Privacy and Cookies Policy

Date: 19 March 2026

Version: v3.1

1 Important information and who we are

1.1 Purpose of this privacy policy

This privacy policy aims to give you information on how Yonder collects and processes your personal data through your use of our website(s) and/or our mobile application(s), including any data you may provide through our website(s) and/or our mobile application(s) or otherwise through communicating with us (together our “Services”)

Our Services are not intended for children and we do not knowingly collect data relating to children.

It is important that you read this privacy policy together with any other privacy policy or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy policy supplements other notices and privacy policies and is not intended to override them.

1.2 Controller

The controller responsible for your personal data is Yonder Technology Netherlands BV if you reside in the European Economic Area (“EEA”), or Yonder Technology Ltd if you reside in the UK or anywhere else outside the EEA, (in either case the relevant Yonder entity is referred to as "Yonder Technology", "Yonder", "we", "us" or "our" in this privacy policy).

Yonder Technology Ltd is a company registered in England and Wales. Its company registration number is 12739942 and its registered office is at Shoreditch Exchange Senna Building, Gorsuch Pl, London, England, E2 8JF. It is registered with the Information Commissioner’s Office and our ICO registration number is ZA930713.

Yonder Technology Netherlands B.V. is a company registered in the Netherlands. Its Chamber of Commerce (KvK) number is 98050702 and its registered address is Herengracht 450, 1017 CA Amsterdam.

If you reside in the UK and have a Yonder Account:
Our partner Transact Payments Limited (“TPL”), is the issuer of your payment card and is an independent data controller for the personal data which you provide to us in relation to processing undertaken to enable you to use the card. TPL is an e-money institution, authorised and regulated by the Gibraltar Financial Services Commission. TPL’s registered office address is 6.20 World Trade Center, 6 Bayside Road, Gibraltar, GX11 1AA and its registered company number is 108217. When you apply for a Yonder Account in the UK, you agree to TPL’s Privacy Policy which is provided to you when you sign up. It is also available within the Yonder mobile application and at the bottom of this document. We encourage you to read the TPL Privacy Policy.

If you reside in the Netherlands and have a Yonder Account:
Our partner Transact Payments Malta Limited (“TPML”) is the issuer of your account and card, and is an independent Data Controller for the personal data which you provide to us. TPML is an e-money institution, authorised and regulated by the Malta Financial Services Authority. TPML’s registered office address is Vault 14, Level 2, Valletta Waterfront, Floriana, FRN 1914, Malta and its registered company number is C 91879. When you apply for a Yonder Account in the Netherlands, you agree to TPML’s Privacy Policy which is provided to you when you sign up. It is also available within the Yonder mobile application at the bottom of this document. We encourage you to read the TPML Privacy Policy.

1.3 Contact details

If you have any questions about this privacy policy or our privacy practices, please contact us by email on help@yonder.com

2 Why we collect data

We need to collect certain types of information to allow us to make a decision on your request for financial products, provide our products and services to you and to provide you with relevant product and service benefits. We also need to comply with legal and regulatory requirements relating to anti-fraud, anti-money laundering, know your customer and responsible lending obligations.

We will only collect the information we need to be able to provide you with the service you have requested. You need to make sure that the information you provide is accurate, complete and not misleading. Your personal information may need to be disclosed or shared with third parties when we are obliged to by law, for purposes such as national security, taxation, defence of a legal claim or criminal investigations.

3 The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data from which personal identification has been rendered impossible (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

1. **"Identity Data"** includes first name, middle name, last name, date of birth, username or similar identifier, title, nationality, passport, driver's licence, selfie and/or video (if requested), visa type and expiry date, marital status, number of dependents, employment status, occupation, employment industry, residential status, and residential address (current or prior);
2. **"Contact Data"** includes billing address, email address and telephone numbers;
3. **"Financial Data"** includes account number, sort code and bank name for direct debit purposes or "know your customer" or anti-money laundering purposes
4. **"Transaction Data"** includes details about payments to and from you, other details of products and services you have purchased from us and day of month to take payments;
5. **"Credit Risk and Affordability Data"** includes information about you that we receive from you or third parties such as credit reference agencies including information about your credit card, bank and savings accounts, spending habits, regular payments or repayment plans, monthly earnings before and after tax, monthly rent or mortgage payments and other financial data that, with your permission, we receive from your credit card providers, banks or building societies;
6. **"Vulnerability Data"** based on aspects of the data mentioned above, and further information provided by you (for example, regarding financial difficulty, health condition or additional assistance required), information from which we may determine you are a vulnerable customer;
7. **"Technical Data"** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, device type, your device

interaction patterns, and other technology on the devices you use to access our Services;

8. **"Profile Data"** includes your username and password, credit made to you, desired credit amount and duration, borrowing purpose, your interests, preferences, feedback and survey responses;
9. **"Usage Data"** includes information about how you use our Services and behavioural usage data such as interactions with our website, movement patterns; and
10. **"Marketing and Communications Data"** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share **"Aggregated Data"** such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

We may from time to time need to process **"Special Categories of Personal Data"** about you. This may include, for example, details about your mental or physical health when we collect certain Vulnerability Data about you (as defined above). Where we process Special Category Data about you, we will do so only if we have an appropriate lawful basis (including where we are under a regulatory obligation to do so) and in accordance with this privacy policy.

3.1 If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with products or services). In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

3.2 Changes to your personal data

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

4 How is your personal data collected?

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your Identity, Contact, Vulnerability and Financial Data by filling in forms or by corresponding with us by app, phone, email or otherwise. This includes personal data you provide when you:

1. create an account on our mobile application;
2. enquire about our products;
3. request marketing to be sent to you; and/or
4. give us feedback or contact us.

We may also request a scan of identity and other financial documents (e.g bank statements or employment contracts) if this is required for “know your customer” or anti-money laundering purposes.

Automated technologies or interactions. As you interact with our Services, we will automatically collect Usage and Technical Data about your equipment, browsing actions and patterns, including how you interact with your device. We collect this personal data by using cookies, server logs, visit statistics such as Google Analytics, artificial intelligence tools, and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our Cookie Policy for further details. We may also record within the browser information necessary for the functioning of our Services, for example whether cookie consent has been agreed to or progress through online forms.

Third parties. We also collect personal information received from other sources such as comparison sites, data from credit reference agencies, open banking data (including name, address, bank account number, sort codes, balance, overdraft limit and statement information) and results of “politically exposed persons” or sanction checks.

5 How we use personal data

We will only use your personal data if we have a legal basis for doing so. Most commonly, we will use your personal data in the following circumstances:

1. where we need to perform the contract we are about to enter into or have entered into with you;
2. where it is necessary for our legitimate interests (or those of a third party), and your interests and fundamental rights do not override those interests; and/or
3. where we need to comply with a legal obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data although, where we are required to do so by law, we will get your consent before sending direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

5.1 Purposes for which we will use your personal data

We have set out below, in a table format, a description of the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of Data	Lawful Basis for Processing (Including Basis of Legitimate Interest)
To register you as a new customer	(a) Identity (b) Contact (c) Credit Risk and Affordability (d) Profile	Performance of a contract with you
To enable you to access and use our Services, and allow us to supply our services to you	Any and all personal data mentioned above as needed.	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to provide a service to you)

To provide you with information and materials that you request from us	(a) Identity (b) Contact (c) Transaction (d) Usage	Necessary for our legitimate interests (to respond to your queries and provide any information and materials requested, to generate and develop business)
To carry out 'know your customer', anti-money laundering, compliance (including sanctions and 'politically exposed persons') and other background checks as needed and, where necessary, share this with other financial institutions and regulatory bodies to comply with relevant laws.	(a) Identity (b) Contact (c) Financial (d) Credit Risk and Affordability (e) Profile	Necessary to comply with a legal obligation. Otherwise, such processing is necessary for the performance of our contract with you.
To facilitate our customer referral or any similar benefit programmes	(a) Identity (b) Contact (c) Technical (d) Usage	Necessary for our legitimate interests (to generate and develop business)
To create and maintain a trusted and safe environment on the Services by: (a) detecting and preventing fraud and other harmful activity (b) conducting investigations and risk assessments (c) verifying any identifications provided by you (d) conducting checks against databases and information sources for	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Technical (f) Profile (g) Usage	(a) Necessary to comply with a legal obligation (b) Necessary for our legitimate interests (to carry out checks to ensure prevention against fraud and other harmful activity and ensure our Services are safe and secure)

fraud detection and prevention, risk assessment and harm prevention purposes (e) analysing interactions with our Services to assess legitimacy, identify deviations from normal human activity, and detect suspicious patterns that indicate fraudulent intent.		
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey (c) Dealing with your requests, complaints and queries	(a) Identity (b) Contact (c) Transaction (d) Usage (e) Profile (f) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated, manage our relationship with you, and to study how customers use our products/services)
To identify and provide the necessary support to our customers who are in, or may be going into, financial difficulty or other vulnerable circumstances.	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Credit Risk and Affordability (f) Profile (g) Vulnerability	Necessary to comply with a legal obligation. To the extent we need to process Special Category Data (for example, information pertaining to health), we will do so as necessary for reasons of substantial public interests, in particular to comply with our legal and regulatory obligations, provide confidential counselling, advice or support and/or protect the economic well-being of individuals.

To administer and protect our business, and our Services (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, mobile application, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our services updated and relevant, to develop our business and to inform our marketing strategy)
Use of cookies or similar tracking technologies for data analytics to improve our website and email marketing (to the extent this processes your personal data)	(a) Technical (b) Usage	Your consent (for more information, please see our Cookie Policy)

To make suggestions and recommendations to you about products or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications	Necessary for our legitimate interests (to develop our products/services and grow our business)
To provide card benefits to you	(a) Identity (b) Contact (c) Transaction (d) Usage (e) Profile (f) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to ensure our card benefits provide value for customers)
Compliance with any legal and / or regulatory requirements. To exercise or protect the rights, property, or personal safety of Yonder, its customers, staff or others, including to recover monies owed to us.	Any and all personal data mentioned above as needed.	Necessary for compliance with a legal obligation. Otherwise, as necessary to pursue our legitimate interests in protecting the rights, property, or personal safety of Yonder, its customers, staff or others (including for the purpose of establishing, exercising or defending our legal rights).

5.2 Fraud prevention

As part of our financial services products, we may use your information in order to be able to:

1. search your record with credit reference and fraud prevention agencies to check and verify your identity (and the identity of any other individual named on your application) and collect your credit report (and that of any other individual named on your application). Credit reference agencies will keep a record of our enquiries, which may also be used by other organisations with access granted by the credit reference agencies. This may affect your ability

to get credit. Please see sections 7 and 8 for further details about how your personal data may be used by credit reference and fraud prevention agencies; and

2. undertake appropriate checks to prevent or detect crime, money-laundering and or fraud, including with the use of artificial intelligence or similar technologies.

5.3 Automated decision-making

We sometimes use algorithms to make decisions on our behalf. This is referred to as automated decision-making. We have provided further detail regarding the means and purposes of automated decision-making below.

5.3.1 How the automated processes make decisions

We use automated decision-making for the following purposes, which are necessary for the performance of the contract between us, and also to comply with our legal and regulatory requirements:

- **To verify you and assess your application for an account**. Our algorithms verify your identity and assess your suitability for an account with us based on information such as your age, residency, nationality, financial position and other circumstances, such as the results of anti-money laundering and sanctions checks. This means that we may automatically decide that you present a fraud or money-laundering risk or pose a risk to us in terms of breaking financial sanctions, in which case we will reject your application for an account.
- **To determine creditworthiness and affordability**. This is based on the information we collect regarding your income, spending and credit history. We may also use open banking data, collected and provided to us by third parties. We use this to decide how easily you will be able to manage repaying credit and the interest rate we may charge you. We may compare you with other people in a set (for example, people who are in a certain age bracket may be more likely to be able to manage credit).
- **To decide whether we need to help you**. If our algorithms detect that you may have become financially vulnerable, we may have a regulatory obligation to help you. Such decisions may be based on your repayment history and

adverse changes to your credit score, together with additional information you have provided to us.

- **To detect and prevent fraud**. Our algorithms may freeze a transaction or account if we suspect fraud or money-laundering against Yonder or our customers. Such decisions are based on patterns in our data, such as a Yonder service being used in a way that fraudsters work.

Personal data derived from the above will be used to obtain information about you from, and carry out checks with credit reference agencies (for further details, please see the section below regarding credit reference and fraud prevention agencies).

If you do not pass all of our checks then your credit card application will either be refused or will be referred for further checks and additional consideration by us.

5.3.2 Your rights relating to automated decision-making

You have the right to request that we review or reconsider any decision that we make about your application which is based solely on automated processes. If you wish to exercise this right, please contact us as above.

5.4 Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased products from us and you have not opted out of receiving that marketing.

5.5 Opting out

You can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product purchase, product/service experience or other transactions.

5.6 Cookies

For information about the cookies we use, please see our Cookie Policy.

6 Disclosures of your personal data

We may share your personal data with the parties set out below for the purposes set out in the table above.

1. Credit Reference Agencies ("**CRAs**") and Fraud Prevention Agencies ("**FPAs**").
2. Firms and businesses that help us provide you with the right product and services. Service providers and business partners who we engage, or are potentially looking to engage, to assist with the operation of our business including banking partners, advertising and marketing partners, communications tools, IT support providers, customer support providers, verification providers, customer relationship management tools, storage, production and hosting providers, providers of card benefits, and payment processors.
3. Potential and/or actual customers as part of a referral programme in which you are involved.
4. Professional advisers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
5. Regulators and other authorities (including tax authorities) who require reporting of processing activities in certain circumstances.
6. Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy policy.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law.

7 How do credit reference and fraud prevention agencies use your data?

When you apply to us for membership, we will check the following records about you:

1. any records we may already have about you;
2. those held by CRAs; and

3. those held by FPAs.

CRAs supply us with public information (including from the electoral register, court judgments and bankruptcies registers) and shared credit and fraud prevention information, including information about previous applications and the conduct of accounts in your and your financial associate(s)' name(s).

You should be aware, when CRAs receive a search from us they will place a soft search footprint on your credit file, which is not visible to other lenders. This will occur during your initial eligibility check. If you agree to apply after the eligibility check, a hard search will be recorded with the CRAs, which may be seen by other lenders. If you agree to the credit terms we offer, we will continue to exchange information about you with CRAs, whilst you have a relationship with us.

We will send the information that you submit through our Services to CRAs. This information will be recorded by them. We and other organisations may access and use this information to prevent fraud and money laundering and CRAs and FPAs may use your information for statistical analysis. Information held by CRAs and FPAs will be disclosed to us and to other organisations in order to (for example):

1. prevent fraud and money laundering and to check and assess applications for credit, credit related facilities or other facilities;
2. recover debts that you owe and trace your whereabouts;
3. manage credit accounts and other facilities and decide appropriate credit limits;
4. verify your identity;
5. make decisions on credit and other facilities for you or your business;
6. check details on proposals and claims for all types of insurance; and
7. check details of job applicants and employees.

When you borrow from us, we will give details of your credit card and how you manage it to the CRAs. If you borrow and do not repay in full and on time, the CRAs will record the outstanding debt and, in some cases, the length of time that the debt remains outstanding. Other organisations may see these updates, and this may affect your ability to obtain credit in the future.

If you fall behind with your payments and a full payment or satisfactory proposal is not received within the date specified in your Notice of Default, then your account will be closed and a default registered on your Credit File with CRA's.

This information may be supplied to other organisations by CRAs and FPAs to perform similar checks and to trace your whereabouts and recover debts that you owe.

If you give us false or inaccurate information and we have reasonable grounds to suspect fraud or we identify fraud we may record this and may also pass this information to FPAs and other organisations involved in crime and fraud prevention including law enforcement agencies who may then access this information.

If you have any further questions about our use of CRAs (or would like to receive details of these agencies) please email us using the contact details provided above in this Privacy Policy.

In the UK, Equifax, Experian and TransUnion, the ICO and the major financial services trade associations have developed a common statement, Credit Reference Agency Information Notice (CRAIN). This defines the standards that all three Credit Reference Agencies will apply across all products and services in relation to processing consumer data. These can be found at www.experian.co.uk/crain, www.transunion.co.uk/crain, and www.equifax.co.uk/crain.

8 How do we work with fraud prevention agencies?

We undertake checks for the purposes of preventing fraud and money laundering, and to verify your identity before we make a decision about your application. We also monitor your account usage. These checks require us to process personal information about you.

We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

We process your personal data on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the services or financing you have requested.

Fraud prevention agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.

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

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you.

If you reside in the UK, further details of how your information will be used by us and these fraud prevention agencies, and your data protection rights, can be found by www.cifas.org.uk/fpn

9 International transfers

Personal data is stored on secure servers hosted in the UK. We may, however, transfer your personal data to third parties in countries outside either the UK or the European Union (EU), whose data protection and privacy laws are less strict than in the UK or the EU.

Where we do so, we will make sure suitable safeguards are in place to protect your personal data, in line with applicable data protection law. The safeguards may include relying on adequacy decisions (made by the EU and/or UK as applicable) where relevant or entering into the appropriate standard contractual clauses.

10 Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality where appropriate.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

11 Data retention

11.1 How long will you use my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax,

accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

By law we have to keep information about our customers for six years in the UK, and seven years in the Netherlands, after they cease being customers for regulatory and tax purposes.

In some circumstances you can ask us to delete your data: see your legal rights below for further information.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

12 Your legal rights

Under certain circumstances, you have rights under applicable data protection laws in relation to your personal data. You have the right to:

"**Request access**" to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it;

"**Request correction**" of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us;

"**Request erasure**" of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of

erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request;

"**Object to processing**" of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms;

"**Request restriction of processing**" of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

1. if you want us to establish the data's accuracy;
2. where our use of the data is unlawful but you do not want us to erase it;
3. where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
4. you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it;

"**Request the transfer**" of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to information which you initially provided consent for us to use or where we used the information to perform a contract with you; and

"**Withdraw consent at any time**" where we are relying on consent to process your personal data. 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.

If you wish to exercise any of the rights set out above, please contact us as above.

12.1 No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded,

repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

12.2 What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

12.3 Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

13 Complaints

If you reside in the UK, you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

If you reside in the Netherlands, you have the right to make a complaint at any time to the Autoriteit Persoonsgegevens (AP), the Dutch supervisory authority for data protection issues (www.autoriteitpersoonsgegevens.nl). We would, however, appreciate the chance to deal with your concerns before you approach the AP so please contact us in the first instance.

14 Changes to this privacy policy

We keep our privacy policy under regular review. This version was last updated on [x] March 2026.

TPL’s Privacy Policy

This applies to you if you reside in the UK and have a Yonder Account.

1 Purpose

This policy explains when and why we collect personal information about you, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

TPL is committed to safeguarding the privacy of your information. By “your data”, "your personal data”, and “your information” we mean any personal data about you which you or third parties provide to us.

We may change this Policy from time to time so please check this page regularly to ensure that you’re happy with any changes.

2 Who are we?

Transact Payments Limited (“TPL”, “we”, “our” or “us”) is the issuer of your card and is the Data Controller for the personal data which you provide to us in relation to the credit card only. TPL is an e-money institution, authorised and regulated by the Gibraltar Financial Services Commission. Our registered office address is 6.20 World Trade Center, 6 Bayside Road, Gibraltar, GX11 1AA and our registered company number is 108217.

Yonder Technology Ltd manages your card program and is the Data Controller for any personal data which you provide which is not related to the card. Yonder Technology Ltd is incorporated in England and Wales under company number 12739942 with its registered office at Shoreditch Exchange Senna Building, Gorsuch Pl, London, England, E2 8JF.

3 How do we collect your personal data?

We collect information from you when you apply online or via a mobile application for a payments card which is issued by us. We also collect information when you use your card to make transactions. We also obtain information from third parties (such as fraud prevention agencies) who may check your personal data against any information listed on an Electoral Register and/or other databases.

4 On what legal basis do we process your personal data?

Contract

Your provision of your personal data and our processing of that data is necessary for each of us to carry out our obligations under the contract (known as the Cardholder Agreement or Cardholder Terms & Conditions or similar) which we enter into when you sign up for our payment services. At times, the processing may be necessary so that we can take certain

steps, at your request, prior to entering into that contract, such as verifying your details or eligibility for the payment services. If you fail to provide the personal data which we request, we cannot enter into a contract to provide payment services to you or will take steps to terminate any contract which we have entered into with you.

Legal/Regulatory

We may also process your personal data to comply with our legal or regulatory obligations.

Legitimate Interests

We, or a third party, may have a legitimate interest to process your personal data, for example:

- To analyse and improve the security of our business;
- To anonymise personal data and subsequently use anonymised information.

5 What type of personal data is collected from you?

When you apply for a card, we, or our partners on our behalf, collect the following information from you: full name, physical address, email address, mobile phone number, phone number, date of birth, gender, login details, IP address, identity and address verification documents.

When you use your card to make transactions, we store that transactional and financial information. This includes the date, amount, currency, card number, card name, account balances and name of the merchant, creditor or supplier (for example a supermarket or retailer). We also collect information relating to the payments which are made to/from your account.

6 How is your personal data used?

We use your personal data to:

- maintain and administer your account, including processing your financial payments, processing the correspondence between us, monitoring your account for fraud, facilitating the provision of insurance and other services provided via Mastercard and providing a secure internet environment for the transmission of our services.
- comply with our regulatory requirements, including anti-money laundering obligations.

improve our services, including creating anonymous data from your personal data for analytical use, including for the purposes of training, testing and system development.

7 Who do we share your information with?

When we use third party service providers, we have a contract in place that requires them to keep your information secure and confidential.

We pass your information to the following categories of entity:

- companies and organisations that assist us in processing transactions you make (including but not limited to payment processing service providers) and in providing services that you have requested;
- companies and organisations that run and manage the card program;
- identity verification agencies to undertake required verification, regulatory and fraud prevention checks;
- information security services organisations, web application hosting providers, mail support providers, network backup service providers and software/platform developers;
- payment networks, payment service providers and mobile payments providers (i.e. Mastercard, Visa or any third parties involved in processing the financial transactions that you make);
- document destruction providers;
- anyone to whom we lawfully transfer or may transfer our rights and duties under this agreement;
- any third party as a result of any restructure, sale or acquisition of TPL or any associated entity, provided that any recipient uses your information for the same purposes as it was originally supplied to us and/or used by us; and/or
- regulatory and law enforcement authorities, whether they are outside or inside of the EEA, where the law requires us to do so.

8 Sending personal data outside of the EEA

To deliver services to you, it is sometimes necessary for us to share your personal information outside the European Economic Area (EEA), e.g.:

- with service providers located outside the EEA (such as Mastercard);
- if you are based outside the EEA;
- where there is an international dimension to the services we are providing to you.

These transfers are subject to special rules under European and Gibraltar data protection law.

These non-EEA countries do not have the same data protection laws as Gibraltar and EEA. We will, however, ensure the transfer complies with data protection law and all personal information will be secure. We will send your data to countries where the European Commission has made an adequacy decision, meaning that it has ruled that the legislative framework in the country provides an adequate level of data protection for your personal information. You can find out more about this here.

Where we send your data to a country where the European Commission has not made an adequacy decision, our standard practice is to use standard data protection contract clauses that have been approved by the European Commission. To obtain a copy of those clauses, please go to the European Commission's website. Mastercard uses Binding Corporate Rules which you can access at:
https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-bcrs.pdf

If you would like further information please contact our Data Protection Officer on the details below.

9 How long do we store your personal data?

We will store your information for a period of five years after our business relationship ends in order that we can comply with our obligations under applicable legislation such as anti-money laundering and anti-fraud regulations. If any changes to applicable legislation require us to retain your data for a longer period of time, we shall retain it for that period. We will not retain your data for longer than is necessary.

10 Your rights regarding your personal data?

You have certain rights regarding the personal data which we process:

- You may request a copy of some or all of it.
- You may ask us to rectify any data which we hold which you believe to be inaccurate.
- You may ask us to erase your personal data.
- You may ask us to restrict the processing of your personal data.
- You may object to the processing of your personal data.
- You may ask for the right to data portability.

- If you would like us to carry out any of the above, please email the Data Protection Officer at DPO@transactpay.com.

11 How is your information protected?

We implement security policies and technical measures in order to secure your personal data and take steps to protect it from unauthorised access, use or disclosure.

While we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk. Once we receive your information, we make our best effort to ensure its security on our systems. Where we have given (or where you have chosen) a password which enables you to access certain parts of our websites, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

12 Complaints

We hope that our Data Protection Officer can resolve any query or concern you may raise about our use of your personal information.

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in Gibraltar is the Gibraltar Regulatory Authority. Their contact details are as follows:

Gibraltar Regulatory Authority,

2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar.

(+350) 20074636/(+350) 20072166 info@gra.gi

13 Changes to our Privacy Policy

We keep our Privacy Policy under review and we regularly update it to keep up with business demands and privacy regulation. We will inform you about any such changes. This Privacy Policy was last updated on 25th May 2018.

14 How to contact us

If you have any questions about our Privacy Policy or the personal information which we hold about you or, please send an email to our Data Protection Officer at DPO@transactpay.com.

version: 1.0

TPML’s Privacy Policy

This applies to you if you reside in the Netherlands and have a Yonder Account.

This policy explains when and why we collect personal information about you, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

We are committed to safeguarding the privacy of your information. By “your data”, "your personal data”, and “your information” we mean any personal data about you which you or third parties provide to us.

We may change this policy from time to time so please check this page regularly to ensure that you’re happy with any changes.

Who are we?

Transact Payments Malta Limited (“TPML”, “we”, “our” or “us”) is the issuer of your account and card, and is an independent Data Controller for the personal data which you provide to us. TPML is an e-money institution, authorised and regulated by the Malta Financial Services Authority. Our registered office address is Vault 14, Level 2, Valletta Waterfront, Floriana, FRN 1914, Malta and our registered company number is C 91879.

Yonder Technology Ltd is the Program Manager for your account and card program and is an independent Data Controller for any personal data which you provide which is related to facilitating the management of the card program. Yonder Technology Ltd, incorporated and registered in England and Wales with company number 12739942 and registered office of Shoreditch Exchange Senna Building, Gorsuch Pl, London, England, E2 8JF.

How do we collect your personal data?

We collect information from you when you either apply online or via a mobile application for a payments card which is issued by us or a payments account is opened in your name. We also collect information when you use your card or account to make transactions. We may also process information from the Program Manager, other third-party payment partners and service providers. We also obtain information from third parties (such as fraud prevention agencies) who may check your personal data against any information listed on an Electoral Register and/or other databases. When we process your personal data we rely on legal bases in accordance with data protection law and this privacy policy. For more information see: ***On what legal basis do we process your personal data?***

On what legal basis do we process your personal data?

Contract
Your provision of your personal data and our processing of that data is necessary for each of us to carry out our obligations under the contract (known as the customer terms and conditions or similar) which we enter into when you use our payment services. At times, the processing may be necessary so that we can take certain steps, or at your request, prior to entering into that contract, such as verifying your details or eligibility for the payment services. If you fail to provide the personal data which we request, we cannot enter into a contract to provide payment services to you or will take steps to terminate any contract which we have entered into with you.

Legal/Regulatory
We may also process your personal data to comply with our legal or regulatory obligations.

Legitimate Interests
We, or a third party, may have a legitimate interest to process your personal data, for example:

- To analyse and improve the security of our business;
- To anonymise personal data and subsequently use anonymised information.

What type of personal data is collected from you?

When you either apply for a card or receive an account, we, or our partners or service providers, collect the following information from you: full name, physical address, email address, mobile phone number, phone number, date of birth, gender, login details, IP address, identity and address verification documents.

When you use your card or account to make transactions, we store that transactional and financial information. This includes the date, amount, currency, account balances and name of the merchant, creditor or supplier (for example a supermarket or retailer). We also collect information relating to the payments which are made to/from your account. If we are required by law to process additional personal data (for example, if we suspect that there may be fraud related to the use of your card or the payment services linked to it), we will also process that extra personal data.

How is your personal data used?
We use your personal data to:

- set up your account (including processing your application for a card and printing your card, if applicable), creating your account and verifying your identity;
- maintain and administer your account, including processing your financial payments, processing the correspondence between us, monitoring your account for fraud and providing a secure internet environment for the transmission of our services;
- comply with our regulatory requirements, including anti-money laundering obligations; and

- improve our services, including creating anonymous data from your personal data for analytical use, including for the purposes of training, testing and system development.

Who do we share your information with?

When we use third-party service partners, we have a contract in place that requires them to keep your information secure and confidential.

We may receive and pass your information to the following categories of entity:

- the program manager, co-brand provider of the website/app through which you access the account and/or card and the wallet platform provider which provides the infrastructure for the account provision;
- any banking partner which provides underlying banking services;
- identity verification agencies to undertake required verification, regulatory and fraud prevention checks;
- information security services organisations, web application hosting providers, mail support providers, network backup service providers and software/platform developers;
- document destruction providers;
- Mastercard, Visa, digital payment service partners or any third party providers involved in processing the financial transactions that you make;
- anyone to whom we lawfully transfer or may transfer our rights and duties under this agreement;
- any third party as a result of any restructure, sale or acquisition of TPML or any associated entity, provided that any recipient uses your information for the same purposes as it was originally supplied to us and/or used by us; and
- regulatory and law enforcement authorities, whether they are outside or inside of the European Economic Area (EEA), where the law requires us to do so.

Sending personal data overseas

To deliver services to you, it is sometimes necessary for us to share your personal information outside the European Economic Area (EEA) e.g.:

- with service providers located outside the EEA;
- if you are based outside the EEA;
- where there is an international dimension to the services we are providing to you.

These transfers are subject to special rules under European and Malta data protection law.

These non-EEA countries do not have the same data protection laws as Malta and the EEA. We will, however, ensure the transfer complies with data protection law and all personal information will be secure. We will send your data to countries where the European Commission has made an adequacy decision meaning that it has ruled that the legislative framework in the country provides an adequate level of data protection for your personal information. You can find out more about adequacy regulations here and here.

Where we send your data to a country where the European Commission has not made an adequacy decision, our standard practice is to use standard data protection contract clauses that have been approved by the European Commission. To obtain a copy of those clauses, please go to the European Commission's website.

If you would like further information, please contact our Data Protection Officer on the details below.

How long do we store your personal data?

We will store your information for a period of six years after our business relationship ends in order that we can comply with our obligations under applicable legislation such as anti-money laundering and anti-fraud regulations. If any applicable legislation or changes to this require us to retain your data for a longer or shorter period of time, we shall retain it for that period. We will not retain your data for longer than is necessary.

Your rights regarding your personal data?

You have certain rights regarding the personal data which we process:

- you may request a copy of some or all of it;
- you may ask us to rectify any data which we hold which you believe to be inaccurate;
- you may ask us to erase your personal data (where applicable);
- you may ask us to restrict the processing of your personal data;
- you may object to the processing of your personal data (where applicable); and
- you may ask for the right to data portability.

If you would like us to carry out any of the above, please email your request to the Data Protection Officer at DPO@transactpay.com.

How is your information protected?

We recognise the importance of protecting and managing your personal data. Any personal data we process will be treated with appropriate care and security.

These are some of the security measures we have in place:

- we use a variety of physical and technical measures to keep your personal data safe;
- we have detailed information and security policies to ensure the confidentiality, integrity, and availability of information;
- your data is stored securely on computer systems with control over access on a limited basis;
- our staff receives data protection and information security training on a regular basis;
- we use encryption to protect data at rest and anonymization where applicable;

- we have adequate security controls to protect our IT infrastructure and staff computers including but not limited to Identity and Access Management, Firewalls, VPN, Antivirus, Advanced Email Threat Protection and more; and
- we conduct regular audits such as PCI-DSS to ensure we are following adequate security controls to protect your data.

While we take all reasonable steps to ensure that your personal data will be kept secure from unauthorised access, we cannot guarantee it will be secure during transmission by you to the applicable mobile app, website or other services over the internet. However, once we receive your information, we make appropriate efforts to ensure its security on our systems.

Complaints
We hope that our Data Protection Officer can resolve any query or concern you may raise about our use of your personal information.
The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred.

The supervisory authority in Malta is the Office of the Information and Data Protection Commissioner. Their contact details are as follows:
IDPC,
Floor 2, Airways House, Triq il-Kbira, Tas-Sliema, SLM1549, Malta.
(+356) 23287100 / info@idpc.org.mt

Other websites
Our website may contain links to other websites. This privacy policy applies only to our website, so we encourage you to read the privacy statements on the other websites you visit. We cannot be responsible for the privacy policies and practices of other sites even if you access them using links from our website.

Changes to our Privacy Policy
We keep our privacy policy under review and we regularly update it to keep up with business demands and privacy regulation. We will inform you about any such changes. This privacy policy was last updated on 12th March 2026.

How to contact us
If you have any questions about our privacy policy or the personal information which we hold about you or, please send an email to our Data Protection Officer at DPO@transactpay.com.

Yonder's Cookie Policy

1 What are cookies

Cookies and other similar tracking technologies are small text files or code placed on your device (e.g. computer, smartphone or other electronic device) when you use our Services or view a message. Cookies allow a website or app to recognise a particular device.

2 Our use of cookies

We use cookies and other similar tracking technologies on our Services. These help us recognise you and your device and store some information about your preferences or past actions.

For example, we may monitor how many times you visit our Services, which pages you go to, traffic data, location data and the originating domain name of your internet service provider. This information helps us to build a profile of our users. Some of this data will be aggregated or statistical, which means that we will not be able to identify you individually.

You can set your browser not to accept cookies and the websites below tell you how to remove cookies from your browser. However, some of our website or service features may not function as a result.

For further information on our use of cookies and other similar tracking technologies, including a detailed list of your information which we and others may collect through cookies, please see below.

3 Why do we use cookies?

We use cookies and other similar tracking technologies to:

1. recognise you whenever you visit our website or app (this speeds up your access to this as you do not have to log in each time);
2. obtain information about your preferences and use of our Services;
3. carry out research and statistical analysis to help improve our content and services and to help us better understand our users' requirements; and
4. make your online experience more efficient and enjoyable.

4 Types of cookies

The cookies we place on your device fall into the following categories:

1. Strictly necessary cookies. These cookies are essential for you to be able to navigate our Services and use their features. Without these cookies, the services you have asked for could not be provided.

2. Analytical / performance cookies. These cookies collect information about how you use our Services, e.g. which pages you go to most often. These cookies do not collect personally identifiable information about you. All information collected by these cookies is aggregated and anonymous and is only used to improve how our website works.
3. Functionality cookies. These cookies allow our website to remember the choices you make (such as your username, language, last action and search preferences) and provide enhanced, more personal features. The information collected by these cookies is anonymous and cannot track your browsing activity on other websites.
4. Targeting cookies. Also known as advertising cookies, these cookies are used to deliver adverts more relevant to you and your interests. They are also used to limit the number of times you see an advertisement on our website and help measure the effectiveness of the advertising campaign. They are usually placed by advertising networks with the website operator's permission. They remember that you have visited a website and this information is shared with other organisations such as advertisers.

5 The cookies we use

At Yonder we set and use some cookies ourselves but only on our site. We refer to these as first party cookies. When cookies are served by another domain or by one of our service providers we refer to them as third party cookies. Please see what cookies and other similar tracking technologies we use below:

Cookie Name	Provider	Expiry	Purpose	Type
fs-cc	Yonder	6 months	Stores the user's cookie consent preferences.	Functional
ANONCHK	Microsoft Clarity	10 minutes	Indicates whether MUID is transferred to ANID (used for advertising). Clarity doesn't use ANID, so always set to 0.	Analytics
MR	Microsoft Clarity	13 months	Used by Microsoft Clarity/Advertising to measure or refresh MUID for analytics.	Analytics

SRM_B	Microsoft Bing	1 year	Used by Bing/Microsoft to collect usage data for analytics and performance measurement.	Analytics
MUID	Microsoft Clarity	13 months	Identifies unique browsers visiting Microsoft sites; used for advertising, analytics, and other operational purposes.	Analytics
_tt_enable_cookie	TikTok	90 days	Determines whether TikTok tracking is enabled, allowing measurement of conversions and ad performance.	Advertising
_gcl_au	Google	90 days	Used by Google AdSense/Tag Manager code on Yonder's site to measure ad campaign performance and conversions.	Advertising
_clsk	Microsoft Clarity	1 year	Connects multiple page views by a user into a single Clarity session recording.	Analytics
__Secure-ENID	Google	13 months	Helps secure/encrypt user preferences; can support personalized services and protect against malicious activity.	Functional
_ttp	TikTok	13 months	Used by TikTok to store and track conversions for ad analytics.	Advertising

NID	Google	6 months	Stores user preferences, helps personalize ads on Google sites.	Advertising
SRCHD	Microsoft Bing	1 year	Stores Bing search preferences or usage data for analytics.	Analytics
IDE	Google DoubleClick	13 months	Used by Google DoubleClick to measure ad performance and present targeted ads.	Advertising
HSID	Google	2 years	Contains encrypted Google Account ID/sign-in time for security/fraud prevention.	Analytics
SSID	Google	2 years	Contains encrypted info to help secure user sessions on Google services.	Analytics
SIDCC	Google	6 months	Used by Google for security to protect user data and detect unauthorized access.	Analytics
__Secure-3PSIDCC	Google	6 months	Used for targeting/advertising; helps Google build a profile of user interests.	Advertising
__Secure-1PSIDCC	Google	1 year	Helps secure Google user data (encrypted) and store certain preferences.	Functional

AEC	Google	6 months	Ensures requests during a browsing session are from the user, preventing malicious site requests.	Analytics
SM	Microsoft Clarity	Session	Stores user session data for Microsoft Clarity analytics/session replay.	Analytics
SRCHUSR	Microsoft Bing	1 year	Stores user preferences/usage data for Bing services (analytics, personalization).	Analytics
_ga	Google Analytics	1 year	Used by Google Analytics scripts on Yonder to distinguish unique users and measure site usage.	Analytics
_ga_3RYJJEB7BQ	Google Analytics	1 year	Additional Google Analytics cookie to persist session state.	Analytics
_SS	Microsoft Bing	Session	Bing session cookie; stores user session data for analytics or search.	Analytics
SRCHHPGUSR	Microsoft Bing	1 year	Stores user preferences (e.g., language, region) for personalized Bing search.	Analytics
SRCHUID	Microsoft Bing	1 year	Uniquely identifies a user for Bing analytics.	Analytics
_podscribe_yonder_referrer	Podscribe	1 year	Tracks the referring URL for	Analytics

			Podscribe analytics.	
S	Google	Session	Generic Google session cookie for maintaining session state.	Functional
testedUserId:cm1tinlzl001n7gk3i6mc6rd0	Optibase	30 days	Stores a test user identifier (often for QA or A/B testing).	Functional
__Secure-3PAPISID	Google	2 years	Used by Google for ad personalization and retargeting.	Advertising
SAPISID	Google	2 years	Used by Google to store user preferences; can be used for YouTube or ad targeting.	Advertising
__Secure-1PAPISID	Google	2 years	Used by Google for security and user preference settings.	Functional
CLID	Microsoft Clarity	13 months	Identifies the first time Clarity saw this user on any site using Clarity (user ID tracking).	Analytics
APISID	Google	2 years	Used by Google to store user preferences and possibly build ad profiles.	Advertising
__Secure-1PSID	Google	2 years	Used by Google for security and preference settings.	Functional
__Secure-3PSID	Google	2 years	Used by Google for targeting/advertising.	Advertising

SID	Google	2 years	Contains encrypted Google Account ID/sign-in time; used for security and to prevent fraudulent use.	Security
_podscribe_yonder_landing_url	Podscribe	1 year	Records the landing page URL for Podscribe analytics.	Analytics
__podscribe_yonder_landing_url	Yonder	1 year	Same as above, for Podscribe analytics on Yonder's domain.	Analytics
_clck	Microsoft Clarity	13 months	Persists the Microsoft Clarity User ID so visits are attributed to the same user ID.	Analytics
_podscribe_did	Podscribe	1 year	Stores a unique device/user ID for Podscribe tracking.	Analytics
__podscribe_did	Yonder	1 year	Same Podscribe device ID, hosted on Yonder's domain.	Analytics
__Secure-1PSIDTS	Google	1 year	Used by Google for security or preference settings.	Functional
__Secure-3PSIDTS	Google	1 year	Used by Google for ad personalization and targeting.	Advertising
fs-cc-updated	Yonder	6 months	Indicates an update to user cookie consent preferences.	Functional
ajs_anonymous_id	Segment	1 year	Used by Segment to identify an anonymous user for analytics.	Analytics

ajs_user_id	Segment	1 year	Used by Segment to store a user's ID (if logged in) for analytics.	Analytics
ko_id	Segment	1 year	Used by Segment to uniquely identify a user for analytics.	Analytics
mkjs_user_id	Segment	1 year	Another Segment cookie storing user identity for analytics.	Analytics
AMCV_32523BB96217F7B60A495CB6%40AdobeOrg	Adobe	1 year	Adobe Experience Cloud ID to recognize unique visitors across solutions (served via .segment.com).	Analytics
AMP_d2d2c4eada	Yonder	1 year	Used for analytics on AMP pages (often storing a client ID for tracking).	Analytics
AMP_MKTG_d2d2c4eada	Yonder	1 year	Similar to above, for marketing/tracking on AMP pages.	Analytics
mkjs_group_id	Segment	1 year	"Group" identifier in Segment for advanced analytics (e.g., grouping users under an account).	Analytics
_fbp	Facebook	90 days	First-party cookie set by Facebook Pixel to deliver ads and track visits/conversions across websites.	Advertising
AMCVS_32523BB96217F7B60A495CB6%40AdobeOrg	Adobe	Session	Adobe Marketing Cloud session ID to identify the	Analytics

			visitor during the session.	
datoAccountEmail	DatoCMS	Session	Stores the user's DatoCMS account email for functional login/service use.	Functional
usida	Facebook	Session	Used by Facebook to collect user data for analytics/ad targeting within a session.	Advertising
sb	Facebook	2 years	Identifies the browser securely to help with account security and site integrity on Facebook.	Security
datr	Facebook	2 years	Identifies the browser for Facebook security/integrity checks (fraud prevention).	Security
ar_debug	Google Analytics	30 days	Used by Google Analytics/Double Click for debugging or troubleshooting analytics/ad code.	Analytics
driftt_aid	Drift	1 year	Unique user ID for Drift chat/analytics (loaded via Segment).	Analytics
timezone	Segment	1 year	Stores the user's timezone in Segment for analytics or personalization.	Functional

_cq_duid	cQuotient (Salesforce)	90 days	Unique user ID for cQuotient analytics/personalization (loaded via Segment).	Analytics
drift_aid	Drift	1 year	Duplicate naming for Drift's user ID tracking for live chat/analytics.	Analytics
notice_behavior	Segment	Session	Stores user cookie-banner or privacy-notice interactions.	Functional
optimizelyEndUserId	Optimizely	6 months	Identifies a visitor for A/B testing and analytics (loaded via Segment).	Analytics
_hjSessionUser_1635800	Hotjar	1 year	Hotjar user/session analytics cookie (loaded via Segment).	Analytics
cookies-accepted	DatoCMS	1 year	Tracks whether the user accepted cookies in DatoCMS.	Functional
ph_phc_u7FPCuTnUpVlYYTYmfeutKpnI7qEE2cjwgzjz3JDuH6_posthog	PostHog	1 year	PostHog analytics cookie tracking user interactions and sessions (via .datocms.com).	Analytics
oo	Facebook	2 years	Facebook "opt-out" cookie for ad settings or data collection preferences.	Advertising
_cq_suid	cQuotient (Salesforce)	Session	Short-term unique ID for cQuotient/Segment session analytics.	Analytics

yonderpass_code	Yonder	Session	Used to facilitate our referral program, YonderPass. Unique code for the referral.	Functional
referral_code	Yonder	Session	Used to facilitate our referral program, YonderPass. Unique code for the referral.	Functional
Lead	Yonder	Session	Stores attribution data (e.g., UTM parameters) to help identify lead sources.	Analytics

We may also use pixels or web beacons in direct marketing emails that we send to you. These pixels track whether our email was delivered and opened and whether links within the email were clicked. They also allow us to collect information such as your IP address, browser, email client type and other similar details. We use this information to measure the performance of our email campaigns, and for analytics.

6 Consent to cookies

We will ask for your permission (consent) to place cookies or other similar tracking technologies on your device, except where these are essential for us to provide you with a service that you have requested.

There is a notice on our home page which describes how we use cookies and requests your consent before we place any non-essential cookies on your device.

7 How to turn off cookies

If you do not want to accept cookies, you can change your browser settings so that cookies are not accepted. If you do this, please be aware that you may lose some of the functionality of our Services.

To find out more about cookies, including how to see which cookies have been set and how to manage and delete them, you can visit the third-party website: www.allaboutcookies.org.