Jetsense Privacy Policy

1. Definitions and Scope

1.1. This Privacy Policy (the “Policy”) sets out the rules for processing personal data of users of the Jetsense platform (the web terminal, hereinafter the “Platform”). “Personal data” means any information relating to an identified or identifiable natural person (“user” or “you”), directly or indirectly. “Processing” means any operation or set of operations performed on personal data, such as collection, recording, structuring, storage, use, transfer, anonymisation and deletion.

1.2. The controller (operator) of personal data collected through the Platform is Top Trading Solutions Inc., Republic of Panama (the “Company”, “we”, “us”). The Policy applies to all users of the Platform, regardless of their country of residence, and to all data collected when you use the service and interact with us through the available channels. We comply with applicable data protection laws, including but not limited to the principles of the EU General Data Protection Regulation (GDPR), as well as generally accepted international privacy standards and principles.

1.3. This Policy governs only the data processing carried out directly by the Company in connection with the use of the Platform. It does not apply to third-party websites, services and exchanges which you may access via links from our Platform or which you use to execute transactions through the Platform. Such third-party resources operate independently and have their own privacy policies. We do not control how these third parties process data and we recommend that you review their rules before providing any data to them.

1.4. By continuing to use the Platform, you confirm that you have read this Policy and agree to its terms. If you do not agree with any of its provisions, please stop using the Platform.

2. Data Controller and Contact Information

2.1. The controller of your personal data (i.e. the person that determines the purposes and means of processing) is Top Trading Solutions Inc., registered in the Republic of Panama.

2.2. If you have any questions regarding this Policy or the processing of your personal data, you can contact us by sending an email to the following address:

support@jetsense.io

2.3. Privacy-related enquiries are handled by the Company promptly and in accordance with legal requirements. We value the trust of our users and make every effort to address any issues related to personal data processing in a professional manner.

3. Categories of Data Collected

3.1. In the course of Jetsense’s operations, we collect and process the following main categories of personal data:

3.1.1. Information you provide when registering and using your account.

This includes your email address and your Telegram username. This data is used to create and maintain your account, to authenticate you when you log in, and to communicate with you (for example, to send notifications or support responses). It may also be used to send you product-related messages about new features, capabilities and updates of the Platform, but only if you have previously consented to receiving such communications. You can withdraw your consent and unsubscribe at any time in your account settings or via the unsubscribe links in the emails.

3.1.2. Exchange API keys and technical identifiers.

To execute trading operations, you may provide unique API keys or access tokens to your exchange accounts. This data is used solely to communicate with exchanges on your behalf and is stored in encrypted form in accordance with the established security measures.

3.1.3. Technical data about your device and connection.

This is information that is collected automatically when you access the Platform. It may include:

– IP address of your device;

– browser type and version;

– operating system;

– language settings and time zone;

– screen resolution;

– unique device or browser identifiers (for example, cookies or mobile device IDs).

We may also collect information about your activity on the Platform:

– dates and times of visits;

– pages or sections viewed;

– clicks on interface elements;

– volume of transmitted data;

– actions in the interface (for example, opening specific tools);

– application errors and crashes.

This technical data helps us ensure the proper operation of the service, adapt the interface to your device and detect issues.

3.1.4. Authentication and security data.

Unique identifiers, tokens and other data necessary for logging into your account and protecting access. For example, when you sign in via a third-party provider (Privy), an access token is generated and stored as a cookie or in your browser's localStorage to maintain your session. We also store in localStorage a certain digital "fingerprint" of your device, which allows us to recognise your device on subsequent logins. This supports additional checks during authentication (for example, if a login attempt occurs from a new device, the system will detect this).

3.1.5. Cookie and localStorage data.

To operate the Platform, we use browser cookies (small text files) and the browser's local storage (localStorage). A more detailed description of the cookies and localStorage data we use is provided in section 5 of this Policy.

3.1.6. Information you provide voluntarily.

In addition to the above, we may process any additional data you provide to us. This may include data from correspondence with support (for example, an additional contact email), responses to surveys, comments and feedback. We will use such information only for the purposes for which you provided it (for example, to respond to your request or to take your feedback into account when improving the service).

3.1.7. Anonymised and aggregated data.

We may also create aggregated statistics based on the use of the Platform. Such information does not contain data that can identify you and is used, for example, to analyse system load (such as the number of active users at a particular time of day) or the performance of new features. Aggregated data does not fall under personal data laws. However, if we combine it with your personal data in a way that makes you identifiable, we will treat such combined information as personal data.

3.2. We do not knowingly collect sensitive personal data ("special categories" of personal data), such as information about race or ethnic origin, political opinions, religious or philosophical beliefs, health, biometric or genetic data, sexual life or sexual orientation. We also do not request or process personal data considered sensitive under the laws of certain countries (for example, social security numbers, data on trade union membership, etc.). The Platform does not require such data. Please refrain from providing us with unnecessary personal information. If we accidentally receive such data (for example, if you include sensitive information in a support request), we will delete it and will not use it for any purpose other than responding to your specific request.

3.3. We do not collect or process your payment instrument details, such as bank card data, account numbers, security codes (CVV/CVC) or similar information, nor do we collect sensitive data of cryptocurrency wallets (seed phrases, private keys or other data that allow disposal of funds).

4. Purposes of Data Processing

4.1. We process your personal data exclusively for lawful purposes and ensure an appropriate legal basis for each processing operation in accordance with applicable law, including Article 6 of the GDPR.

4.2. The table in the Russian original describes, for each purpose of processing:

– which categories of data are used;

– why they are necessary;

– and on what legal basis processing is carried out (performance of a contract, legal obligation, legitimate interests, consent).

4.3. We do not use your personal data for purposes incompatible with those listed above, and we do not begin processing for a new purpose without obtaining your prior consent or another valid legal basis. If in the future we need to process data for a purpose not mentioned in this Policy, we will notify you in advance and, where required by law, request your consent.

5. Cookies and Local Storage

5.1. For the operation of Jetsense and to improve your user experience, we use cookies and the browser's local storage (localStorage).

5.1.1. A cookie is a small file that your browser stores on your device at the request of our server.

5.1.2. LocalStorage is a mechanism for storing data in the browser that is kept locally and is accessible through scripts on the page. Both mechanisms are important for web applications.

5.2. Storage technologies used

We may use, in particular, the following technologies (names as in the Russian original):

– session_token (cookie, strictly necessary):

Session identifier used to maintain your login. Without it, an authenticated session cannot be maintained.

– cm.assigned.564f5328… (localStorage, strictly necessary):

Technical key of the authentication provider Privy for managing access.

– print (localStorage, strictly necessary):

Unique device "fingerprint" for recognising known devices and ensuring security.

– tv.layout.tab-1.1, tv.logger.* and other TradingView keys (localStorage, functional):

Store your chart settings and widget parameters between sessions.

– registration_utm (localStorage, analytical/marketing):

Stores information about how you arrived at our Platform (used once at registration to analyse acquisition channels).

5.3. When you first visit Jetsense, a cookie notice is displayed, allowing you to accept cookies or configure them.

5.4. You can:

– refuse non-essential cookies via your browser settings;

– clear localStorage using your browser's developer tools;

– email us at support@jetsense.io for help with withdrawing your consent.

6. User Rights and How to Exercise Them

6.1. In accordance with applicable data protection laws, you, as a data subject, have a number of rights designed to give you control over your personal data. We provide mechanisms for exercising these rights and value your involvement in data protection matters. Below we list your main rights and explain how you can exercise them:

6.1.1. Right of access (right to know).

You can request confirmation as to whether we process your personal data and obtain a copy of the data we hold about you. In addition to the data itself, you have the right to request information about the purposes of processing, the sources from which your data was obtained, the third parties to whom data is disclosed, the retention periods, as well as other information required by law. We will provide this information in an understandable form, usually electronically.

6.1.2. Right to rectification (correction).

If any of your personal data held by us is inaccurate, incomplete or outdated, you have the right to request that it be rectified or updated. Some data can be updated directly through the Platform interface (where such functionality is available).

6.1.3. Right to erasure ("right to be forgotten").

You can request the deletion of your personal data that we process if certain conditions are met. This right is not absolute: the law provides for situations where we may refuse deletion (for example, if the data is necessary to perform a contract with you, or we are legally obliged to retain it). However, in most cases, when you request the deletion of your account and data, we will delete it. We will assess your request against the legal criteria and either comply or provide a reasoned refusal.

6.1.4. Right to restriction of processing.

Instead of full deletion, you have the right to request that we restrict processing of your data in certain cases. Restriction means that we will store the data but will not carry out with it any operations (other than storage) without your consent.

6.1.5. Right to data portability.

This is the right to receive your personal data in a structured, commonly used and machine-readable format and (where technically feasible) to transmit it to another service provider. It applies only to data that you provided to us yourself and that is processed by automated means on the basis of your consent or a contract with you. Exercising the right to portability does not automatically mean deletion of your data from our systems.

6.1.6. Right to object to processing.

You have the right to object at any time to the processing of your personal data where such processing is based on our legitimate interests. In that case, we must cease processing unless we demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or the data is needed to establish, exercise or defend legal claims. You also have an absolute right to object to processing of your data for direct marketing purposes – in such case we will immediately stop using your data for that purpose.

6.1.7. Right to withdraw consent.

If we process any of your personal data based on consent, you may withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

6.1.8. Right not to be subject to automated decision-making.

You have the right not to be subject to a decision based solely on automated processing, including profiling, if such decision produces legal effects concerning you or similarly significantly affects you. We do not use such practices – decisions on blocking or restricting an account in Jetsense are made with the involvement of responsible staff, not solely by algorithms.

6.2. To exercise any of the above rights, please contact us in any convenient way, preferably by email at support@jetsense.io. In your request, please describe which right you wish to exercise and provide information that will help us verify your identity. We must make sure that the request comes from you (or your authorised representative), so that we do not disclose your data to third parties.

6.3. After receiving your request, we typically:

– confirm receipt of the request (within a few days);

– clarify details if necessary (if it is not entirely clear which data or operation you are requesting);

– fulfil the request or provide a reasoned refusal (if there are legal grounds to refuse).

6.4. The time limit for responding to data subject requests is up to 1 month from the date of receipt. Where necessary, this period may be extended by up to 2 additional months, in which case we will notify you in advance and explain the reasons for the extension.

6.5. If you have concerns that your data is being processed unlawfully or that your rights have been violated, you have the right to lodge a complaint with the competent data protection authority. We would appreciate it if you first contact us directly, but this is your legal choice.

7. Data Disclosure to Third Parties

7.1. We do not sell or transfer your personal data to third parties for their own marketing purposes. Data disclosure occurs only in the cases described below and subject to appropriate safeguards.

7.2. We engage trusted service providers to operate the Platform. All such processors act on our instructions and are bound by data protection agreements, including in particular:

– hosting and cloud infrastructure (data storage, backups);

– authentication services (Privy – processing data for logging into your account);

– communication platforms (delivery of email and push notifications);

– security services (DDoS protection, monitoring).

7.3. When you connect an exchange account, you authorise us to transmit data to the exchange via API solely to execute your trading operations, including:

– API keys and identifiers for authorisation;

– trade parameters (instrument, size, price, etc.).

Exchanges are independent data controllers and apply their own privacy rules.

7.4. We may disclose data in the following cases:

– to affiliated entities – for administrative purposes, subject to this Policy;

– to professional advisors (lawyers, auditors) – under confidentiality obligations;

– where required by law – upon receipt of a lawful request from public authorities;

– in the context of corporate transactions (mergers, acquisitions, etc.), with notice to users and with continuity of data protection.

7.5. All third parties are required to ensure the confidentiality and security of the data. We only transfer the minimum amount of information necessary for the relevant purpose.

8. Cross-Border Data Transfers

8.1. Jetsense operates globally, and your data may be processed in other countries, including those that may not provide an adequate level of protection according to the legislation of your jurisdiction.

8.2. In such cases, the Company takes necessary measures to protect the data, including entering into contracts with recipients in accordance with applicable law. In particular, we may rely on:

– EU Standard Contractual Clauses (SCC);

– contracts with service providers that require appropriate data protection;

– technical and organisational security measures.

8.3. By continuing to use Jetsense, you consent to such cross-border transfer of data, provided that the measures described above are applied.

9. Security Measures

9.1. We implement comprehensive technical and organisational security measures to protect your personal data against unauthorised access, loss or disclosure. The level of protection is proportionate to the nature of the data processed and current risks.

9.2. Key protection measures include, but are not limited to:

– encryption of data: transmission of data via TLS/SSL; storage of critical data in encrypted form;

– access control: role-based access for employees on a need-to-know basis, multi-factor authentication;

– network segmentation: isolation of production environments, protection of databases by firewalls;

– threat monitoring and detection: logging of events, systems for monitoring activity;

– vulnerability management: regular software updates, vulnerability scanning, penetration testing;

– incident response plan: procedures in case of data breaches, including notification of regulators and affected users;

– employee training: security briefings, confidentiality agreements.

9.3. Despite the measures taken, absolute security cannot be guaranteed. We also recommend that you act prudently: keep your login credentials confidential, use strong passwords and keep your software up to date.

10. Data Retention Periods

10.1. We retain personal data for no longer than is necessary to achieve the purposes for which it was collected, unless a longer period is required by law. Once the purpose has been fulfilled, the data is deleted or anonymised.

10.2. Retention periods may vary by category of data (account data, API keys, logs, correspondence, backups, etc.) as described in the Russian original. In general:

– account data is stored while your account is active and for a short period thereafter;

– technical logs and activity journals are stored for a limited time necessary for security and diagnostics;

– backup copies are stored for a limited period and then overwritten.

10.3. Special cases and exceptions

10.3.1. Legal obligations.

Data that must be retained by law is stored for the period established by applicable legislation (usually 3–10 years).

10.3.2. Security incidents.

Data related to incident investigations may be stored for a longer period, for the duration of the investigation and any related proceedings.

10.3.3. Anonymised data.

Anonymised data may be stored without limitation, as it does not allow identification of specific individuals.

10.4. After the expiry of retention periods, data is removed from active systems. Deletion from backups occurs within the timeframe of overwrite cycles.

11. Protection of Children's Data

11.1. The Jetsense Platform is intended only for users who are at least 18 years old and/or have reached the age of majority in their jurisdiction (if applicable law sets a higher age). We do not intend to collect or process personal data of individuals who do not meet these requirements.

11.2. By registering, you confirm and warrant that:

– you are at least 18 years old;

– you have reached the age of majority in your jurisdiction (if it exceeds 18 years);

– you have full legal capacity and the right to make independent decisions regarding the use of the Platform and the processing of your personal data.

11.3. We apply reasonable technical and organisational measures to prevent use of the Platform by underage persons. If we become aware that an account has been created by a person who does not meet the requirements set out in clause 11.1, we may immediately suspend or restrict access to that account and cease processing the related personal data, except where further processing is required to comply with legal obligations.

11.4. Responsibility for complying with age requirements and requirements related to financial capacity when performing trading operations lies with the users themselves and with the integrated exchanges through which such operations are executed.

12. Changes to This Policy

12.1. We may update this Policy from time to time in connection with changes in legislation, the launch of new features or the enhancement of security measures. When we update the Policy, we change the revision date and publish the new version on our website.

12.2. In the event of material changes affecting your rights, we will notify you by email or through a prominent notice in the Platform interface. Where required by law, we will obtain your separate consent.

12.3. Continued use of Jetsense after the Policy is updated constitutes your acceptance of the changes. If you do not agree with the new version, you must stop using the Platform and exercise your right to have your data deleted.

12.4. The current version of the Policy is always available on our website. An archive of previous versions is available upon request to ensure transparency.

13. Contact Information

13.1. If you have questions, comments or complaints regarding this Privacy Policy or the processing of your data, please contact us.

13.2. You can reach us on data processing matters via the following channels:

– Email: support@jetsense.io (preferred method)

13.3. We aim to respond to all enquiries as quickly as possible:

– standard requests – within a few business days;

– complex requests, including requests to exercise your rights (section 6) – within 1 month;

– in particularly complex cases, the period may be extended by up to 2 months, in which case we will inform you of the reasons for the delay.

13.4. For faster processing, we recommend using email. When contacting us, please indicate the nature of your request in the subject line (for example, “Request for data deletion”, “Question about the Policy”, etc.).

13.5. If your enquiry requires additional verification, we may ask you to provide information to confirm your identity for security purposes.

Date of last update: 12/11/2025.