Trilo Privacy Policy

Version: 1.0
Last updated: 1 July 2026
Effective from: 1 July 2026

This Privacy Policy explains how Trilo Group Limited collects, uses, stores and shares personal data.

It applies to people who use Trilo, including merchants, merchant staff, customers, End Users, website visitors, prospective customers, business contacts, suppliers and anyone who contacts us.

Please read this policy carefully. It explains what personal data we collect, why we use it, the lawful bases we rely on, who we share it with, how long we keep it, and the rights you have.

---

1. Who we are

Trilo Group Limited is a company registered in England and Wales with company number 11684530.

Our registered office is:

2nd Floor, South One Castle Park, Tower Hill, Bristol, England, BS2 0JA

Trilo Group Limited is authorised by the Financial Conduct Authority under the Payment Services Regulations 2017 with permission to provide account information services and payment initiation services. Our Firm Reference Number is **919295**.

For the purposes of data protection law, Trilo Group Limited is usually the controller of the personal data described in this Privacy Policy. This means we decide how and why that personal data is used.

You can contact us about privacy and data protection at:

privacy@trilo.io

You can also contact us by post at the registered office address above.

---

2. What this policy covers

This policy explains how we use personal data when you:

- visit our website;
- create or use a Trilo account;
- use Trilo to make or receive payments;
- use Trilo as a merchant, business owner, employee or representative;
- use Trilo as an End User or customer;
- use Trilo Boost, rewards, payment links, QR payments, terminals, shopfronts or other Trilo services;
- contact us for support or sales enquiries;
- receive marketing or other communications from us;
- interact with us as a supplier, contractor, adviser, investor, partner or business contact.

This policy should be read alongside our Terms & Conditions, Merchant Terms of Service, Cookie Policy and any other privacy or data terms provided to you.

---

3. Personal data we collect

The personal data we collect depends on how you interact with Trilo.

We may collect and use the following categories of personal data.

3.1 Identity and contact information

This may include:

- name;
- email address;
- phone number;
- postal address;
- business name;
- job title;
- username;
- account login details;
- information about the business or organisation you represent.

3.2 Merchant and business information

If you create or use a merchant account, we may collect:

- business name and trading name;
- company number;
- registered office and trading address;
- business email address and telephone number;
- website and social media links;
- details of owners, directors, shareholders, beneficial owners, authorised users and staff;

- business category, products, services and trading information;
- bank account details for receiving payments;
- onboarding, verification, due diligence, fraud prevention and risk information;
- information submitted through account forms, onboarding flows, support requests or merchant dashboards.

3.3 Payment and Open Banking information

When you use Trilo to make, initiate, receive, manage or refund payments, we may process information such as:

- payment amount;
- payment reference;
- payment status;
- payment date and time;
- merchant details;
- payer and payee information;
- bank account name;
- sort code and account number;
- IBAN, where relevant;
- transaction identifiers;
- refund information;
- information received through Open Banking connections;
- payment metadata provided by banks, merchants, users or payment partners.

We do not ask you to provide online banking passwords to Trilo. Where you authorise an Open Banking payment or account connection, this is handled through your bank or the relevant Open Banking flow.

3.4 Account and profile information

This may include:

- account preferences;
- authentication details;
- device details;
- account settings;
- profile details;
- Trilo Boost or rewards activity;
- merchant or customer history;
- saved preferences;
- linked accounts or businesses;
- support history.

3.5 Technical and usage information

When you use our website or services, we may collect:

- IP address;
- browser type and version;
- device type;
- operating system;
- approximate location derived from IP address;
- pages viewed;
- links clicked;
- date and time of access;
- referring website;
- error logs;
- session information;
- analytics data;
- security logs;
- fraud and risk signals.

3.6 Communications and support information

When you contact us, we may collect:

- your name and contact details;
- the content of your message;
- support tickets;
- emails;
- chat messages;
- call notes;
- feedback;
- complaints;
- information needed to investigate and respond to your enquiry.

3.7 Marketing and sales information

This may include:

- name;
- email address;
- business name;
- job title;
- marketing preferences;
- communication history;
- whether you open, click or respond to marketing communications;
- information from events, referrals, public sources or business directories.

3.8 Information from third parties

We may receive personal data from third parties, including:

- merchants;
- customers;

- banks;
- Open Banking providers;
- payment processors;
- acquiring partners;
- fraud prevention providers;
- identity verification providers;
- analytics providers;
- support providers;
- public registers;
- Companies House;
- business directories;
- professional advisers;
- regulators or public authorities.

3.9 Special category data

We do not normally collect special category personal data, such as health information, religious beliefs, political opinions, trade union membership, ethnicity or biometric data.

Please do not provide special category data to us unless we specifically ask for it or it is strictly necessary.

---

4. How we collect personal data

We collect personal data in the following ways:

- directly from you when you create an account, use Trilo, contact us, complete a form, make a payment or use our services;
- from merchants or businesses that use Trilo;
- from banks and payment account providers when you authorise an Open Banking connection or payment;
- from payment processors, acquiring partners and other payment service providers;
- from service providers that help us operate Trilo;
- automatically when you use our website or services;
- from public sources, such as Companies House, business websites and public directories;
- from referrals, partners, suppliers, advisers and other third parties.

---

5. How we use personal data

We use personal data for the purposes set out below.

5.1 To provide Trilo services

We use personal data to:

- create and manage accounts;
- onboard merchants;
- provide payment initiation services;
- provide account information services where enabled;
- process, initiate, manage and record payments;
- support refunds;
- operate Trilo Boost and rewards;
- provide payment links, QR payments, shopfronts, dashboards, terminals, integrations and related services;
- provide customer support;
- communicate service messages;
- maintain service records.

Our lawful bases for this processing are usually:

- performance of a contract;
- legitimate interests;
- legal obligation;
- consent, where required.

Where we provide regulated Open Banking services, we may also ask for explicit consent under payment services rules. This is separate from consent under data protection law.

5.2 To onboard, verify and monitor merchants

We use personal data to:

- verify merchant accounts;
- assess eligibility to use Trilo;
- carry out due diligence;
- prevent fraud and misuse;
- assess risk;
- comply with legal and regulatory obligations;
- monitor use of the services;
- investigate suspicious activity;
- manage account limits, restrictions, suspensions and terminations.

Our lawful bases for this processing are usually:

- legal obligation;
- legitimate interests;
- performance of a contract.

5.3 To process payments and refunds

We use personal data to:

- initiate payments;
- confirm payment status;
- support refunds;
- reconcile payments;
- provide transaction records;
- communicate with merchants, banks and payment partners;
- investigate failed, disputed, suspicious or unauthorised payments.

Our lawful bases for this processing are usually:

- performance of a contract;
- legal obligation;
- legitimate interests;
- consent, where required.

5.4 To provide card, wallet and terminal services

Where card, Apple Pay, Google Pay, terminal or acquiring partner services are enabled, we may use personal data to:

- support card and wallet payments;
- manage terminal subscriptions;
- connect merchants with acquiring partners or processors;
- process transaction and settlement information;
- manage chargebacks, reversals, disputes and refunds;
- prevent fraud and misuse;
- comply with scheme, acquiring partner, legal and regulatory requirements.

Our lawful bases for this processing are usually:

- performance of a contract;
- legal obligation;
- legitimate interests.

5.5 To communicate with you

We use personal data to:

- respond to enquiries;
- provide support;
- send service updates;
- send account notifications;
- send security alerts;
- provide information about changes to our terms, policies or services;
- manage complaints;
- maintain records of communications.

Our lawful bases for this processing are usually:

- performance of a contract;
- legitimate interests;
- legal obligation.

5.6 To improve and secure Trilo

We use personal data to:

- monitor performance;
- fix bugs;
- improve products and features;
- develop new services;
- analyse usage;
- prevent security incidents;
- detect fraud, misuse and unauthorised access;
- audit and test systems;
- maintain logs and backups.

Our lawful bases for this processing are usually:

- legitimate interests;
- legal obligation.

5.7 To send marketing and business communications

We may use personal data to:

- contact prospective merchants;
- send updates about Trilo;
- send product information;
- invite businesses to use Trilo;
- provide offers, promotions or referral information;
- measure engagement with our communications.

Our lawful bases for this processing are usually:

- legitimate interests for business-to-business marketing;
- consent where required by law.

You can opt out of marketing communications at any time by using the unsubscribe link in our emails or by contacting us at privacy@trilo.io.

5.8 To comply with law and protect our rights

We use personal data to:

- comply with legal, regulatory, tax, accounting and audit obligations;
- respond to regulators, law enforcement, courts or public authorities;
- keep required business and compliance records;

- enforce our terms;
- bring or defend legal claims;
- protect Trilo, users, merchants, partners and others.

Our lawful bases for this processing are usually:

- legal obligation;
- legitimate interests.

---

6. Our legitimate interests

Where we rely on legitimate interests, our interests may include:

- operating and improving Trilo;
- supporting merchants and End Users;
- preventing fraud and misuse;
- protecting the security of our systems;
- managing risk;
- enforcing our terms;
- recovering debts;
- developing our products;
- communicating with business customers and prospective customers;
- keeping records;
- protecting our legal rights;
- supporting business operations.

We only rely on legitimate interests where we consider that our interests are not overridden by your rights, interests and freedoms.

You have the right to object to processing based on legitimate interests. You can contact us at privacy@trilo.io.

---

7. When we use consent

We may rely on consent where required, including for certain marketing, cookies or optional product features.

Where we rely on consent, you can withdraw that consent at any time. Withdrawing consent will not affect processing that took place before consent was withdrawn.

For Open Banking payment initiation and account information services, we may also ask for explicit consent under payment services rules before providing the relevant regulated service. This is not the same as consent under data protection law.

8. Who we share personal data with

We may share personal data with the following categories of recipient where necessary and lawful:

- banks and payment account providers;
- Open Banking providers;
- payment processors;
- acquiring partners;
- card schemes and wallet providers;
- terminal providers;
- fraud prevention and identity verification providers;
- cloud hosting and infrastructure providers;
- analytics providers;
- customer support and communication providers;
- email and marketing providers;
- professional advisers, including lawyers, accountants, auditors and insurers;
- regulators, courts, law enforcement agencies, tax authorities and public bodies;
- merchants, where necessary to provide Trilo services;
- End Users, where necessary to provide Trilo services;
- suppliers, contractors and business partners;
- potential buyers, investors, funders or advisers in connection with a sale, investment, restructuring or corporate transaction.

We only share personal data where we have a lawful basis to do so and where appropriate safeguards are in place.

---

9. International transfers

Some of our service providers or partners may process personal data outside the United Kingdom.

Where personal data is transferred outside the UK, we will ensure that appropriate safeguards are in place. These may include:

- an adequacy regulation;
- the UK International Data Transfer Agreement;
- the UK Addendum to the EU Standard Contractual Clauses;
- other safeguards permitted by data protection law.

You can contact us at privacy@trilo.io for more information about international transfer safeguards.

---

10. How long we keep personal data

We keep personal data only for as long as necessary for the purposes for which it was collected.

The retention period depends on the type of data, the reason we use it, legal and regulatory requirements, fraud prevention requirements, accounting requirements, and whether we need it to bring or defend legal claims.

As a general guide:

- account and merchant records may be kept for up to 7 years after the end of the relationship;
- payment and transaction records may be kept for up to 7 years, or longer if required by law or regulation;
- support and correspondence records may be kept for up to 7 years where relevant to the account or services;
- marketing records may be kept until you unsubscribe or ask us to stop contacting you, subject to keeping a suppression record;
- enquiry records where no account is created may usually be kept for up to 12 months after the last contact;
- security logs may be kept for a shorter period unless needed for investigation, fraud prevention, legal or regulatory reasons;
- records needed for legal claims, complaints, fraud prevention, tax, accounting, regulatory or audit purposes may be kept for longer where necessary.

When we no longer need personal data, we will delete it, anonymise it or securely archive it.

---

11. Security

We take appropriate technical and organisational measures to protect personal data.

These measures may include:

- encryption in transit;
- encryption at rest where appropriate;
- access controls;
- multi-factor authentication for internal systems where appropriate;
- staff access controls based on role and need;
- logging and monitoring;
- secure cloud infrastructure;
- regular review of permissions;
- security testing and operational monitoring;
- policies and procedures for data handling and incident response.

No system is completely secure. You are responsible for keeping your own login details, devices and accounts secure and for telling us promptly if you suspect unauthorised access.

If you believe there has been a security issue involving Trilo, please contact:

security@trilo.io

---

12. Data breaches

If we become aware of a personal data breach, we will assess it and take appropriate action.

Where required by law, we will notify the Information Commissioner's Office. Where required by law, we will also notify affected individuals.

---

13. Automated decision-making and profiling

We may use automated tools to help detect fraud, assess risk, protect our systems, monitor transactions, prevent misuse and support compliance.

We do not currently make decisions based solely on automated processing that have legal or similarly significant effects on individuals, unless this is lawful and appropriate safeguards are in place.

---

14. Your rights

Under data protection law, you may have the following rights:

- the right to be informed about how your personal data is used;
- the right to access your personal data;
- the right to correct inaccurate or incomplete personal data;
- the right to ask for personal data to be erased;
- the right to restrict processing;
- the right to object to processing based on legitimate interests;
- the right to object to direct marketing;
- the right to data portability;
- rights relating to automated decision-making and profiling;
- the right to withdraw consent where processing is based on consent;
- the right to complain to the Information Commissioner's Office.

These rights are not absolute and may depend on the circumstances. For example, we may need to keep certain information to comply with legal, regulatory, accounting or fraud prevention obligations.

To exercise your rights, contact us at:

privacy@trilo.io

We may need to verify your identity before responding.

We will usually respond within one month. If your request is complex or you have made multiple requests, we may take longer, as permitted by law.

---

15. Marketing preferences

You can opt out of marketing emails at any time by using the unsubscribe link in the email or by contacting us at:

privacy@trilo.io

If you opt out, we may keep a suppression record so that we know not to send you further marketing.

You may still receive service, account, legal, security or transactional messages where necessary.

---

16. Cookies and similar technologies

We use cookies and similar technologies on our website and services.

Some cookies are necessary for the website and services to work. Others may help us understand website usage, improve performance, remember preferences or support marketing.

More information is available in our Cookie Policy.

---

17. Third-party websites and services

Our website and services may contain links to third-party websites, services or applications.

We are not responsible for the privacy practices, content or security of third-party websites or services. You should read their privacy policies before providing personal data to them.

18. Complaints

If you have a concern about how we use your personal data, please contact us first so that we can try to resolve it.

You can contact us at:

privacy@trilo.io

You also have the right to complain to the Information Commissioner's Office, the UK supervisory authority for data protection.

ICO website: **https://ico.org.uk**
ICO telephone: **0303 123 1113**

---

19. Changes to this Privacy Policy

We may update this Privacy Policy from time to time.

The latest version will be made available on our website. Where changes are material, we may take additional steps to notify you, such as by email, in-product notice or dashboard message.

Your continued use of Trilo after an updated Privacy Policy is published will be treated as your acknowledgement of the updated policy.

---

20. Contact us

For questions about this Privacy Policy or how we use personal data, contact:

Trilo Group Limited
Bath House, Bath Street, Redcliffe, Bristol, England, BS1 6HL
Email: **privacy@trilo.io**

For security issues, contact:

security@trilo.io