PRIVACY POLICY OF THE ZETA SIGNALS SERVICE

Effective date: [date]

Document version: 1.1

Service address: [domain address]

§ 1. General provisions

1. This Privacy Policy sets out the rules for processing personal data of users of the website operating under the name Zeta Signals, available at [domain address], hereinafter referred to as the "Service".

2. This Privacy Policy has been prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, hereinafter referred to as "GDPR", and applicable Polish laws on personal data protection and electronic services.

3. The Service is a SaaS platform providing access to analytical software and the Zeta Signals information panel.

4. Use of the Service may involve the processing of the User's personal data, in particular for account creation, login, subscription handling, Service security, fraud prevention, payment handling and compliance with the Controller's legal obligations.

5. The Controller exercises due care to protect Users' privacy and applies technical and organisational measures appropriate to the nature, scope, context and purposes of personal data processing.

6. The Controller does not sell Users' personal data. Personal data may be disclosed only to the extent necessary to provide the Service, process payments, ensure security, comply with legal obligations, establish or pursue claims, defend against claims, or based on a separate consent of the User.

§ 2. Personal data Controller

1. The Controller of Users' personal data is:

[Full Name]

contact address: [Residential/Contact Address]

e-mail address for personal data matters: support@zetasignals.pl

hereinafter referred to as the "Controller".

2. The Controller operates the Service as a natural person conducting non-registered activity under applicable Polish law.

3. In matters related to personal data protection, the User may contact the Controller via e-mail at: support@zetasignals.pl.

4. The Controller has not appointed a Data Protection Officer because, as of the effective date of this Privacy Policy, there is no legal obligation to appoint one. All personal data matters should be addressed directly to the Controller.

§ 3. Definitions

For the purposes of this Privacy Policy, the following terms have the meanings assigned below:

1. Controller - the entity indicated in § 2, determining the purposes and means of processing Users' personal data.

2. Personal Data - any information relating to an identified or identifiable natural person.

3. GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

4. Service - the Zeta Signals website available at [domain address].

5. User - a natural person using the Service, holding an account in the Service or purchasing a subscription.

6. Account - the individual User account created in the Service.

7. Subscription - paid access to selected Service features, in particular the analytical panel.

8. Supabase - the provider of database infrastructure and authentication system used by the Service.

9. Lemon Squeezy - an external payment operator and entity handling transactions, subscriptions, invoicing and transactional taxes in the Merchant of Record model.

10. Processor - an entity that processes personal data on behalf of the Controller under a data processing agreement or another appropriate legal instrument.

§ 4. Categories of personal data processed

1. The Controller may process the following categories of Users' personal data:

a) e-mail address,

b) Account password in a secured form, in particular hashed or otherwise technically secured,

c) User identifier in the Supabase system,

d) Account status information,

e) Subscription status information,

f) transaction or subscription identifier received from Lemon Squeezy,

g) Account creation date,

h) last login date,

i) IP address,

j) technical data of the device and browser,

k) system and security log data,

l) information on accepted document versions, in particular the Terms of Service, Privacy Policy, Cookie Policy, Risk Warning and consents required at purchase,

m) data concerning login attempts, technical activity and security events,

n) information on potential abuse, chargebacks, attempts to bypass security measures or unauthorised access,

o) correspondence content sent to the Controller if the User contacts the Controller.

2. The Controller does not intend to collect special categories of personal data referred to in Article 9 GDPR, in particular health data, political opinions, religious beliefs, biometric data or data concerning sexuality.

3. The User should not provide the Controller with special categories of personal data unless this is absolutely necessary in a specific matter and has been expressly agreed with the Controller.

4. The Service is not intended for persons under the age of 18. The Controller does not knowingly collect personal data of minors.

§ 5. Purposes and legal bases of processing

1. Users' personal data are processed for the following purposes and on the following legal bases:

1) Account creation and management

Scope of data: e-mail address, password in secured form, User identifier, technical data related to login.

Purpose: creating the Account, enabling login, managing access to the Service and providing the electronic service.

Legal basis: Article 6(1)(b) GDPR, i.e. processing necessary for the performance of a contract or to take steps prior to entering into a contract.

2) Subscription handling and access to paid features

Scope of data: e-mail address, User identifier, Subscription status, transaction identifier, customer or subscription identifier in Lemon Squeezy.

Purpose: activating the Subscription, verifying payment, managing access to paid Service features and handling the automatically renewing Subscription.

Legal basis: Article 6(1)(b) GDPR.

3) Payment handling through Lemon Squeezy

Scope of data: e-mail address, transaction data, order identifier, Subscription identifier, payment status, technical data necessary to link the payment to the User's Account.

Purpose: linking the payment to the User's Account, activating or deactivating access to paid Service features, handling refunds, chargebacks and settlements.

Legal basis: Article 6(1)(b) GDPR and Article 6(1)(f) GDPR, i.e. the Controller's legitimate interest in payment handling, fraud prevention and protection against claims.

4) Ensuring Service security

Scope of data: IP address, browser data, technical device data, system logs, login attempt data, timestamps, technical error data.

Purpose: ensuring Service security, detecting abuse, protecting against unauthorised access, protecting against attacks, diagnosing errors and ensuring Service stability.

Legal basis: Article 6(1)(f) GDPR, i.e. the Controller's legitimate interest in ensuring the security, integrity and stability of the Service.

5) Preventing fraud, abuse and unauthorised use of the Service

Scope of data: e-mail address, User identifier, IP address, system logs, technical device data, transaction data, Subscription history, information on chargebacks, suspicious login attempts, attempts to bypass security measures or unauthorised access to paid Service features.

Purpose: preventing abuse, payment fraud, chargebacks, attempts to bypass security measures, creation of multiple accounts to abuse the Service, unauthorised access to paid Service features and protecting the Controller and other Users.

Legal basis: Article 6(1)(f) GDPR, i.e. the Controller's legitimate interest in protecting the Service, payments, rights and claims of the Controller and preventing unlawful activities.

6) Handling requests, complaints and correspondence

Scope of data: e-mail address, message content, data voluntarily provided by the User, correspondence history.

Purpose: responding to inquiries, handling complaints, conducting correspondence, clarifying technical or payment issues.

Legal basis: Article 6(1)(b) GDPR if the correspondence concerns contract performance, or Article 6(1)(f) GDPR if the basis is the Controller's legitimate interest in handling contact and defending against claims.

7) Compliance with legal obligations

Scope of data: transaction data, settlement data, data necessary to document performance of the service, data required by law or authorised authorities.

Purpose: fulfilling obligations arising from legal provisions, in particular tax, accounting, consumer protection or personal data protection obligations.

Legal basis: Article 6(1)(c) GDPR.

8) Pursuing claims and defending against claims

Scope of data: Account data, transaction data, system logs, document acceptance history, Subscription history, correspondence, technical data.

Purpose: establishing, pursuing or defending against claims, including claims relating to payments, use of the Service, complaints, chargebacks, violations of the Terms of Service or legal disputes.

Legal basis: Article 6(1)(f) GDPR, i.e. the Controller's legitimate interest.

9) Documenting acceptance of terms, consents and statements

Scope of data: e-mail address, User identifier, date and time of acceptance, document version, IP address, user agent, transaction or Subscription identifier.

Purpose: demonstrating that the User read the relevant documents, accepted the required terms, received information on risk, subscription, withdrawal rights and rules of the Service.

Legal basis: Article 6(1)(b) GDPR and Article 6(1)(f) GDPR.

10) Technical, organisational and transactional communication

Scope of data: e-mail address, Account identifier, Account or Subscription status, information concerning security or changes to legal documents.

Purpose: sending messages necessary for contract performance, Account handling, payment handling, Service security, legal document changes or technical changes.

Legal basis: Article 6(1)(b) GDPR and Article 6(1)(f) GDPR.

§ 6. Minor Users

1. The Service is intended only for persons who are at least 18 years old and have full legal capacity.

2. The Controller does not knowingly collect personal data of minors.

3. If the Controller obtains credible information that an Account has been created by a minor, the Controller may delete the Account and data to the extent permitted by law and refuse to provide further services.

4. A parent, legal guardian or other authorised person may contact the Controller at support@zetasignals.pl if they have reasonable suspicion that a minor has provided personal data through the Service.

§ 7. Voluntary provision of data

1. Providing personal data is voluntary but necessary to create an Account, use the Service and purchase a Subscription.

2. Failure to provide an e-mail address or data required to create an Account prevents use of features requiring registration.

3. Failure to provide data required by Lemon Squeezy may prevent payment, issuance of a sales document or activation of the Subscription.

§ 8. Recipients of personal data

1. Users' personal data may be transferred or entrusted to the following categories of recipients:

a) technical infrastructure providers,

b) database and authentication service providers,

c) payment operators,

d) subscription management tool providers,

e) hosting, IT, security and technical monitoring providers,

f) legal, accounting or tax service providers if necessary,

g) public authorities, courts or other authorised entities where disclosure is required by law.

2. The Controller does not sell Users' personal data or transfer them to third parties in exchange for remuneration for the data itself.

3. The main external providers used by the Service are:

1) Supabase

1. The Service uses Supabase, in particular database infrastructure and Supabase Auth.

2. Supabase may process data such as e-mail address, password in secured form, User identifier, login data, technical data and data necessary for Account operation.

3. With respect to end-user data stored in the Service database or processed through Supabase Auth, Supabase generally acts as a processor processing data on behalf of the Controller.

4. With respect to the Controller's technical account data in Supabase, the Controller's billing data or data concerning the Controller's use of Supabase services, Supabase may act as a separate data controller.

5. The Controller should have a concluded or accepted data processing agreement with Supabase, in particular a Data Processing Addendum or equivalent document.

6. The Controller should periodically verify Supabase's subprocessor list and data processing region settings where such configuration is available under the relevant service plan.

2) Lemon Squeezy

1. The Service uses Lemon Squeezy as an external payment, subscription, invoicing and settlement operator in the Merchant of Record model.

2. Lemon Squeezy may receive the User's e-mail address and data necessary to link a transaction to the User's Account and activate the Subscription.

3. Lemon Squeezy may independently collect and process payment data, billing data, tax data, payment method data, IP address, device information and other data required for transaction handling, abuse prevention, chargeback handling, fraud detection and compliance with legal obligations.

4. To the extent Lemon Squeezy independently determines the purposes and means of processing, in particular regarding payments, taxes, invoicing, fraud prevention, chargebacks and legal obligations, it acts as a separate data controller.

5. With respect to certain technical or integration data processed for the operation of the Service, Lemon Squeezy may also act as a processor if this follows from the applicable agreement, documentation or service configuration.

6. Full payment card data are not stored by the Controller in the Service.

7. The Controller should periodically verify Lemon Squeezy's legal documents, in particular its privacy policy, Data Processing Agreement, Merchant of Record rules and lists of entities supporting data processing.

4. The Controller may also use other technical service providers if necessary for the proper operation of the Service, with data transferred only to the extent necessary for the relevant purpose.

§ 9. Transfers of data outside the European Economic Area

1. Due to the use of services such as Supabase and Lemon Squeezy, Users' personal data may be transferred to countries outside the European Economic Area, in particular to the United States.

2. Transfers outside the European Economic Area may take place only where the requirements set out in GDPR are met, in particular where:

a) the European Commission has issued an adequacy decision for the relevant country or entity,

b) standard contractual clauses approved by the European Commission have been applied,

c) a data processing agreement or another appropriate legal instrument has been applied,

d) other appropriate safeguards provided for in GDPR have been applied,

e) the transfer is permitted on another legal basis provided for in GDPR.

3. The Controller takes steps to ensure that external providers processing personal data apply appropriate legal, technical and organisational safeguards.

4. The Controller should verify whether external providers used, in particular Supabase and Lemon Squeezy, apply transfer mechanisms provided for in GDPR, such as adequacy decisions, standard contractual clauses, DPAs or equivalent documents.

5. The User may obtain additional information on the safeguards applied by contacting the Controller at support@zetasignals.pl.

§ 10. Data retention period

1. Personal data are stored for the period necessary to achieve the purposes for which they were collected, unless a longer retention period results from law or is justified by defence against claims.

2. The Controller applies the following general retention rules:

• Account data, in particular e-mail address and User identifier - for the period during which the User has an active Account in the Service;

• Subscription, transaction, payment and access status data - for the period required by law, settlement rules or the limitation period for potential claims;

• data concerning consents, document acceptances, document versions and User statements - for the duration of the Account and the limitation period for potential claims;

• correspondence data - for the period necessary to handle the matter and then for the limitation period for potential claims;

• technical and security logs - for the period necessary to ensure Service security, diagnose errors and detect abuse, generally no longer than 12 months, unless longer storage is necessary due to a security incident, dispute, complaint, chargeback, legal proceeding or legal obligation;

• data related to fraud prevention and abuse - for the period necessary for analysis, abuse prevention, chargeback handling, pursuing claims or defending against claims.

3. After Account deletion, the User's data are deleted or anonymised, subject to data that must be stored longer due to:

a) the Controller's legal obligations,

b) tax, accounting or settlement obligations,

c) the need to handle complaints,

d) the need to prevent abuse,

e) the need to establish, pursue or defend against claims.

4. If data are stored by third parties such as Supabase or Lemon Squeezy, their retention period may also result from the legal documents, retention policies, security requirements, payment, tax or settlement requirements of those entities.

§ 11. User rights

1. The User has the rights set out in GDPR, in particular:

a) the right of access to data,

b) the right to obtain a copy of data,

c) the right to rectification of data,

d) the right to erasure, also known as the right to be forgotten,

e) the right to restriction of processing,

f) the right to data portability,

g) the right to object to data processing,

h) the right to withdraw consent where processing is based on consent,

i) the right to lodge a complaint with a supervisory authority.

2. The right to erasure is not absolute. The Controller may refuse to delete data to the extent further processing is necessary to:

a) comply with a legal obligation,

b) establish, pursue or defend against claims,

c) handle complaints,

d) demonstrate performance of the contract,

e) comply with tax or settlement obligations,

f) prevent abuse or fraud, where further processing is lawful.

3. The right to data portability applies to data processed on the basis of contract or consent and by automated means.

4. The right to object applies where data are processed on the basis of the Controller's legitimate interest, for reasons related to the User's particular situation.

5. If data are processed for direct marketing purposes, the User may object at any time. After the objection is lodged, the data will no longer be processed for that purpose.

6. To exercise rights, the User may contact the Controller at support@zetasignals.pl.

7. The Controller may request additional information necessary to confirm the User's identity if there are reasonable doubts as to the identity of the person submitting the request.

8. The Controller responds to the request without undue delay and no later than within one month of receiving the request. If necessary, this period may be extended by a further two months due to the complexity or number of requests.

§ 12. Right to lodge a complaint with a supervisory authority

1. The User has the right to lodge a complaint with a supervisory authority if they believe that the processing of their personal data violates GDPR.

2. The supervisory authority in Poland is:

President of the Personal Data Protection Office

ul. Stawki 2

00-193 Warsaw

website: https://uodo.gov.pl

3. Before lodging a complaint, the User may contact the Controller to clarify the matter.

§ 13. Cookies and Local Storage

1. The Service uses cookies and similar technologies, including Local Storage, to ensure the proper operation of the Service.

2. Cookies and Local Storage may be used in particular to:

a) maintain the User's session,

b) enable Account login,

c) remember authentication status,

d) ensure Service security,

e) prevent abuse,

f) handle payments and Subscriptions,

g) detect technical errors,

h) protect against unauthorised access.

3. In the area of login and session handling, the Service may use technical mechanisms provided by Supabase Auth.

4. In the area of payment handling, financial abuse prevention, fraud prevention and transaction processing, cookies or similar technologies may be used by Lemon Squeezy or entities cooperating with Lemon Squeezy.

5. Detailed information on cookies, Local Storage, Session Storage and similar technologies is provided in the separate Cookie Policy of the Service.

§ 14. Automated decision-making and profiling

1. The Controller does not make decisions concerning Users based solely on automated processing of personal data that would produce legal effects concerning the User or similarly significantly affect the User.

2. The Service may automatically verify the User's Subscription status in order to grant or restrict access to paid Service features. This verification serves contract performance and is based on payment or Subscription status information.

3. Security mechanisms may automatically detect suspicious activities such as unusual login attempts, technical abuse, unauthorised access or attempts to bypass security measures.

4. Automatic verification of access to the Service does not constitute marketing profiling or assessment of the User's personal characteristics.

§ 15. Data security

1. The Controller applies appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction, alteration, disclosure or unlawful processing.

2. Security measures may include in particular:

a) use of encrypted HTTPS connection,

b) storage of passwords in a secured form, in particular hashed,

c) restriction of access to administrative panels,

d) use of strong passwords and access controls,

e) restricting data access only to persons and entities for whom it is necessary,

f) monitoring technical and security logs,

g) use of security measures of external providers such as Supabase and Lemon Squeezy,

h) backups where implemented within the infrastructure used,

i) periodic verification of administrative access and security settings,

j) limiting the scope of processed data to data necessary for specified purposes.

3. The User is obliged to keep Account login credentials confidential.

4. The User should use a strong, unique password and should not reuse the same password in other services.

5. If the Service provides two-factor authentication, the Controller recommends enabling it.

6. In the event of suspected unauthorised access to the Account, the User should immediately contact the Controller.

§ 16. Personal data breaches

1. In the event of a personal data breach, the Controller takes actions required by GDPR, in particular analyses the nature of the breach, its scope, possible consequences and risk to the rights or freedoms of natural persons.

2. If the breach is likely to result in a risk to the rights or freedoms of natural persons, the Controller will notify the competent supervisory authority in accordance with applicable law.

3. If the breach is likely to result in a high risk to the User's rights or freedoms, the Controller will notify the User of the breach in accordance with GDPR.

§ 17. Payment and billing data

1. Payments in the Service are handled by Lemon Squeezy.

2. The Controller does not process or store full payment card data of Users.

3. Payment data, billing data, tax data, payment method data, billing address and other data required for payment handling may be collected directly by Lemon Squeezy.

4. With respect to data collected directly by Lemon Squeezy, Lemon Squeezy's legal documents also apply, in particular its privacy policy, terms of service and data processing documents.

5. The Controller may receive from Lemon Squeezy information necessary to handle the Subscription, in particular e-mail address, customer identifier, transaction identifier, Subscription identifier, payment status and Subscription period.

6. Lemon Squeezy may process payment-related data for transaction processing, tax handling, invoicing, fraud prevention, chargeback handling and compliance with its own legal obligations as Merchant of Record.

§ 18. Links to external websites

1. The Service may contain links to websites or services of third parties, in particular Lemon Squeezy, Supabase or other technical service providers.

2. The Controller is not responsible for privacy practices applied by third parties outside the scope in which the Controller acts as the controller of the User's data.

3. The User should read the privacy policies of third parties before using their services.

§ 19. Marketing and commercial communication

1. The Controller may send the User technical, organisational and transactional messages concerning the operation of the Service, Account, Subscription, payments, security or changes to legal documents.

2. Technical and transactional messages do not constitute a newsletter or direct marketing if they are necessary to perform the contract or ensure proper operation of the Service.

3. Sending newsletters, marketing messages or commercial information not directly related to contract performance may take place only on the basis of separate consent of the User, if such consent is required by law.

4. The User may withdraw consent to receive marketing communication at any time if such communication is launched.

§ 20. Changes to the Privacy Policy

1. The Controller may amend this Privacy Policy in the event of:

a) changes in law,

b) changes in the operation of the Service,

c) changes in the scope of processed data,

d) changes in external service providers,

e) changes in Service features,

f) the need to clarify data processing rules,

g) implementation of new security measures or technical tools.

2. The new version of the Privacy Policy will be published in the Service.

3. If changes are material for Users' rights or freedoms, the Controller may also inform Users of the change by e-mail.

4. Use of the Service after the changes come into effect means that the current version of the Privacy Policy applies, subject to situations where a separate User consent is required.

§ 21. Contact

1. In matters concerning this Privacy Policy and personal data processing, please contact the Controller at: support@zetasignals.pl.

2. The correspondence should indicate what the request concerns and provide data enabling identification of the person submitting the request, in particular the e-mail address associated with the Account in the Service.

§ 22. Final provisions

1. This Privacy Policy applies from [date].

2. The Privacy Policy is available free of charge in the Service in a manner that allows it to be obtained, reproduced and stored.

3. In matters not regulated by this Privacy Policy, GDPR and applicable Polish law apply.

§ 23. Language versions

1. This Privacy Policy may be made available in Polish and English language versions.

2. The English language version is prepared for the convenience of Users using the English version of the Service. To the extent permitted by mandatory provisions of law, in the event of discrepancies between the Polish and English language versions, the Polish version shall prevail.