Triodos Bank.
UK Privacy Statement

The Triodos Bank UK (TBUK) Privacy Statement sets out your rights and the measures TBUK will take to protect your personal data. This includes how we will use your information, what rights you have, and how the law protects you as an individual. TBUK is *a Data Controller* as defined under data privacy legislation.

Triodos will review and amend this privacy statement from time to time. You can always find the most up to date version on our website www.triodos.co.uk. Any terms with a specific definition used in this statement, are highlighted in *italics* and are explained in the Glossary section.

What is *personal data*?

Personal data means any information relating to an individual who can be directly or indirectly identified by reference to the information. Individuals are referred to as *Data Subjects* under data privacy legislation. A wide range of information constitutes personal data including names, contact information, identification numbers such as National Insurance numbers, and online identifiers often referred to as *'cookies'* for example. This applies to both digital and paper-based information included within filing systems, or which is intended to be placed within a filing system.

What does processing mean?

The processing of personal data means any interaction with the information including viewing, collecting, sharing, storing, transferring or analysing it for instance. This can be by both a Data Controller, or a *Data Processor*.

Who holds your personal data?

Your personal data will be held by Triodos Bank N.V in The Netherlands and by TBUK. You can find information on how to contact us as well as further information on what Triodos does, on our website. TBUK has appointed a *Data Privacy Officer* (DPO) and any data privacy queries which cannot be resolved through the information provided on our website can be directed to them using the contact details included on our website.

The use of your personal data is covered by Triodos Bank's registration with the UK *Information Commissioner's Office;* registration number Z6794013.

Why is your personal data required?

When you apply for a product or service with Triodos you will need to provide certain personal data to enable us to process your application, and to then provide the product or service you want on an on-going basis. For example, your name, contact details such as your email address and phone number(s), addresses, or your National Insurance number. Triodos may also hold personal data about you throughout our relationship with you; the transactions you make using your current account or how you use our website for instance.

How will Triodos use your personal data?

The *General Data Protection Regulation (GDPR)* legislation which applies across Europe only allows the processing of personal data if one or more conditions are met; this is known as a *lawful basis for processing.* There are six lawful bases provided under GDPR, which are included in the Glossary section. Triodos will only process your personal data for the reasons it was provided for, and only where there is a lawful basis for processing allowing this.

What we use your personal data for?	Why do we need to use your personal data and which lawful basis for processing is applicable?	What are our legitimate interests in using your personal data?
To manage our relationship with you and deliver our products and services	Fulfilling a contract we have agreed between us *(contract)* We are legally required to complete certain activities *(legal obligation)* Undertake activity for your and our legitimate interests *(legitimate interests)*	Keeping our records up to date Working out which of our products and services will be of interest to you Developing our products and services based on your use of them and any feedback Informing you of relevant products and services that may be of interest to you
To detect, investigate, report and try to prevent financial crime	We are legally required to complete certain activities *(legal obligation)* Fulfilling a contract we have agreed between us *(contract)* Undertake activity for your and our legitimate interests *(legitimate interests)*	Complying with our legal requirements Reviewing and improving how we deal with financial crime
To run our business properly and efficiently	We are legally required to complete certain activities *(legal obligation)* We have a legal duty to provide you with a fair and easy to understand service *(legal obligation)* Undertake activity for your and our legitimate interests *(legitimate interests)*	Complying with regulations that apply to us (such as those set by *The Financial Conduct Authority* – FCA or *The Information Commissioner's Office* - ICO for instance) Being as efficient as we can and providing you with information you need

What personal data will Triodos use?

We use different types of personal data and have grouped them into the following categories:

Category of personal data	Description
Contact information	How to contact you including where you live, your telephone number and you email address (where relevant).
Personal details	Personal information such as your gender, date of birth, or occupation.
Special categories of personal data	GDPR categorises certain sensitive personal information as 'special category' personal data; this includes information about your health, political opinions, or sexual orientation for instance. Triodos will not collect and use these types of data, unless there is a legal obligation to do so, or it is required to provide (or continue to provide) a product or service to you in accordance with legal or regulatory requirements.
National Identification numbers	A number or code given to you by a government authority to identify who you are, such as your UK National Insurance number.
Financial information	Financial information such as your bank account number and transaction history.
Contractual information	Details about the products or services we provide you.
Administrative information	Registration numbers and administrative reports.
Transactional information	How you use our products such as your bank account for example, how and where your debit card is used or what you use our Internet Banking services to do for instance. This information is used to help protect you from fraud and comply with our legal and regulatory obligations.
Socio-demographic data	What you do for a living, what communication channels you prefer to use; this information is used to help us ensure you receive the right information at the right time, using the right method of communication.

Where will your personal data be obtained from?

Triodos collects personal data that you provide when interacting with us, from companies we use to complete financial transactions, and if you have given us consent to do so through agreeing with our cookie statement on our website, registration of your online activities. Personal data that we have collected from you will include data you have provided when you:

- Apply for our products or services;
- Talk to us on the phone or in person;
- Use our websites or mobile device applications;
- Subscribe to a newsletter or other marketing messages;
- Send us e-mails or letters; or
- Take part in financial reviews, interviews, customer surveys, competitions or promotional activities.

We may also obtain your personal data from other companies we deal with if there is a lawful basis to do so, in which case you will be notified of how and why we will use them. This could include the following:

- Companies that introduce you to us;
- Card providers and associations such as Mastercard for example;
- Credit Reference Agencies such as *Experian;*
- Financial advisers or representatives;
- Insurers;
- Fraud prevention agencies such as CIFAS *(Credit Industry Fraud Avoidance System);*
- Public information sources;
- Agents working on our behalf;
- Market researchers;
- Medical practitioners; and
- Government and law enforcement agencies.

Cookies

After you have given us consent we collect data from your personal electronic devices to register your online and mobile activities. We monitor data sessions to register your visits and use cookies to enable required functionality, increase the quality of our website or mobile services, optimise your personal experience and support promotional and direct marketing activities. You can read more about how we use cookies in the cookie statement included on our website.

Who do we share your personal data with?

How will personal data be shared?

Triodos will only share your data if there is a lawful basis to do so. We will treat all your personal data as private and confidential and in accordance with data privacy legislation (even when you are no longer a customer). Information we hold about you will not be disclosed to anyone unless:

- we are legally required to disclose the information. This includes sharing your information with tax authorities and law enforcement agencies such as HMRC or the police for example;
- we need to disclose the information for the purposes of or in connection with any legal proceedings, or for the purposes of obtaining legal advice, or the disclosure is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- disclosure is required to protect our legitimate interests, or someone else's legitimate interests (for example, to prevent fraud);
- the disclosure is made with your consent; and
- disclosure is to a third party for the purposes of providing administrative or processing services on behalf of Triodos. If this is required, we will ensure that the third party protects your personal data in the same way that we do.

Why is your personal data shared?

We may need to share your personal data with other organisations to provide you with the product or service you have chosen. For example:

- Credit reference agencies, such as Experian;
- Agents who collect money from persons in debt;
- Government authorities who are entitled to request your data;
- Fraud prevention agencies and legal authorities;
- Companies you ask us to share your data with;
- If you have a debit card with us, we will share transaction details with companies which help us to provide this service such as Mastercard;
- If you use direct debits, we will share your data with the *Direct Debit scheme;* and
- If you have a loan with us, we may share information with other lenders who also hold a charge on the security.

A record of any fraud or money laundering risk will be retained by fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, please contact us.

If false or inaccurate information is provided and fraud is identified, then details will be passed to fraud prevention agencies:

- Law enforcement agencies may access and use this information;
- We and other organisations may also access and use information to prevent fraud and money laundering for example, when:
  - Checking details on applications for credit and credit related or other facilities;
  - Managing credit and credit related accounts or facilities; or
  - Recovering debt.

We and other organisations may access and use the information recorded by fraud prevention agencies, including in other countries. Please contact us if you want to receive details of the relevant fraud prevention agencies.

The use of your personal data by *third parties*

When a third party processes your personal data on our behalf, we ensure that they follow our instructions to process and protect your personal data. Third parties are required to sign agreements in which they commit themselves to safeguard your personal data, agree to only use the data to provide services to us specifically outlined in the agreement, and follow our instructions.

Your personal data will be shared with the following categories of third parties for the purposes described:

Category of third parties	Data type	Purposes
Administrative services	Contact information, personal details, financial/ contractual/transactional information	To provide you with the product or service you applied for
Market research and marketing communications companies	Contact information, socio-demographic information, personal details, financial information	To ensure that you receive the right marketing communication messages from us, at the right time and in areas that you are interested in.

Category of third parties	Data type	Purposes
Credit Reference Agencies	Contact information, personal details, financial/ contractual/transactional information	To help us make decisions and assess risk when considering your application for our products or services
Fraud Prevention Systems	Contact information, personal details, financial/ contractual/transactional information	To help protect you from fraud
Governmental departments	Any information requested, once legal authority has been verified.	To fulfil our legal and regulatory obligations

Does Triodos share your data outside of the European Economic Area?

Triodos' default position is that we will not disclose or transfer personal data to organisations outside of the *European Economic Area* ('EEA'). However, where this is required we will inform you and confirm why we need to do this. When we do transfer personal data outside of the EEA, we will make sure that it is protected at the same level as within the EEA by using one of these safeguards:

- Transfer data to organisations in non-EEA countries (or states or provinces of these countries) with privacy laws in place providing the same level of data privacy protection as within the EEA;
- Transfer data to organisations that are part of *Privacy Shield* which is an international framework that sets privacy standards at a similar level as those of the EEA; or
- Put a contract in place with the recipient ensuring that they will process the data with the same level of data protection as within the EEA.

How we use your information to make automated decisions

We use external providers and Triodos systems to help us make some decisions about you or your business. This helps us to make sure our decisions are quick, fair, efficient and correct, and are based on up to date information. These decisions can affect the products, services or features we may offer you now or in the future. In case a decision produces legal effects such as changing a contract we offer you (or similarly affects you), you have the right not to be subject to a decision based solely on automated processing. We use your data to support decision-making in the following ways:

Opening an account

When you open an account with us, we check that the product or service is relevant for you, based on the data you have provided, and any reference information held by external providers. We check that you or your business meet our requirements to open an account. This may include verifying your identity and personal details such as your age, residency status, nationality and credit history.

Approving credit

When you apply for credit we make a risk assessment to decide whether to lend you money. This risk assessment is based on the information included in your application, credit reference information we obtain externally and our analysis to help understand your financial situation. When approving credit, we ensure that decisions are never solely based on automated systems and that there is always a person involved to help make a sound, fair and unbiased decision.

Credit Reference Agencies

When you apply for a product or service we are required to perform checks on the data you have provided about you and/or your business. We also check your credit history if you have applied for a product which includes credit facilities. Triodos shares the personal data you provide during your application with Credit Reference Agencies that help us with these checks. The data we exchange with the Credit Reference Agencies includes:

- Contact information and personal details;
- Credit application;
- Details of any shared credit;
- Financial situation and history; and
- Information made available to the public e.g. electoral or commercial registers.
- Assess what marketing communication messages we send you

We'll use this data to:

- Assess whether you or your business can afford repayments;
- Make sure that what you've told us is true and correct;
- Help detect and prevent fraud and money laundering;
- Manage accounts with us; and
- Trace and recover debts.

We share your data with Credit Reference Agencies for as long as you remain a customer. This will include details about any repaid or outstanding debts. It will also include details of funds going into the account, and the account balance. If you borrow money from us, it will also include details of your repayments and whether you repay in full and on time.

When Credit Reference Agencies receive a search request from us they will place a search footprint on your credit file that may be seen by other lenders.

The identities of the Credit Reference Agency used by Triodos, and the ways in which they use and share personal data, are explained in more detail at www.experian.co.uk/crain

Tailoring products and services

We monitor financial activities to study and learn about our customers' behaviour and needs, and to make decisions based on what we learn to improve our service quality and products. We put customers with similar activities into groups called *customer segments.* The use of customer segments helps us to design products and services that better suit our customers' needs, and market them appropriately and effectively to customers who are likely to be interested in them.

Protecting you from fraud

We monitor your personal or business account to identify whether you may have been a victim of fraud. If we identify that there is a risk of fraud, we may stop financial transactions and temporarily block access to your account while this is investigated. You will be contacted and kept up to date during this process.

Fraud Prevention Agencies (FPAs)

Fraud Prevention Agencies (FPA's) and law enforcement agencies can legally access your personal data. In cooperation with these agencies, we use your personal data to confirm your identity before we provide products or services to you or your business. When Triodos and fraud prevention agencies process your personal data, processing is undertaken on the basis that there is a legitimate interest in preventing fraud and money laundering, and to verify your identity. This is to protect our business and to comply with laws that apply to us as a Bank.

Once you have become a customer, we share your personal data with these agencies to help detect, investigate, prevent and prosecute financial crime. These agencies may keep your personal data for up to 10 years depending on their findings and (inter-) national legal requirements. Law enforcement agencies may keep files of criminal offences for up to 20 years.

If Triodos, or a fraud prevention agency, determine that you pose a fraud or money laundering risk we may refuse to provide the products or services you have requested, or we may stop providing existing products and/ or services to you.

If you choose not to provide your personal data

We may need to collect personal data by law such as your identity documents, or under the terms and conditions of a contract we have with you. If you choose not to provide us with, or choose to restrict the processing of, the information we need it may prevent us from meeting our contractual obligations and providing you with the product you have applied for. This situation could result in the cancellation of a product or service you have with us or the termination of our contract with you. We will discuss this with you at the time before making any changes to your products or services.

Where personal data has been collected using your consent as the lawful basis for processing, you are free to withdraw your consent at any time and without any contractual or service delivery consequences other than the services you choose not to make use of.

Marketing communications

From time to time we will send you information about our products and services and the projects we lend to. We are careful not to send you information, or additional information about our services, where you do not want it. You can choose what information you want to receive when you apply for or open a product or service with us and you can change your communication preferences in Internet Banking or through the Triodos Crowdfunding website if you have registered, or by contacting us. You will also be provided with an opportunity to stop receiving information from us through an 'unsubscribe' link in any emails we may send you.

If you are not yet a customer of Triodos and want to receive marketing communications from us, you can request this through our website or by calling our contact team. You will be asked to provide us with your contact details and to give your consent for Triodos to use your personal data. You may withdraw your consent and unsubscribe from the marketing communications whenever you want. We will not give your personal data to anyone else for marketing purposes (other than those described above in 'The use of your personal data by third parties') without informing you and obtaining your consent.

Personal data used for marketing purposes consists of the personal data we have received from you, and data we have collected when you use our products or services. We only use your personal data to send you marketing communications if we have either a legitimate interest or your consent. A legitimate interest in a

marketing context means that we will only send you marketing communications in relation to products or services that may be of interest to you based on what we already know about you. Our legitimate interests will always be balanced with your interests, and you can ask us at any time to stop sending you marketing communications.

How long does Triodos keep your personal data for?

As long as you are a customer of Triodos we will process your personal data to provide you with the products and services you have asked us to provide. After you end your contract with Triodos we may retain some or all of your personal data for up to 12 years (depending on the products or services you took out) for one or more of these reasons:

- To respond to any questions or complaints;
- To show that we treated you fairly; or
- To meet our ongoing legal and regulatory requirements.

We may keep your personal data for longer than 12 years if we cannot delete it for legal, regulatory or technical reasons. Personal data will be retained with the utmost care and security measures will be applied to ensure your privacy and security are maintained.

What are your rights?

GDPR entitles you to several rights in relation to your personal data:

The right to be informed

Individuals or data subjects as they are referred to under data privacy legislation, have the right to be informed about the collection, use and sharing of their personal data. Organisations must provide individuals with certain information at the time personal data is collected. This Privacy Statement provides you with the information you are entitled to and we are required to give you.

The right to access your data

You have the right to access your data to establish what it is being used for and verify the lawfulness of any processing. Before providing access to your personal data we will ask you to verify your identity to protect you from identity theft and financial crime. We may also need to ask you some questions to ensure we have understood your request correctly. You can request access to your personal data through our website.

The right to rectification (correcting mistakes and inaccuracies)

It is important that any personal data we use is accurate, up to date, and relevant. To ensure that your data is correct you have the right to access, correct and/or update your personal data at any time. If you think your data is incorrect or incomplete and you wish to correct your data or privacy settings, please contact us.

The right to erasure (the deletion of your personal data)

You have right to request that we delete your personal data if:

a. your personal data is no longer needed in relation to the purposes for which was collected;

b. you withdraw your consent and there are no other legal bases to process your personal data;

c. you object to us processing your personal data for direct marketing purposes;

d. you object to us processing your personal data for the legitimate interests of Triodos;

e. you feel that your personal data is not being processed lawfully; and

f. your personal data needs to be deleted to comply with legal requirements.

As a financial services provider operating in the UK, Triodos needs to keep your personal data for a certain period of time to provide you with our financial products and services, and to remain compliant with legal and regulatory requirements.

The right to restrict processing

You have the right to request the restriction of the processing of your personal data for a limited period and under certain circumstances. For example, this could apply if you feel that your personal data held by Triodos is inaccurate, has not been processed lawfully, or is no longer needed for the purposes it was originally collected for. Triodos has the right to store your personal data while your query is investigated.

The right to data portability

You have the right to receive your personal data in a structured, commonly used and machine-readable format. We are looking at the best way to achieve this for our customers and will provide more information when it is available.

The right to object to processing

You have the right to object to the processing of your personal data based on legitimate interests, direct marketing, and processing for historical research and statistical purposes. If you decide to exercise this right,

please contact us and we will consider your request; Triodos is legally allowed to continue to process your data if one of the following can be demonstrated:

a. compelling legitimate grounds for the processing, which override your interests, rights and freedoms; or

b. processing is required for the establishment, exercise or defence of legal claims.

Rights related to automated decision making, including profiling

Triodos does not undertake any processing which includes decisions made by solely automated means, including profiling.

How to Complain

Please contact us in the first instance if you have any concerns with how we have processed your personal data. Details on how to do this are included in our website. You also have the right to lodge a complaint directly with the ICO; please visit their website (https://ico.org.uk/for-the-public/) for further details on how to do this.

If you choose, you can also lodge a complaint with the Dutch Data Protection Supervisory Authority (Autoriteit Persoonsgegevens); they are the *lead supervisor* for data privacy for Triodos. Please visit their website (https://autoriteitpersoonsgegevens.nl/en) for further details.

Glossary

Term	Definition
CIFAS - Credit Industry Fraud Avoidance System	A UK, not-for-profit fraud prevention service run on a membership association basis. CIFAS hold and exchange information both on known criminals, as well as innocent victims of fraud to help prevent further fraudulent activity.
Cookies	A message given to an Internet Browser by a Server, which is stored in a text file; the message is then sent back to the Server each time the Browser requests a webpage to be opened. Cookies are used to identify users of webpages and to customise content where applicable.
Customer segments	Customer segmentation is the process of dividing customers into groups based on common characteristics, so organisations can market to each group effectively and appropriately.
Data Controller	An individual or organisation which determines why personal data needs to be processed, and the manner it is processed in.
Data Privacy Officer	A position within an organisation responsible for ensuring that personal data is processed in accordance with UK data privacy requirements.
Data Processor	An individual or organisation which processes personal data on behalf of a data controller, in accordance with instructions from the data controller.
Data Subject	An individual who can be identified from the personal data i.e. the person the data is about.
Direct Debit Scheme	A UK payment mechanism run by Bank Account Clearing System Payment Schemes Limited enabling electronic payments to be made once authorisation has been provided by the originator.
European Economic Area (EEA)	The European area which provides for the free movement of persons, goods, services and capital; it is made up of EU members plus other countries within Europe which have agreements in place with the EU.
Experian	An independent UK organisation which helps other organisations identify and assess information about prospective customers. Experian holds both publicly available information from sources such as the Electoral Roll, as well as information provided by other organisations such as credit card providers and Banks who provide loans for example.
Financial Conduct Authority	A UK regulatory body operating independently of the UK Government, which oversees the regulation of conduct by financial services firms operating in the UK.
GDPR - General Data Protection Regulation	The legal framework that sets the guidelines and requirements for the collection, processing and storage of personal data of identifiable individuals within the European Union (EU). The GDPR legislation was adopted in April 2016 and comes into force across the EU on 25 May 2018.
Information Commissioner's Office (ICO)	The independent UK authority set up to uphold data privacy rights in the public interest.

Term	Definition
Lawful basis for processing	One of six allowable lawful bases for processing must be satisfied for Triodos to process your personal data. The six lawful bases are: 1. Consent - the individual has given clear consent 2. Contract - processing is necessary for a contract to be provided 3. Legal obligation - processing is necessary to comply with the law 4. Protect life - processing is necessary to protect someone's life 5. Public interest - processing is necessary to perform a task in the public interest 6. Legitimate interest - processing is necessary for Triodos' legitimate interests, or the legitimate interests of a third party, unless there is a good reason to protect the individual's data which overrides these legitimate interests.
Lead Supervisor	Triodos operates across Europe in the UK, France, Belgium, Germany, Spain and The Netherlands. The Group headquarters are in The Netherlands, which means that the main data privacy supervisory body is the Dutch Data Protection Supervisory Authority. TBUK also follows UK data privacy requirements set by the UK government and the ICO.
Legitimate interests	The business reason for Triodos to use your information. It must not conflict unfairly with your rights and interests. GDPR specifically mentions several examples of legitimate interests such as the prevention of fraud, marketing customers could reasonably expect to receive, or IT security for instance.
Personal Data	Any information relating to an identified or identifiable natural person (an individual).
Privacy Shield	A framework for transatlantic exchanges of personal data between the European Union (EU) and the United States of America (USA). It was designed to provide organisations on both sides with a mechanism compliant with data privacy requirements when transferring personal data from the EU to the USA.
Special Categories of Personal Data	Personal data which relates to particular characteristics including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health or medical information, sexual life or orientation. Additional protection is required for personal data falling into this category, and both a general and specific lawful basis for processing are required. This means that one of the six general GDPR lawful bases for processing is needed, as well as one of the following which relate specifically to special categories of personal data: 1. explicit consent 2. processing is necessary for meeting obligations under employment, social security and social protection law 3. processing is necessary to protect the vital interests of someone who is unable to provide consent 4. processing is carried out during legitimate activity by a Foundation, Association or other not-for-profit body with a political, philosophical, religious, or trade union-based aim and processing relates to current or former members of that organisation, and that personal data is not disclosed outside of that organisation 5. processing relates to personal data which has been disclosed by the individual 6. processing is necessary in connection with legal claims 7. processing is necessary for substantial public interest 8. processing is necessary for preventative or occupational health 9. processing is necessary for public interest in the area of public health 10. processing is necessary for archiving purposes in the public interest such as scientific, historic or statistical research
Third parties	Organisations external to Triodos who undertake services and activity on our request such as our business partners, suppliers and affiliates.

Freephone: 0330 355 0355
contact@triodos.co.uk
www.triodos.co.uk

Calls to and from Triodos Bank may be recorded for training and monitoring purposes.

Triodos Bank

TB/UKPRIV/MAY18