PRIVACY POLICY

FINTECH VALLEY LTD
(trading as "Cepheus" and/or "Cepheus Pay")

Last updated: 09 April 2026
Version: 2.0

1. INTRODUCTION

This Privacy Policy explains how FINTECH VALLEY LTD ("Fintech Valley", "Cepheus", "we", "us", "our") collects, uses, stores, shares, and otherwise processes personal data in connection with our website, mobile application, platform, electronic money services, payment services, card-related services, onboarding procedures, compliance checks, and related business operations.

This Privacy Policy applies to:

- prospective clients;
- current clients;
- former clients;
- authorised users acting on behalf of clients;
- beneficial owners, directors, shareholders, and representatives of corporate clients;
- cardholders;
- website and application users;
- counterparties, payees, and payers;
- suppliers, introducers, and business contacts.

This Privacy Policy should be read together with our Terms of Use / Terms of Business and any product-specific terms.

2. WHO WE ARE

FINTECH VALLEY LTD is a company incorporated in England and Wales under company number 11456625. We are authorised by the Financial Conduct Authority as a Small Electronic Money Institution, FCA reference number 900986. For the purposes of data protection law, Fintech Valley LTD is generally the controller of the personal data described in this Privacy Policy, unless we expressly state otherwise in a specific context.

Contact details:
FINTECH VALLEY LTD
960 Capability Green
Luton, Bedfordshire
LU1 3PE
United Kingdom

Email: privacy@cepheus-pay.com
General support: support@cepheus-pay.com

We have appointed a Data Protection Officer ("DPO") responsible for overseeing data protection and privacy matters.

You may contact our DPO at:
Email: dpo@cepheus-pay.com

The DPO is available for all enquiries relating to this Privacy Policy, the processing of personal data, and the exercise of your rights.

3. CATEGORIES OF PERSONAL DATA WE COLLECT

We may collect and process the following categories of personal data:

3.1 Identity and profile data

- full name;
- date of birth;
- nationality;
- photograph, selfie, or video identification data;
- username, profile details, and account identifiers.

3.2 Contact data

- residential address;
- registered office or business address;
- email address;
- telephone number;
- other contact details provided to us.

3.3 Corporate and ownership data

- company name, registration number, incorporation details;
- constitutional documents;
- details of directors, shareholders, beneficial owners, controllers, authorised signatories, and representatives;
- ownership and control structure information.

3.4 Verification and compliance data

- passport, identity card, driving licence, residence permit, or similar documents;
- proof of address;
- source of funds and source of wealth information;
- sanctions, politically exposed person, and adverse media screening results;
- fraud prevention and device-risk indicators;
- enhanced due diligence information;
- communications and records relating to onboarding or compliance reviews.

3.5 Financial and transaction data

- User Account identifiers (as defined in our Terms of Use, referring to system access credentials, profile identifiers, and internal system references, and not to a bank account or deposit account);
- internal ledger information;
- payment instructions;
- transaction history;
- counterparty details;
- payer and beneficiary information;
- bank account and IBAN details;
- card transaction information;
- top-ups, payouts, foreign exchange, and settlement data;
- fees, charges, recalls, disputes, reversals, and chargeback information.

3.6 Card programme data

Where you use card services, we may process:

- card status and card identifiers;
- card transaction data;
- card usage controls and spending limits;
- merchant category and transaction location data;
- tokenised or masked card data;
- lost, stolen, replacement, and dispute records.

Card data is processed in accordance with applicable card scheme rules and industry security standards, including where applicable the Payment Card Industry Data Security Standard (PCI DSS), and may be tokenised or otherwise protected using industry-standard security measures.

3.7 Technical and usage data

- IP address;
- browser type;
- operating system;
- device identifiers;
- app version;
- login history;

- authentication events;
- geolocation inferred from device or network, where relevant;
- cookie and analytics data.

3.8 Communications data

- emails;
- chat and support messages;
- call notes;
- complaints;
- documents submitted to us;
- records of interactions with our staff, systems, or providers.

3.9 Marketing and preference data

- communication preferences;
- consent records where applicable;
- interaction with marketing communications;
- preferences relating to our services.

3.10 Special category data

We do not seek to collect special category personal data unless this is necessary and lawful. In limited cases, identity verification, fraud prevention, AML/CTF checks, accessibility requests, or legal matters may result in processing data requiring enhanced protection.

4. HOW WE COLLECT PERSONAL DATA

We may collect personal data:

4.1 Directly from you

For example when you:

- apply for a User Account;
- complete onboarding;
- submit KYC/AML documents;
- use the website, mobile application, or services;
- request support;
- communicate with us;
- use card services;
- respond to requests for updated information.

4.2 From the client you represent

If you are a director, beneficial owner, authorised user, or employee of a corporate client, we may receive your personal data from that client or from another person acting on its behalf.

4.3 From third parties

Including:

- identity verification providers;
- compliance and screening providers;
- fraud prevention providers;
- card programme partners;
- Card Issuers;
- Payment Processors;
- banking and infrastructure partners;
- public registers;
- corporate databases;
- sanctions and PEP lists;
- law enforcement or regulators, where applicable.

4.4 Automatically

Through cookies, system logs, device telemetry, fraud-monitoring tools, and analytics tools when you use our website, mobile application, or services.

5. PURPOSES OF PROCESSING AND LAWFUL BASES

We may process personal data for the following purposes:

5.1 To assess applications and onboard clients

This includes verifying identity, establishing eligibility, assessing risk, and opening User Accounts.

Lawful basis:

- performance of a contract or steps at your request before entering into a contract;
- compliance with legal obligations;
- legitimate interests in operating secure and responsible services.

5.2 To provide our services

Including maintaining User Accounts, issuing electronic money, processing payments, enabling currency exchange, supporting card functionality, managing balances and fees, and providing support.

Lawful basis:

- performance of a contract;
- legitimate interests in operating and improving services.

5.3 To comply with AML, CTF, sanctions, fraud, and regulatory obligations

Including KYC, due diligence, ongoing monitoring, suspicious activity review, sanctions screening, record-keeping, safeguarding administration, and regulatory reporting.

Lawful basis:

- compliance with legal obligations;
- legitimate interests in preventing financial crime and protecting our business and partners.

5.4 To manage card programme services

Including card issuance support, transaction monitoring, fraud controls, merchant dispute support, and interactions with the Card Issuer and Card Programme Partner.

Lawful basis:

- performance of a contract;
- compliance with legal obligations;
- legitimate interests in fraud prevention, dispute management, and secure operation.

5.5 To protect security and service integrity

Including authentication, access control, incident detection, abuse prevention, cyber defence, and audit logging.

Lawful basis:

- compliance with legal obligations;
- legitimate interests in protecting our clients, systems, and business.

5.6 To communicate with you

Including operational notices, service messages, support replies, legal notices, and updates to terms or policies.

Lawful basis:

- performance of a contract;
- compliance with legal obligations;
- legitimate interests.

5.7 To improve our products and services

Including analytics, troubleshooting, testing, service development, business intelligence, and risk calibration.

Lawful basis:

- legitimate interests.

5.8 Marketing communications

We may use your personal data to send you information about our services, updates, and relevant offerings.

Where required by applicable law, we will obtain your consent before sending marketing communications.

Where permitted, we may rely on our legitimate interests to send communications relating to similar services, provided that you are given a clear opportunity to opt out.

You may opt out of receiving marketing communications at any time by using the unsubscribe mechanism or by contacting us.

5.9 To establish, exercise, or defend legal claims

Including disputes, investigations, debt recovery, complaints handling, and litigation.

Lawful basis:

- legitimate interests;
- compliance with legal obligations where applicable.

6. AUTOMATED DECISION-MAKING

We may use automated tools for:

- identity verification;
- fraud screening;
- sanctions and risk screening;
- transaction monitoring;
- device and behavioural risk analysis.

Where such processing is used, it may contribute to decisions about onboarding, transactions, restrictions, or further review. We generally combine automated tools with human review in risk-sensitive situations.

Where applicable, you may have the right to request human review and to contest a decision.

This may include profiling based on transaction behaviour, geographic indicators, device data, historical activity, and other risk-related factors in order to assess fraud risk, financial crime exposure, and compliance requirements.

7. WHO WE SHARE PERSONAL DATA WITH

We may share personal data with the following categories of recipients where necessary:

7.1 Group entities and affiliates

For compliance, operational support, risk management, fraud prevention, service delivery, and administration.

7.2 Banking and payments partners

Including:

- Safeguarding Account providers;
- Correspondent Banks;
- Intermediary Banks;
- Payment Processors;
- beneficiary or sending institutions;
- settlement and messaging providers.

7.3 Card programme participants

Including:

- Card Programme Partner;
- Card Issuer;
- card scheme participants;
- fraud and chargeback service providers.

7.4 Compliance and verification providers

Including:

- KYC / AML vendors;
- sanctions and adverse media screening providers;
- fraud prevention providers;
- identity verification services.

7.5 Technology and support providers

Including:

- cloud hosting providers;
- customer support tools;
- analytics providers;
- security vendors;
- email, communications, and document-processing providers.

7.6 Professional advisers

Including lawyers, accountants, auditors, consultants, and insurers.

7.7 Authorities and regulators

Including:

- the FCA;
- the ICO;
- law enforcement agencies;
- tax authorities;
- courts or tribunals;
- other competent authorities where required.

7.8 Corporate transactions

If we undergo or consider a merger, acquisition, restructuring, financing, sale of assets, or similar transaction, personal data may be shared with relevant parties subject to appropriate safeguards.

8. INTERNATIONAL TRANSFERS

Because we use international service providers and may work with payment, compliance, technology, and card partners in multiple jurisdictions, your personal data may be transferred outside the United Kingdom.

Where we transfer personal data internationally, we will do so using one or more lawful safeguards, including:

- transfer to a jurisdiction recognised as adequate under UK law;
- the UK International Data Transfer Agreement (IDTA);
- the UK Addendum to the EU Standard Contractual Clauses;
- another lawful transfer mechanism recognised under applicable law.

You may contact us for more information about the safeguards we use for relevant transfers.

9. DATA RETENTION

We retain personal data only for as long as necessary for the relevant purposes, including:

- providing services;
- maintaining security;
- complying with AML, safeguarding, financial crime, legal, tax, accounting, and regulatory obligations;
- resolving disputes and enforcing rights.

Retention periods vary depending on the category of data and legal requirements. In general:

- identification, onboarding, and AML/CTF records are retained for at least five (5) years following the end of the business relationship, or longer where required by law or regulatory expectation;

- transaction and payment records are typically retained for at least five (5) years in accordance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Records may be retained for a longer period where necessary to comply with other legal, regulatory, accounting, tax, dispute-resolution, or enforcement requirements;
- contractual and service-related records are retained for the duration of the relationship and applicable legal limitation periods;
- marketing data is retained until you opt out, withdraw consent (where applicable), or it is no longer necessary;
- incomplete or rejected application data may be retained for a reasonable period for fraud prevention, compliance, audit, and legal purposes.

Where possible, we may anonymise data so it no longer identifies individuals.

10. DATA SECURITY

We apply technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

These measures may include:

- access controls and least-privilege permissions;
- encryption in transit and, where appropriate, at rest;
- authentication controls;
- audit logging;
- fraud detection tools;
- vendor due diligence;
- internal policies, training, and incident response procedures.

No system is completely secure, but we work to maintain an appropriate level of protection relative to the risks.

11. YOUR RIGHTS

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

- request access to your personal data;
- request rectification of inaccurate or incomplete data;
- request erasure of personal data in certain circumstances;
- request restriction of processing;
- request portability of certain data;
- object to processing based on legitimate interests;
- object to direct marketing;
- withdraw consent where processing is based on consent;
- complain to the Information Commissioner's Office.

To exercise your rights, contact: **privacy@cepheus-pay.com** or **km@cepheus-pay.com**

We may ask for proof of identity before responding.

Some rights are subject to legal or regulatory limitations, including in the context of AML/CTF, fraud prevention, legal privilege, or the rights of others.

12. COOKIES AND SIMILAR TECHNOLOGIES

We may use cookies, SDKs, pixels, local storage, and similar technologies to:

- operate the website and mobile application;
- remember preferences;
- improve usability;
- measure performance;
- support security and fraud controls;
- analyse traffic and usage.

Where required by law, we will obtain consent before using non-essential cookies or similar technologies.

You can manage cookie preferences through our cookie tools and browser settings.

13. THIRD-PARTY LINKS AND SERVICES

Our website or application may contain links to third-party websites, services, or integrations. We are not responsible for their privacy practices. You should review their privacy information separately.

14. CHILDREN

Our services are not intended for children. We do not knowingly provide services to minors or intentionally collect their personal data except where this arises incidentally and lawfully in a specific context. If you believe a child has provided personal data to us improperly, contact us.

15. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in law, regulation, guidance, our services, or our data practices.

We will publish the updated version on our website or otherwise make it available through the services. Where required by law, we will take additional steps to notify you.

16. HOW TO CONTACT US

If you have questions about this Privacy Policy or our handling of personal data, contact:

Privacy Contact
Email: privacy@cepheus-pay.com

Data Protection Officer
Email: dpo@cepheus-pay.com

General support:
support@cepheus-pay.com

Postal contact:
FINTECH VALLEY LTD
960 Capability Green
Luton, Bedfordshire
LU1 3PE
United Kingdom

17. HOW TO COMPLAIN

If you are unhappy with how we use your personal data, please contact us first so we can try to resolve the issue.

You also have the right to complain to the Information Commissioner's Office (ICO) where our Registration reference is ZB398259.