PRIVACY POLICY

Last updated: 11/07/2026

1. Introduction

FEDAFONE LTD respects your privacy and is committed to protecting your personal data.

This Privacy Policy explains how we collect, use, store, disclose and protect your personal data when you:

- visit or use the fedafone website;
- create or use a fedafone account;
- purchase an eSIM or another service;
- use the fedafone mobile application;
- interact with the fedafone Telegram bot;
- contact our customer support;
- use any other service operated under the fedafone brand.

It also explains your rights under applicable data protection legislation, including the UK General Data Protection Regulation, the Data Protection Act 2018 and, where applicable, the EU General Data Protection Regulation 2016/679.

Please read this Privacy Policy carefully.

2. Who We Are

FEDAFONE LTD, trading under the brand name **fedafone**, is a company registered in the United Kingdom.

Company number: 15111795
Registered office: 2nd Floor, College House, 17 King Edwards Road, Ruislip, HA4 7AE, United Kingdom
Email: hello@fedafone.com
Website: www.fedafone.com

For the purposes of applicable data protection law, FEDAFONE LTD is the **data controller** of the personal data described in this Privacy Policy, unless otherwise stated.

A data controller determines why and how personal data is processed.

3. Scope of This Privacy Policy

This Privacy Policy applies to the processing of personal data by FEDAFONE LTD in connection with services provided to customers outside the Russian Federation.

The infrastructure and databases used for these customers are hosted primarily in France through OVH or its associated infrastructure providers.

This Privacy Policy does not govern the independent processing activities of third-party services, including payment providers, mobile network operators, Telegram, Apple, analytics providers or other third parties that operate under their own privacy policies.

4. Definitions

For the purposes of this Privacy Policy:

Personal data means any information relating to an identified or identifiable natural person.

Processing means any operation performed on personal data, including collecting, recording, organising, storing, using, disclosing, transferring, deleting or destroying it.

User, **you** or **your** means any person who visits, registers with or uses the fedafone services.

Account means a user account registered with fedafone.

Services means the fedafone website, mobile application, Telegram bot, customer-support services and the sale or provision of eSIM products.

eSIM means a digital SIM profile supplied for use with a compatible device.

Service provider or **processor** means a third party that processes personal data on our behalf.

5. Personal Data We Collect

We aim to collect only the personal data that is reasonably necessary to provide and operate our Services.

5.1. Account information

When you create an Account, we collect:

- your email address;
- your internal user or account identifier;
- the date and time of registration;
- account status and authentication information;
- optional profile information that you choose to provide.

An email address is required to create an Account.

Other profile information, including a name or display name, may be optional. We do not require users to provide their legal name unless it is necessary for a specific purpose.

5.2. Order and eSIM information

When you purchase an eSIM, we may process:

- your email address;
- internal order number;
- purchased destination, region or coverage area;
- eSIM package or tariff identifier;
- data allowance and validity period;
- date and time of purchase;
- price, currency and payment status;
- eSIM delivery and activation status;
- order history;
- information relating to the technical status of an eSIM;
- refund or cancellation information.

5.3. Payment information

When you pay using Stripe payment system, we may receive:

- your email address;
- transaction identifier;
- payment status;
- amount and currency;
- payment date;
- limited payment-method information, such as card brand and the final digits of the card number;
- information necessary to manage refunds, disputes or fraud prevention.

We do not receive or store your full payment-card number, card security code or complete banking credentials.

When you pay using cryptocurrency, we may process:

- transaction identifier or blockchain transaction hash;
- wallet address;
- cryptocurrency type;
- amount;
- payment status;
- date and time of payment;
- information provided by the applicable cryptocurrency payment processor.

Blockchain transactions may be publicly visible and cannot generally be deleted or altered by us.

5.4. Customer-support information

When you contact us through email, Telegram or another support channel, we may process:

- your email address, where provided;
- your name, display name or username;
- Telegram username or Telegram identifier;
- message content and correspondence history;
- order and eSIM information;
- screenshots, files or other attachments;
- technical information supplied by you;
- date and time of the communication;
- information required to investigate an eSIM or connectivity issue.

You may initially use the Chatra support service without providing an email address.

However, if a matter requires further investigation, preservation of correspondence or identification of an order, we may ask you to provide the email address associated with your Account.

Please do not send passport details, full payment-card details, health information or other unnecessary sensitive information through customer-support channels.

5.5. Telegram information

When you use our Telegram bot or contact us through Telegram, Telegram may provide us with information associated with your account, such as:

- Telegram user identifier;
- username;
- display name;
- profile image, where made available;
- language setting;
- messages and commands sent to the bot;
- order and interaction history within the bot.

Telegram independently processes personal data under its own terms and privacy policy.

5.6. Website and device information

When you visit or use our website or application, we may process:

- IP address;
- browser type and version;
- device type;
- operating system;
- device and browser identifiers;
- language and time-zone settings;
- approximate geographical location derived from network information;
- pages viewed;
- referring website or source;
- date, time and duration of visits;
- clicks, navigation and interactions with website elements;
- error logs and diagnostic data;
- authentication and session information;
- cookie and similar technology identifiers.

5.7. Information from third parties

We may receive information from:

- Stripe;
- cryptocurrency payment processors;
- eSIM suppliers;
- mobile network or connectivity providers;
- Telegram;
- Apple;
- Chatra;
- analytics providers;
- fraud-prevention or security providers.

The information received is limited to what is reasonably necessary for the relevant purpose.

5.8. Special-category personal data

We do not intentionally collect special-category personal data, such as information concerning:

- health;
- racial or ethnic origin;
- political opinions;
- religious beliefs;
- sexual orientation;
- trade-union membership;
- genetic or biometric data.

Please do not provide such information unless we specifically request it and have a lawful basis for processing it.

6. How We Collect Personal Data

We collect personal data:

- directly from you when you register, purchase a Service or contact us;
- automatically when you use our website, application or online services;
- from payment providers when a transaction is processed;
- from Telegram when you interact with our Telegram bot;
- from eSIM suppliers and connectivity providers;
- from analytics and technical service providers;
- from publicly available blockchain records in connection with cryptocurrency payments.

7. How We Use Personal Data and Our Legal Bases

We process personal data only where we have a valid legal basis.

7.1. Account registration and administration

Purposes	• creating and maintaining your Account; • authenticating you; • enabling access to purchases and order history; • managing Account security; • allowing you to update or delete your Account.
Data used	• email address; • Account identifier; • registration data; • optional profile information; • authentication and session information.
Legal basis	• performance of a contract; • steps taken at your request before entering into a contract; • our legitimate interest in securing and administering our Services.

7.2 Processing and fulfilling orders

Purposes	• processing your purchase; • providing and delivering an eSIM; • displaying your order history; • managing activation and technical status; • communicating about your order; • fulfilling our contractual obligations.
Data used	• email address; • order details; • eSIM details; • payment status; • technical and delivery information.
Legal basis	• performance of a contract; • compliance with legal obligations.

7.3 Processing payments

Purposes	• receiving payments; • verifying transaction status; • preventing duplicate or fraudulent payments; • processing refunds; • managing disputes and chargebacks; • maintaining financial records.

Data used	• email address; • transaction identifiers; • payment status; • amount and currency; • limited payment-method information; • cryptocurrency wallet and blockchain transaction information.
Legal basis	• performance of a contract; • compliance with legal obligations; • our legitimate interests in preventing fraud and protecting our financial interests.

7.4 Providing customer support

Purposes	• responding to questions; • resolving technical issues; • checking the status of an eSIM; • investigating connectivity or activation problems; • processing complaints and refund requests; • maintaining support records.
Data used	• contact information; • message content; • support history; • order and eSIM information; • attachments; • technical and diagnostic information.
Legal basis	• performance of a contract; • our legitimate interests in providing effective customer service, resolving disputes and improving our Services.

7.5 Security and fraud prevention

Purposes	• protecting Accounts and systems; • detecting unauthorised access; • preventing fraud, abuse and malicious activity; • enforcing our Terms and Conditions; • investigating suspected violations.
Data used	• Account information; • transaction information; • device and browser data; • security logs; • IP address; • order and support history.
Legal basis	• our legitimate interests in protecting our users, systems, business and legal rights; • compliance with legal obligations.

Where we rely on legitimate interests, we assess whether the processing is necessary and whether your rights and interests override our interests

7.6 Website analytics and improvement

Purposes	• understanding how users interact with our website; • measuring website performance; • identifying errors and usability problems; • improving content, navigation and user experience; • producing statistical reports.
Data used	• cookie identifiers; • device and browser information; • IP and approximate location information; • pages viewed; • traffic source; • date, time and duration of visits; • interactions with website elements.
Legal basis	• your consent.

We use analytics technologies only in accordance with your cookie choices.

7.7 Service communications

We may send transactional or service-related communications, including:

- Account registration messages;
- login or security messages;
- order confirmations;
- eSIM delivery information;
- activation or usage notifications;
- password-reset messages;
- refund information;
- responses to support requests;
- important changes affecting a purchased Service.

Legal basis:

- performance of a contract;
- our legitimate interests in administering and securing our Services;
- compliance with legal obligations.

These messages are not marketing communications.

7.8 Marketing communications

We do not currently send regular marketing emails.

If we introduce marketing communications in the future, we may send news, offers or promotional information only where:

- you have given valid consent; or
- another lawful basis is available under applicable law.

You will be able to withdraw your consent or unsubscribe at any time.

Legal basis:

- consent, where required;
- legitimate interests only where permitted by applicable law.

7.9 Legal compliance and claims

Purposes:

- complying with legal and regulatory obligations;
- responding to lawful requests;
- maintaining accounting and transaction records;
- establishing, exercising or defending legal claims;
- resolving disputes.

Legal basis:

- compliance with legal obligations;
- our legitimate interests in protecting and enforcing our legal rights.

8. Cookies and Similar Technologies

We use cookies and similar technologies on our website.

Cookies are small text files or identifiers stored on or accessed from your device.

8.1. Categories of cookies

We may use:

Strictly necessary cookies

These are required for essential functions, including:

- Account login;
- authentication;
- security;
- session management;
- shopping and payment functionality;
- remembering privacy choices.

These cookies cannot normally be disabled through our cookie settings because the website may not function properly without them.

Analytics cookies

These help us understand how visitors use our website and improve its performance.

Analytics cookies are activated only after you provide consent through our cookie banner or consent-management tool.

Functional cookies

These may remember preferences such as language, region or display settings.

Marketing cookies

We do not currently use cookies for targeted advertising unless this is expressly disclosed through our cookie settings.

8.2. Cookie consent

When you first visit our website, you are presented with options to:

- accept optional cookies;
- reject optional cookies;
- manage cookie preferences.

Rejecting optional cookies does not prevent you from purchasing or using our core Services.

You may withdraw or change your consent at any time through the cookie settings available on our website.

9. Yandex Metrica

We use **Yandex Metrica** to analyse website usage and improve the performance and usability of our Services.

Subject to your consent, Yandex Metrica may process:

- cookie and visitor identifiers;
- IP address and approximate location;
- browser and device information;
- operating system;
- page views;
- referring source;
- date, time and duration of visits;
- clicks, scrolling and interaction information;
- technical and diagnostic information.

Yandex Metrica is used on our website language versions as configured by us.

We configure Yandex Metrica in accordance with available privacy and data-protection settings. Yandex requires website operators to inform users about cookies and the use of Metrica and provides a data-processing agreement for website owners.

Yandex may process data outside the United Kingdom and the European Economic Area. Further information is provided in the section on international transfers.

10. Google Analytics

We use **Google Analytics** on non-Russian-language versions of our website.

Subject to your consent, Google Analytics may process:

- cookie and device identifiers;
- IP address and approximate location;
- browser and operating-system information;
- traffic source;
- pages viewed;
- date, time and duration of visits;
- user interactions and technical events.

Google Analytics is used to create aggregated reports about how our Services are used.

We configure Google Analytics to respect users' cookie choices.

We intend to use a consent-management system and Google Consent Mode so that Google receives and respects the consent status selected by the user. In basic consent mode, Google tags can be blocked until the user interacts with the consent banner and grants permission

11. Payment Providers

11.1. Stripe

We use Stripe to process card payments.

Stripe may process:

- email address;
- cardholder and billing information entered through Stripe;
- payment-card information;
- transaction and fraud-prevention data;
- IP address and device information.

Stripe processes certain information as an independent controller under its own privacy documentation and may also process information on our behalf.

11.2. Cryptocurrency payments

We may use one or more third-party cryptocurrency payment providers.

These providers may process:

- wallet address;
- transaction identifier;
- payment amount;
- cryptocurrency type;
- email address, where required;
- compliance or fraud-prevention information.

The identity of the relevant cryptocurrency payment provider will be displayed during payment or otherwise made available to you.

Cryptocurrency transactions may also be recorded permanently on a public blockchain.

12. Chatra and Customer Support

We use Chatra to provide live-chat support through our website and mobile application.

Chatra may process:

- chat messages;
- email address, if provided;
- name or display name, if provided;
- browser and device information;
- page from which the chat was initiated;
- date and time of communication;
- attachments;
- chat identifiers and history.

Users may initially contact us anonymously through Chatra.

Where an issue requires detailed investigation, we may ask for the email address associated with the Account so that we can identify the relevant order, preserve the conversation or review the technical status of an eSIM.

13. Telegram

We use Telegram to provide access to a Telegram bot and customer-support services.

Telegram is an independent third-party platform. When you use Telegram, Telegram processes your information according to its own privacy policy and terms.

Information made available to us may include:

- Telegram identifier;
- username;
- display name;
- profile image;
- language;
- messages;
- commands;
- order or interaction history within the bot.

You should review Telegram's privacy settings before using the Telegram bot.

14. Hosting and Infrastructure

For users covered by this Privacy Policy, our main website infrastructure and databases are hosted in France through **OVH** or associated OVH infrastructure.

OVH may process technical information necessary to provide hosting, security, storage, network and backup services.

We may also use:

- SMTP and email-delivery providers;
- infrastructure administrators;
- backup providers;
- security and monitoring providers.

Where these providers process personal data on our behalf, we require them to process it only for agreed purposes and to apply appropriate security measures.

15. eSIM and Connectivity Providers

We work with third-party eSIM suppliers and telecommunications or connectivity providers.

We may disclose limited information to these providers where necessary to:

- create or deliver an eSIM;
- verify eSIM status;
- provide connectivity;
- investigate a technical problem;
- replace or disable an eSIM;
- resolve a support request.

We aim not to disclose your email address to an eSIM provider unless it is necessary for the relevant Service or technical investigation.

Mobile network operators may independently process technical and network information when you connect to their networks.

16. Who We Share Personal Data With

We may share personal data with:

- OVH and other hosting or infrastructure providers;
- Stripe;
- cryptocurrency payment providers;
- Chatra;
- Telegram;
- Google Analytics;
- Yandex Metrica;
- email and SMTP providers;
- eSIM suppliers;
- mobile network and connectivity providers;

- Apple, where you use our iOS application;
- technical, security and fraud-prevention providers;
- accountants, auditors, lawyers and professional advisers;
- regulatory, law-enforcement or public authorities where legally required;
- a purchaser, investor or successor in connection with a merger, restructuring or sale of the business.

We do not sell personal data.

We require processors acting on our behalf to comply with contractual obligations concerning confidentiality, security and permitted processing.

17. International Transfers

Our main infrastructure for users covered by this Privacy Policy is located in France.

However, some service providers may process personal data in countries outside the United Kingdom or the European Economic Area.

These providers may include:

- Yandex;
- Google;
- Stripe;
- Chatra;
- Telegram;
- cryptocurrency payment providers;
- eSIM and connectivity providers;
- technical or support service providers.

Where a transfer is subject to the UK GDPR or EU GDPR, we use an appropriate legal transfer mechanism where required, which may include:

- a finding of adequacy by the United Kingdom or European Commission;
- the European Commission's Standard Contractual Clauses;
- the UK International Data Transfer Agreement;
- the UK Addendum to the European Commission's Standard Contractual Clauses;
- another legally permitted safeguard or exception.

Where required, we assess the circumstances of the transfer and the legal and technical protections available.

You may contact us for further information about the safeguards relevant to a particular transfer.

18. Data Retention

We retain personal data only for as long as reasonably necessary for the purposes described in this Privacy Policy, including to comply with legal, accounting and reporting requirements.

Typical retention periods are as follows:

Category	Typical retention period
Active Account information	Until Account deletion or termination
Deleted Account information	Deleted or anonymised within a reasonable period, subject to legal retention requirements
Order and eSIM history	For the duration of the Account and thereafter where required for legal, tax, accounting or dispute purposes
Payment and financial records	Usually up to 6 years, or longer where required by applicable law
Customer-support correspondence	Usually up to 3 years after resolution, unless longer retention is required for a dispute
Fraud and security records	For as long as necessary to protect the Services and manage legal risk
Cookie consent records	For the period necessary to demonstrate and manage consent
Analytics data	According to the configured retention periods of the relevant analytics provider
Marketing consent	Until withdrawal of consent, plus a limited suppression record where necessary

We may retain information for longer where:

- required by law;
- necessary for an active complaint, dispute or legal claim;
- necessary to investigate fraud, abuse or security incidents;
- deletion would interfere with the rights of another person.

When personal data is no longer required, we delete or anonymise it.

19. Data Security

We use appropriate technical and organisational measures designed to protect personal data.

These measures may include:

- encryption in transit using HTTPS or similar technologies;
- restricted access to systems and databases;
- authentication and password controls;
- access permissions based on operational need;
- encrypted or protected storage where appropriate;
- regular software updates;
- backups;
- monitoring and logging;
- incident-response procedures;

- confidentiality obligations;
- security requirements for service providers.

No online service can guarantee absolute security.

You are responsible for keeping your Account credentials confidential and for informing us if you suspect unauthorised access.

20. Personal Data Breaches

If we become aware of a personal-data breach, we will investigate it and take reasonable steps to contain and remedy the incident.

Where required by applicable law, we will notify:

- the relevant supervisory authority; and
- affected individuals where the breach is likely to result in a high risk to their rights and freedoms.

21. Your Data Protection Rights

Depending on your location and the applicable law, you may have the following rights:

21.1. Right to be informed

You have the right to receive clear information about how your personal data is used.

21.2. Right of access

You may request confirmation of whether we process your personal data and obtain a copy of it.

21.3. Right to rectification

You may ask us to correct inaccurate or incomplete personal data.

21.4. Right to erasure

You may ask us to delete your personal data in certain circumstances.

This right is not absolute. We may retain information where necessary to comply with law, maintain financial records, prevent fraud or establish or defend legal claims.

21.5. Right to restriction

You may ask us to restrict processing in certain circumstances.

21.6. Right to data portability

Where processing is based on consent or contract and carried out by automated means, you may request certain personal data in a structured, commonly used and machine-readable format.

21.7.Right to object

You may object to processing based on legitimate interests.

You may object at any time to processing for direct-marketing purposes.

21.8.Right to withdraw consent

Where we rely on consent, you may withdraw it at any time.

Withdrawal does not affect the lawfulness of processing carried out before consent was withdrawn.

21.9.Rights relating to automated decisions

You have the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects, except where permitted by law.

The principal GDPR rights include access, rectification, erasure, restriction, portability, objection and protection from certain solely automated decisions.

22. Exercising Your Rights

To exercise your rights, contact:

Email: hello@fedafone.com

Please provide enough information to allow us to identify you and understand your request.

We may ask for reasonable proof of identity before responding.

We normally respond without undue delay and within one month.

Where permitted by law, this period may be extended by up to two further months where a request is complex or numerous. We will inform you if an extension is necessary.

Requests are normally free of charge.

We may charge a reasonable fee or refuse to act where a request is manifestly unfounded or excessive, where permitted by law.

23. Account Deletion

You may delete your Account using the Account settings where this function is available, or by contacting us.

Following Account deletion:

- access to your Account and order history may end;
- Account data will be deleted or anonymised within a reasonable period;
- certain transaction, tax, fraud-prevention, support or dispute records may be retained where legally necessary.

Deleting an Account does not automatically remove information held independently by third parties, including Stripe, Telegram, blockchain networks or other service providers.

24. Automated Decision-Making and Profiling

We do not normally make decisions about users based solely on automated processing where those decisions produce legal or similarly significant effects.

Automated systems may be used for:

- payment processing;
- fraud detection;
- security monitoring;
- routing support requests;
- website analytics;
- delivery of eSIM services.

Where a solely automated decision with a significant effect is used, we will provide the information and protections required by applicable law.

Use of a Telegram bot to execute user commands does not necessarily constitute significant automated decision-making.

25. Children's Privacy

Our Services are not specifically directed at children.

You must be legally capable of entering into a contract or have the permission of a parent or legal guardian to use the Services.

We do not knowingly collect personal data from children in circumstances where parental consent is required.

If you believe that a child has provided personal data without appropriate permission, please contact us.

26. Third-Party Links and Services

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

We are not responsible for the privacy practices of third parties.

You should review the privacy policy of each third-party service before providing personal data.

27. Complaints

Please contact us first if you have concerns about how we process your personal data.

You also have the right to complain to a supervisory authority.

For the United Kingdom, the supervisory authority is the:

Information Commissioner's Office

Users in the European Economic Area may also complain to the data-protection authority in the country where they live, work or where the alleged infringement occurred.

28. Data Protection Officer

We have not appointed a formal Data Protection Officer because we do not currently consider that our processing activities require one under applicable data protection law.

Questions relating to privacy and data protection may be sent to:

hello@fedafone.com

29. Changes to This Privacy Policy

We may update this Privacy Policy when:

- our Services change;
- we introduce new providers or technologies;
- legal requirements change;
- our processing activities change.

The updated version will be published on our website with a new "Last updated" date.

Where changes materially affect your rights or how we use personal data, we may provide additional notice through the website, application or email.

30. Contact Us

For questions about this Privacy Policy or our use of personal data, contact:

FEDAFONE LTD
Company number: 15111795
2nd Floor, College House
17 King Edwards Road
Ruislip, HA4 7AE
United Kingdom

Email: hello@fedafone.com
Website: www.fedafone.com