PUBLIC PRIVACY NOTICE

Privacy Notice

Website visitors, business contacts and merchant onboarding

Effective date: 7 September 2026

1. About this notice

This notice explains how Vesta Merchant Services collects, uses, shares and protects personal data when you visit our websites, contact us about our services, act for a business that uses or may use our services, or take part in merchant onboarding. It also explains your privacy rights and how to exercise them.

This notice does not cover Vesta employees, workers, contractors or job applicants. Those individuals should be given a separate workforce or recruitment privacy notice. Where we process personal data solely on the instructions of a merchant or other business customer, that customer is responsible for explaining its processing to you in its own privacy notice.

2. Who we are

The controller responsible for the processing described in this notice is Vesta Merchant Services Limited, trading as VestaOne, company number 07108015, with its registered office at Stables 1, Howbery Park, Wallingford, Oxfordshire, OX10 8BA. It forms part of the Vesta Software Group.

If another Vesta group company acts as a separate or joint controller for a particular activity, we will identify that company and explain the arrangement at the point where personal data is collected.

How to contact us

Email: compliance@vestamerchantservices.com

Telephone: 01634 292 867

Post: Vesta Merchant Services, Stables 1, Howbery Park, Wallingford, Oxfordshire, OX10 8BA, United Kingdom

Data Protection Officer: Jenny Ball

DPO email: jenny.ball@vestasoftwaregroup.com

3. Who this notice covers

1. Visitors to Vesta websites, portals and other online services that link to this notice.
2. People who contact us or request information about our products and services.
3. Sole traders, partners and other individuals who apply for or receive merchant services.
4. Directors, beneficial owners, partners, trustees, officers, authorised signatories and other individuals connected with a merchant or prospective merchant.
5. Employees, advisers and other business contacts who communicate with us on behalf of a merchant, supplier, partner or prospective customer.

4. Personal data we collect

The personal data we collect depends on your relationship with us and the services involved. We may collect the following categories:

Identity data: Name, title, date of birth, nationality, signature, photographic identification and unique identification numbers.

Contact data: Business and personal contact details, including postal address, email address and telephone number.

Business and ownership data: Role, employer, company details, ownership or control, directorships, authorised signatories, trading information, sites and payment channels.

Verification and due-diligence data: Identity-verification results, document checks, liveness or electronic verification results, sanctions and politically exposed person screening, source-of-funds or related information where required, and records of compliance reviews.

Financial and payment data: Bank account details, settlement details, billing information and information needed to administer merchant services. We do not intentionally request full card security codes through general website forms.

Service, transaction and risk data: Application status, merchant category, expected and actual transaction information, chargebacks, disputes, fraud indicators, risk assessments, service usage and support history.

Technical and usage data: IP address, device and browser information, login and security data, pages and features used, timestamps, referral information and diagnostic records.

Communications data: Emails, telephone notes, complaints, requests, survey responses and other correspondence with us.

Marketing preferences: Your choices about receiving marketing and how you prefer us to contact you.

Special category and criminal offence data

We do not routinely seek special category personal data through our general website. Where identity, fraud-prevention or regulatory checks reveal special category data or criminal-offence information, we will process it only where an additional legal condition applies and appropriate safeguards are in place.

5. How we obtain personal data

We may obtain personal data:

1. directly from you, including through onboarding forms, websites, portals, emails, telephone calls and meetings;
2. from the merchant, prospective merchant or other organisation with which you are connected;
3. from identity-verification, fraud-prevention, credit-reference, sanctions-screening and due-diligence providers;
4. from acquiring banks, payment processors, card schemes and other partners involved in providing merchant services;
5. from public registers and publicly available sources, including Companies House and professional or corporate websites; and
6. automatically when you use our websites or online services, including through server logs and permitted cookies or similar technologies.

6. How and why we use personal data

We must have a lawful basis for each use of personal data. The bases most likely to apply are: steps requested before entering into a contract; performance of a contract with you; compliance with a legal obligation; consent; and our legitimate interests or those of another organisation, provided those interests are not overridden by your rights and interests.

Responding to enquiries and developing business relationships

What we do: We use identity, contact, business and communications data to answer enquiries, provide requested information and manage relationships with merchants, prospective merchants and partners.

Lawful basis: Legitimate interests in operating and developing our business. Where you are contracting with us personally, taking steps at your request before entering into a contract may also apply.

Assessing and onboarding merchants

What we do: We use identity, contact, business, ownership, verification, financial and risk data to assess applications, verify individuals, establish authority to act and decide whether we can offer services.

Lawful basis: Steps before entering into a contract or contract, where the contract is with you; legal obligation where applicable; and legitimate interests in conducting due diligence, managing risk and preventing misuse of our services.

Meeting legal and regulatory requirements

What we do: We use identity, ownership, verification, transaction and communications data to carry out checks, maintain records, respond to regulators or authorities and meet applicable financial-crime, sanctions, tax, accounting and other requirements.

Lawful basis: Legal obligation. In limited cases, legitimate interests in demonstrating compliance and protecting the integrity of our services.

Providing and administering merchant services

What we do: We use contact, financial, service, transaction and communications data to set up and administer accounts, arrange settlement, provide support, manage fees and rates, maintain service records and communicate operational updates.

Lawful basis: Contract where the contract is with you; otherwise legitimate interests in performing our agreement with the merchant and providing reliable services.

Fraud prevention, security and risk management

What we do: We use identity, verification, technical, transaction and risk data to authenticate users, detect and investigate suspicious activity, protect systems, manage credit and operational risk, and establish or defend legal claims.

Lawful basis: Legal obligation where applicable and legitimate interests in protecting Vesta, merchants, partners and the public from fraud, financial crime, security threats and loss.

Operating and improving websites and services

What we do: We use technical, usage, service and communications data to maintain functionality, troubleshoot, test, analyse performance and improve user experience.

Lawful basis: Legitimate interests in maintaining and improving secure services. Consent, or a specific PECR exception, applies where required for storage and access technologies.

Service and administrative communications

What we do: We use identity and contact data to provide onboarding updates, security notices, changes to contractual terms, policy updates and other non-marketing communications.

Lawful basis: Contract, legal obligation and legitimate interests in keeping relevant people informed.

Marketing

What we do: We use business contact details and marketing preferences to send relevant information about Vesta services and events.

Lawful basis: Consent where required by the Privacy and Electronic Communications Regulations. In other permitted business-to-business circumstances, legitimate interests may apply. You can object or unsubscribe at any time.

Corporate transactions and legal matters

What we do: We may use and disclose relevant personal data in connection with audits, professional advice, restructuring, investment, sale, merger or acquisition, and to establish, exercise or defend legal rights.

Lawful basis: Legitimate interests in managing our business and legal rights, and legal obligation where applicable.

When information is required

If we need personal data to comply with law or to enter into or perform a contract and you do not provide it, we may be unable to complete an application, verify an individual, provide services or continue a business relationship. We will explain any mandatory fields or consequences at the relevant time.

Change of purpose

We will use personal data only for the purposes for which it was collected unless another use is compatible with the original purpose or is otherwise permitted by law. If we need to use personal data for an unrelated purpose, we will provide further information before that processing begins, unless the law allows an exception.

7. Automated decision-making and profiling

Vesta may use automated tools to support identity verification, fraud detection, sanctions screening, transaction monitoring and risk assessment. These tools may generate matches, scores, flags or recommendations that help us decide whether to request more information, refer an application or activity for review, restrict activity, or decline or end a service. We take steps to keep the information used by these tools accurate and to reduce the risk of unfair or biased outcomes.

We will not make a decision based solely on automated processing that produces legal or similarly significant effects unless the processing is permitted by law and appropriate safeguards are in place. Where such processing applies, we will provide further information about the main factors involved and the likely consequences. You may contact us to request human intervention, express your point of view, obtain an explanation and challenge the decision.

8. Who we share personal data with

Where necessary for the purposes described above, we may share personal data with:

1. companies within the Vesta Software Group that provide management, compliance, finance, technology or other support;
2. acquiring banks, payment processors, card schemes, banking partners and other organisations involved in providing merchant services;
3. identity-verification, fraud-prevention, credit-reference, sanctions-screening and due-diligence providers;
4. IT, cloud-hosting, communications, customer-management, analytics and cybersecurity providers;
5. professional advisers, auditors, insurers and prospective purchasers, investors or counterparties in a corporate transaction;
6. law-enforcement bodies, regulators, courts, tax authorities and other public bodies where disclosure is required or permitted by law; and
7. other parties where you ask us to disclose information or give valid consent.

We require service providers acting on our behalf to protect personal data and use it only for agreed purposes. Some recipients, such as acquiring banks, card schemes, regulators and fraud-prevention organisations, may act as separate controllers and provide their own privacy information.

9. International transfers

Some Vesta group companies, service providers or business partners may process personal data outside the United Kingdom. Where this involves a restricted transfer, we will use a lawful transfer mechanism, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved EU standard contractual clauses, binding corporate rules or another mechanism permitted by law. Where required, we also assess whether additional safeguards are needed.

You may contact us for further information about the safeguards relevant to your personal data, subject to appropriate redactions for confidentiality and security.

10. How long we keep personal data

We keep personal data only for as long as reasonably necessary for the purpose for which it was collected, including legal, regulatory, accounting, reporting, fraud-prevention and dispute-resolution requirements. We normally apply the periods below. A longer or shorter period may apply where required by law, a regulator, the circumstances of a dispute or another documented business need.

Record category	Retention period
Merchant and contractual records	For the relationship and normally 6 years afterwards.
KYC, due-diligence and AML records	For the period required by applicable law; commonly 5 years after the relationship ends where the relevant rules apply.
Unsuccessful or withdrawn applications	Normally 12 months after closure, unless a longer period is justified for fraud prevention, legal claims or regulatory reasons.
Enquiries and routine correspondence	Normally 2 years after the matter is closed.
Complaints and disputes	Normally 6 years after final resolution, or longer where a claim or regulatory requirement remains relevant.
Marketing contacts	Until you opt out or after a defined period of inactivity. Minimal suppression information may be retained to respect your objection.
Technical logs and cookies	According to Vesta's security schedule and the cookie details in section 15.

We may anonymise personal data so that it can no longer identify you. We may use genuinely anonymous information for statistical and business purposes without further notice.

11. How we protect personal data

We use appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Measures may include access controls, authentication, encryption where appropriate, logging, monitoring, resilience and recovery procedures, staff training, supplier due diligence and incident-management processes.

No system can be guaranteed completely secure. You should protect account credentials, use strong and unique passwords, and contact us promptly if you believe an account or communication has been compromised.

12. Your privacy rights

Depending on the circumstances, you may have the right to:

1. ask for access to your personal data and certain information about how it is used;
2. ask us to correct inaccurate or incomplete personal data;
3. ask us to erase personal data where there is no lawful reason to continue processing it;
4. ask us to restrict processing in certain circumstances;
5. receive personal data you provided in a structured, commonly used and machine-readable format, and ask us to transmit it to another controller, where the portability right applies;
6. object to processing based on legitimate interests or a public task, based on your particular situation;
7. object at any time to the use of personal data for direct marketing, including related profiling;
8. withdraw consent at any time where processing relies on consent, without affecting earlier lawful processing; and
9. request safeguards and human intervention where rights relating to significant automated decisions apply.

Exercising your rights

Contact compliance@vestamerchantservices.com and describe the right you wish to exercise. You do not normally have to pay a fee. We may request proportionate information to verify your identity and authority, particularly where disclosure could create a risk to another person.

We will respond without undue delay and normally within one month. The law may allow an extension for complex or multiple requests; if so, we will explain the extension. Some rights are subject to exemptions and may not apply in every circumstance. If we cannot comply fully, we will explain why and tell you about available complaint routes.

13. Marketing communications

We may send relevant business-to-business marketing where permitted by law. Where consent is required, we will obtain it before sending the communication. You can unsubscribe by contacting us. Choosing not to receive marketing will not stop essential service, security, legal or administrative communications.

We do not sell personal data. We do not share personal data with organisations outside the Vesta group for their own direct marketing unless we have clearly explained this and have an appropriate lawful basis, including consent where required.

14. Data protection complaints

You may complain to us about how we have used your personal data by emailing complaints@vestamerchantservices.com. We will acknowledge a data-protection complaint within 30 days, investigate it without undue delay, keep you appropriately informed and tell you the outcome.

You also have the right to complain to the Information Commissioner's Office. Information about raising a concern is available through the ICO's official website at ico.org.uk. We would appreciate the opportunity to address your concerns first, but you do not have to contact us before contacting the ICO.

15. Cookies and similar technologies

Our websites may use cookies, pixels, scripts, local storage and similar technologies that store information on, or access information from, your device. We provide clear information about their purposes and available choices. We obtain prior consent for non-exempt technologies and make it as easy to reject them as to accept them. We do not treat continued browsing or inactivity as consent.

Some technologies may be used without consent where a specific legal exception applies, such as where they are strictly necessary to provide a service you request or, subject to all applicable conditions, for limited statistical or appearance purposes. You can revisit your choices using the cookie-settings control on our website.

Category	Purpose	Consent position	Technology, provider and duration
Strictly necessary	Security, authentication, load balancing and services specifically requested by the user.	No, where the legal exception applies.	__cf_bm — Cloudflare — bot management/security — 30-minute rolling expiry; __dpl — hosting/deployment platform — keeps visitors pinned to a consistent deployment build — approx. 24 hours; vestaone_cookie_consent_v2 — VestaOne — stores the user's cookie preferences — persists in localStorage until site data is cleared.
Statistical / analytics	Measure use of the site and improve it.	Consent unless Vesta has documented that every condition of the statistical-purpose exception is met.	No analytics cookies or browser storage identified. Google Analytics, Google Tag Manager, Act-On and other analytics platforms are not currently installed. /~flock.js performs cookieless web-vitals/performance measurement and sets no cookies or browser storage.
Preferences / appearance	Remember a user's display or interface choice.	May be exempt only where every condition of the appearance exception is met.	vestaone_a11y_prefs — VestaOne — localStorage used to remember accessibility/display settings including larger text, high contrast, reduced motion and theme preferences — persists until the user clears site data.

Category	Purpose	Consent position	Technology, provider and duration
Marketing / tracking	Measure campaigns, recognise users or personalise marketing.	Yes, unless another specific exception applies.	None currently identified. Act-On, Meta Pixel, LinkedIn Insight Tag, Google Ads/DoubleClick and other marketing/tracking technologies are not currently installed.

16. Children

Our merchant services and this website are intended for businesses and adults acting in a business capacity. They are not directed at children, and we do not knowingly collect children's personal data through merchant onboarding. If you believe a child has provided personal data to us, please contact us so that we can investigate and take appropriate action.

17. Links and third-party services

Our websites may link to websites or services operated by other organisations. Those organisations control their own processing and their privacy notices apply. We encourage you to review their information before providing personal data.

18. Changes to this notice

We may update this notice to reflect changes in our services, processing or legal obligations. The latest version will be posted on our website with its effective date. Where a change is material, we will take reasonable steps to bring it to the attention of affected individuals before the change takes effect where required.

Effective date: 7 September 2026