applicable law;
- the performance of a task carried out in the public interest;
- archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, under certain circumstances; and/or
- the establishment, exercise, or defence of legal claims.

We shall communicate erasure of Personal Data to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort, and shall inform you about such recipients if you request this information.

The right to restrict processing

You have the right to restrict the processing of your Personal Data under certain circumstances. You may restrict the processing of your Personal Data when:

- you contest the accuracy of the Personal Data;
- processing is unlawful you may request, but you do not want us to erase it;
- we no longer need to process your Personal Data but you need the Personal Data for the establishment, exercise, or defence of legal claims; and/or
- you object to processing that relies on the public interest or on our legitimate interests as the lawful processing grounds, and in this case, we must restrict the challenged processing activity pending the verification of whether our legitimate interests override your interests.

We shall communicate restriction of processing of Personal Data to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort, and shall inform you about such recipients if you request this information

The right to data portability

You have a right to receive the Personal Data concerning you (which you have provided to us) in a structured, commonly used and machine-readable format, or ask us to send it to another person where this is technologically possible. This right only applies where:

- processing is based either (i) on your consent or (ii) on a contract we have with you (or steps taken at your request prior to entering into a contract); **and**
- processing is carried out by automated means (i.e. excluding paper files). Processing by automated means is understood as general electronic processing, and is to be distinguished from automated decision-making (explained below).

This right does not include any additional data that created by us based on the data you have provided. For example, if we use the Personal Data you have provided to create a user profile, then this Personal Data would not be in scope of data portability (but could be in the scope of a *data subject access request* as explained above). Additionally, if we are not responsible for the privacy practices of others where you ask us to *port* your data to a third party.

The right to object to processing

You have the right to object to processing of your Personal Data under certain circumstances. These include:

- where we rely on legitimate interests as the lawful basis of processing of your Personal Data (including profiling based on such interests);
- where processing of your Personal Data is for scientific or historical research purposes or statistical

purposes on grounds relating to your particular situation. TNB does process Personal Data for such purposes;

- where a controller relies on the lawful basis that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. TNB does not rely on this lawful basis, which is usually restricted to public authorities; and/or
- where Personal Data are processed for direct marketing purposes, where this right to object is an *absolute* right (see below under *The right to freedom from direct marketing*)

Where you object on the above bases, we will cease to process your Personal Data unless we can demonstrate compelling legitimate interests for processing your Personal Data that override your interests or we need to process your Personal Data to establish, exercise, or defend legal claims.

The right to complain to a supervisory authority

If you consider that our processing of your Personal Data infringes data protection laws applicable to you, then you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. If you are outside of Gibraltar, you may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement. Before raising a complaint, you may wish to contact us using the ‘Our details’ section of our Privacy Notice so we can investigate the matter.

Alternatively, if we have not responded to you within a reasonable time or if you feel that your complaint has not been resolved to your satisfaction, you are entitled (regardless of where you are based) to make a complaint to the Information Commissioner under the Data Protection Act 2004, which is presently the Gibraltar Regulatory Authority (“GRA”). You may contact the GRA on the below details:

Address: Gibraltar Regulatory Authority, 2nd Floor, Eurotowers 4, 1 Europort Road, Gibraltar
Email: info@gra.gi
Phone: (+350) 200 74636
Fax: (+350) 200 72166
Website: www.gra.gi

In certain cases, you may also have the right under the EU GDPR to lodge a complaint with the supervisory authority in the country of your habitual residence, place of work, or the place where you allege an infringement of one or more of our rights has taken place, if that is based in the EEA

The right to withdraw consent

Where the legal basis for processing your Personal Data is your consent, you have the right to withdraw that consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Consent should be as easy to withdraw as it is to give, so we will normally provide toggle switches, tick boxes or forms that allow you to change your preference at any time online. However, if an online option is not available, or if you have submitted a paper form and no longer have a copy available, you can always enquire about and exercise your right to withdraw consent by contacting us using the information under ‘Our details’ in our Privacy Notice. Note that withholding or withdrawing consent may limit the scope of services we are able to provide, and we will inform you of the consequences of withholding or withdrawal at the relevant time

The right to freedom from direct marketing (opting-out)

You have an absolute, unqualified right to freedom from direct marketing also referred to as “opting out”. You can exercise the right at any time by contacting us, using the details in our Privacy Notice. If we send you any marketing emails, we will always provide an unsubscribe option to allow you to “opt-out” of any further marketing emails. If you opt-out of our marketing materials, you will be added to our suppression list to ensure we do not accidentally send you further marketing. Where you unsubscribe from any postal marketing, you may initially still receive some content which has already been printed or sent, but we will remove you from any future campaigns.

We may still need to contact you administrative or operational purposes, in order to deliver our services to you in compliance with relevant legislation (e.g. send you statements). However, we will make sure that those

communications don't include direct marketing.

The right to freedom from automated decision making (including profiling)

You have a right to request that decisions made about you using your personal information are made by humans, and not by automated means, such as by computers. As noted in our Privacy Notice, we do not use automated decision-making methods (including profiling) and whilst certain risk assessment systems may be *automated* there will be human intervention following such processing, unless we specifically notify you that this is not the case. This means decisions are not made by robots or computers, and therefore not 'automated'.

If any automated decision-making takes place in the future, you have the right in this case to express your point of view and to contest the decision, as well as request that decisions based on automated processing concerning you or significantly affecting you and based on your Personal Data are made by natural persons, not only by computers

Certain third parties (e.g. credit referencing agencies) may use automated decision-making tools or software. Even in such cases, we will continue to ensure our decisions affecting you are made by human beings. We are not responsible for the privacy practices of others and will take reasonable steps to bring such automated decision-making to your attention, but you are encouraged to become familiar with the privacy practices of any third parties you enter into any agreements with.

Note that this right does not apply when the decision:

- is necessary for entering into, or performance of, a contract between you and us;
- is required or authorised by law; or
- is based on your explicit consent