

COOKIE POLICY AND SIMILAR TECHNOLOGIES POLICY OF ZETA SIGNALS

Effective date: [date]

Document version: 1.1

Website address: [domain address]

§ 1. General provisions

1. This Cookie Policy and Similar Technologies Policy, hereinafter referred to as the "Cookie Policy", sets out the rules for using cookies, LocalStorage, SessionStorage and other similar technologies within the website operating under the name Zeta Signals, available at [domain address], hereinafter referred to as the "Service".
2. The Service is administered by [First and Last Name], a natural person conducting non-registered activity, contact address: [Residential/Contact Address], contact e-mail address: support@zetasignals.pl, hereinafter referred to as the "Administrator".
3. This Cookie Policy supplements the Terms of Service of Zeta Signals and the Privacy Policy of Zeta Signals.
4. The Service is based on Next.js technology and uses technical solutions provided by third parties, in particular Supabase and Lemon Squeezy.
5. The purpose of this Cookie Policy is to provide the User with clear information on what technologies are used in the Service, for what purposes, by whom, for how long and how the User may manage them.
6. This Cookie Policy covers both cookies stored in the browser and similar technologies, in particular LocalStorage, SessionStorage, session identifiers, authentication tokens and other mechanisms for storing information in the User's terminal device.
7. This document should be interpreted together with the Privacy Policy, because some information stored or accessed through cookies or similar technologies may constitute personal data or be linked to personal data.

§ 2. What cookies, LocalStorage and similar technologies are

1. Cookies are small text files stored on the User's terminal device, such as a computer, phone, tablet or another device enabling Internet access.
2. Cookies may contain technical information enabling browser recognition, session maintenance, remembering User preferences, ensuring security, login support, payment processing or proper operation of selected Service functions.
3. LocalStorage is a browser storage mechanism that allows data to be stored locally on the User's device. Data stored in LocalStorage may remain stored after the browser is closed until it is deleted by the User, the Service or the browser mechanism.
4. SessionStorage is a browser storage mechanism similar to LocalStorage, but the data stored in SessionStorage is generally maintained only for the duration of a given browser session.
5. Similar technologies mean other technical solutions enabling information to be stored in the User's terminal device or access to information already stored in that device, regardless of the name or technical implementation.
6. In this Cookie Policy, the term "cookies" may also include LocalStorage, SessionStorage and other similar technologies if the context indicates that it concerns storing information or accessing information in the User's terminal device.
7. Deleting data stored in LocalStorage or SessionStorage may result in the User being logged out, losing saved preferences, having to accept the cookie banner again or the malfunction of selected Service functions.

§ 3. Legal grounds for using cookies and similar technologies

1. The use of cookies and similar technologies is carried out in accordance with applicable law, in particular European Union rules on privacy in electronic communications, Polish electronic communications law and the GDPR, where personal data is processed through such technologies.

2. Storing information or accessing information stored in the User's terminal device is permitted in particular where:

- a) the User has been informed in advance about the purpose of such action,
- b) the User has given consent, where consent is required,
- c) storage or access is necessary to provide a service requested by the User,
- d) storage or access is necessary to transmit a communication over a telecommunications network.

3. Cookies and technologies necessary for the operation of the Service may be used without separate User consent if they are necessary to provide a service explicitly requested by the User, ensure communication transmission, login, session maintenance, payment processing, security or remembering the User's privacy choices.

4. Optional cookies and technologies, in particular analytical, advertising, marketing, remarketing, personalization or profiling technologies, may be used only after obtaining the User's appropriate consent, where such consent is required by law.

5. Optional cookies should not be activated before the User gives consent. Lack of consent to optional cookies must not block access to the basic functions of the Service if the technology is not necessary to provide the service requested by the User.

6. Where personal data is processed through cookies or similar technologies, the legal basis for processing may include in particular:

- a) Article 6(1)(b) GDPR - performance of a contract or taking steps prior to entering into a contract,
- b) Article 6(1)(f) GDPR - the Administrator's legitimate interest in ensuring security, stability, protection against abuse, payment support and defense against claims,
- c) Article 6(1)(a) GDPR - the User's consent, where a given category of cookies or similar technologies requires consent.

7. The Administrator's legitimate interest does not replace the requirement to obtain consent to cookies or similar technologies where such consent is required under the rules concerning storing information or accessing information in the User's terminal device.

§ 4. Categories of cookies and technologies used in the Service

1. The Service may use the following categories of cookies and similar technologies:

1) Necessary cookies and technologies

1. These are cookies, LocalStorage, SessionStorage or other technologies necessary for the proper operation of the Service, login, session maintenance, security, Account support, Subscription support, correct checkout operation or remembering the User's cookie decisions.

2. Without these technologies, the Service may not function properly and use of the Account, user panel, paid functions or payments may be impossible.

3. These technologies do not require separate User consent if they are genuinely necessary to provide the service requested by the User.

2) Security cookies and technologies

1. These technologies are used to protect the Service against abuse, attacks, unauthorized access, attempts to bypass security, payment fraud, CSRF attacks and other technical threats.

2. They may include session identifiers, security tokens, timestamps, login attempt information, technical error data or elements allowing suspicious activity to be detected.

3. The purpose of these technologies is to protect the User, the Administrator, payments, the Account and the integrity of the Service.

3) Payment cookies and technologies

1. These technologies are used to process payments, Subscriptions, cart, checkout, link transactions with the User Account and prevent financial fraud.

2. These technologies may be used by Lemon Squeezy as an external payment operator and Merchant of Record.
3. Lemon Squeezy cookies and technologies may be used in particular when the User proceeds to checkout, opens the payment form, initiates a purchase, manages a Subscription or handles a chargeback.

4) Preference cookies

1. These technologies enable remembering the User's cookie settings, language version, interface theme or other basic technical preferences.
2. The Service may store information in LocalStorage regarding whether the User has seen the cookie banner, what choices the User made in available settings or whether the banner should be displayed again.

5) Analytical, marketing and advertising cookies

1. As of the effective date of this Cookie Policy, the Service should not use analytical, advertising, marketing, remarketing cookies or tracking pixels without obtaining the User's separate consent.
2. If the Administrator implements tools such as Google Analytics, Meta Pixel, TikTok Pixel, Hotjar, Microsoft Clarity, affiliate tools or other similar analytical or marketing tools in the future, this Cookie Policy should be updated and the User should be given the option to give or refuse consent before such technologies are activated.

§ 5. Detailed list of cookies and similar technologies

1. The following list describes the main categories of cookies and similar technologies used or potentially used in the Service. Specific technical names may vary depending on the configuration of the Service, Supabase, Lemon Squeezy, browser and software version.
2. Before production launch of the Service, the Administrator should verify the actual cookies, LocalStorage keys and third-party technologies in browser developer tools and supplement the following list with actual names, domains and retention periods.

1) Supabase Auth - session and login

- Provider: Zeta Signals / Supabase.
- Example technology: LocalStorage, session token, access_token, refresh_token, Supabase Auth keys, e.g. sb-[project-ref]-auth-token.
- Purpose: maintaining the User session, enabling login, preserving access after page refresh, supporting the Account and user panel.
- Retention period: for the duration of the session, until logout, token expiry, deletion by the User or according to Supabase configuration.
- Category: necessary.
- Consent: no, if the technology is necessary for login and Account operation.

2) Authorization and access control

- Provider: Supabase / Zeta Signals.
- Example technology: Supabase Auth session data, access token, refresh token, session identifier.
- Purpose: User authentication, securing access to the paid panel, verifying login status.
- Retention period: according to Supabase session configuration.
- Category: necessary.
- Consent: no, if necessary to use the Account.

3) Service security

- Provider: Zeta Signals / technical providers.
- Example technology: CSRF token, session identifier, security data, timestamps.
- Purpose: protection against CSRF attacks, unauthorized access, technical abuse and attempts to bypass safeguards.
- Retention period: usually for the duration of the session or a shorter technical period.

- Category: necessary / security.
- Consent: no, if necessary for Service security.

4) Cookie decision

- Provider: Zeta Signals.
- Example technology: LocalStorage, e.g. cookieConsent, cookiePreferences, zeta_cookie_consent.
- Purpose: remembering the User's decision regarding the cookie banner and privacy preferences so that the banner is not displayed on every visit.
- Retention period: until preferences are changed, browser data is deleted or the period configured in the Service expires.
- Category: necessary / privacy preferences.
- Consent: no, if used only to remember privacy choices.

5) Language and interface preferences

- Provider: Zeta Signals.
- Example technology: LocalStorage, preference cookie, selected language key.
- Purpose: remembering the language version of the Service or basic interface settings.
- Retention period: until the preference is changed or the User deletes the data.
- Category: preferences / necessary to provide the service according to the User's choice.
- Consent: usually no, if used to implement the User's choice.

6) Lemon Squeezy - checkout, payments and Subscription

- Provider: Lemon Squeezy.
- Example technology: Lemon Squeezy checkout cookies and identifiers, transaction identifiers, anti-fraud mechanisms.
- Purpose: checkout, cart, payments, Subscription support, linking transactions with the Account, preventing fraud, chargebacks and payment abuse.
- Retention period: according to Lemon Squeezy policies, payment service configuration and payment security requirements.
- Category: payment / security / necessary for payment processing.
- Consent: generally no, if the technology is necessary for payment processing, transaction security or fraud prevention; otherwise according to Lemon Squeezy policies and applicable law.

7) Analytics and marketing

- Provider: no active provider as of the effective date of this document, unless the Service implements such tools later.
- Example technology: Google Analytics, Meta Pixel, TikTok Pixel, Hotjar, Microsoft Clarity, affiliate pixels.
- Purpose: traffic analysis, statistics, advertising, remarketing, conversion measurement or marketing profiling.
- Retention period: depends on the provider.
- Category: optional.
- Consent: yes, if not necessary for the operation of the Service.

§ 6. Supabase Auth and session storage

1. The Service uses Supabase Auth to handle User registration, login and authorization.
2. Supabase Auth may use LocalStorage, cookies or other browser technical mechanisms to store information about the User session, including access or refresh tokens.
3. Session data is necessary so that the User can:
 - a) log in to the Account,
 - b) remain logged in after refreshing the page,
 - c) use the user panel,
 - d) access functions available only to logged-in Users,

- e) use paid functions after Subscription activation.
- 4. Blocking LocalStorage, cookies or other browser storage mechanisms may prevent login, session maintenance or proper use of the Zeta Signals panel.
- 5. Deleting Supabase Auth data stored in the browser may immediately log the User out and require logging in again.
- 6. The User may end the session by logging out of the Account. The User may also delete locally stored data through browser settings.

§ 7. Lemon Squeezy and payment-related cookies

- 1. Payments and Subscriptions in the Service are handled by Lemon Squeezy.
- 2. When initiating payment, proceeding to checkout, managing a Subscription or processing a transaction, Lemon Squeezy may use its own cookies or similar technologies.
- 3. Lemon Squeezy technologies may be used in particular to:
 - a) properly operate checkout,
 - b) support the cart or payment form,
 - c) identify the transaction,
 - d) link the payment with the User Account,
 - e) support the Subscription,
 - f) detect and prevent financial fraud,
 - g) counteract chargebacks and abuse,
 - h) ensure payment security,
 - i) fulfill Lemon Squeezy's legal obligations as payment operator and Merchant of Record.
- 4. If the User is redirected to the Lemon Squeezy payment environment or uses embedded checkout, independent Lemon Squeezy cookies and technologies may apply, and their detailed scope, retention period and configuration may result from Lemon Squeezy legal documents.
- 5. The Administrator does not have full control over all cookies and technologies used directly by Lemon Squeezy in its own payment environment.
- 6. Lemon Squeezy legal documents may also apply to cookies and similar technologies used by Lemon Squeezy, in particular its privacy policy, cookie policy, terms of service and payment documents.

§ 8. Cookie banner and consent management in the Service

- 1. The Service may display a cookie banner or privacy preferences panel to the User.
- 2. The cookie banner may be used to:
 - a) inform the User about cookies and similar technologies,
 - b) enable acceptance of optional cookies, if any are used,
 - c) enable refusal of optional cookies,
 - d) enable changing preferences,
 - e) save the User's decision so that the message is not displayed on every visit.
- 3. Cookies and technologies necessary for the operation of the Service may remain active regardless of the User's decision concerning optional cookies.
- 4. Optional cookies, in particular analytical, marketing, advertising, remarketing or profiling cookies, are not activated before the User gives consent, where consent is required by law.
- 5. The User should be able to withdraw consent as easily as it was given.
- 6. If a cookie preferences panel is available in the Service, the User may change settings from that panel at any time.
- 7. It is recommended to place a permanent "Cookie settings" link in the footer of the Service, enabling the User to reopen the preferences panel and change or withdraw consent to optional cookies.

8. If the cookie preferences panel is not available, the User may manage cookies and similar technologies through browser settings.

§ 9. How to check cookies saved by the Service

1. The User may independently check cookies and site data saved by the Service through the browser.
2. Examples of how to check cookies:
 - a) Chrome and Edge: click the icon next to the address bar and go to cookie and site data information,
 - b) Firefox: click the shield or lock icon next to the address bar and go to cookie and site data information,
 - c) Safari: go to privacy settings and the section for managing website data.
3. Technical users may also check LocalStorage and SessionStorage using browser developer tools, usually in the Application, Storage or similar tab.
4. The actual list of cookies and local data may depend on whether the User is logged in, has initiated payment, uses the user panel and has consented to optional cookies.

§ 10. How to manage cookies and LocalStorage in the browser

1. The User may independently manage cookies, LocalStorage, SessionStorage and other site data through the settings of the web browser.
2. The User may in particular:
 - a) delete existing cookies and site data,
 - b) block cookie storage,
 - c) block third-party cookies,
 - d) delete LocalStorage and SessionStorage data,
 - e) set automatic deletion of data after closing the browser,
 - f) use private or incognito mode.
3. Blocking cookies and necessary technologies may result in:
 - a) inability to log in to the Account,
 - b) the User session not being maintained after refreshing the page,
 - c) the Zeta Signals panel not working properly,
 - d) the Subscription not being correctly recognized,
 - e) checkout or payment not being processed correctly,
 - f) technical errors being displayed by the Service.
4. The following are sample paths for managing cookies in popular browsers. Settings names may differ depending on the browser version, operating system or interface language.

1) Google Chrome

1. Open Chrome.
2. Click the three-dot icon in the upper right corner.
3. Go to Settings.
4. Go to Privacy and security.
5. Select Third-party cookies or Site settings.
6. Manage permissions, block cookies or delete site data.
7. To delete data for a specific site, go to site data settings and search for the Service domain.

2) Mozilla Firefox

1. Open Firefox.
2. Click the menu icon in the upper right corner.

3. Go to Settings.
4. Go to Privacy & Security.
5. In Cookies and Site Data, select the relevant settings.
6. You may delete data, manage exceptions or block selected tracking mechanisms.

3) Safari

1. Open Safari.
2. Go to Settings or Preferences.
3. Go to the Privacy tab.
4. Manage cookies, website data and tracking settings.
5. You may delete data for selected websites or block certain mechanisms.

4) Microsoft Edge

1. Open Microsoft Edge.
2. Click the three-dot icon in the upper right corner.
3. Go to Settings.
4. Go to Cookies and site permissions.
5. Select Manage and delete cookies and site data.
6. Delete data, block third-party cookies or set exceptions for selected websites.

§ 11. Session and persistent cookies

1. The Service may use both session cookies and persistent cookies.
2. Session cookies are stored for the duration of the browser session and are usually deleted after the browser is closed, unless the browser or service configuration works differently.
3. Persistent cookies remain stored on the User's device for a specified period or until deleted by the User, browser, Service or provider of a given technology.
4. LocalStorage may work similarly to persistent cookies because data stored in it may remain in the browser until deleted.
5. The retention period of individual cookies and local data may depend on the configuration of the Service, Supabase, Lemon Squeezy, the User's browser settings, manual deletion by the User or technical changes in the Service.

§ 12. First-party and third-party cookies

1. First-party cookies are set directly by the Service or within its domain.
2. Third-party cookies are set by external service providers whose solutions are used in the Service or in the payment process.
3. Cookies or third-party technologies in the Service may come in particular from:
 - a) Supabase - for authentication, database and session infrastructure,
 - b) Lemon Squeezy - for payments, checkout, Subscription, settlements and transaction security.
4. The Administrator does not have full control over the lifecycle of all cookies used by third parties in their own environments, in particular in the external Lemon Squeezy checkout.
5. When proceeding to an external provider's website, the User should read that provider's legal documents.

§ 13. Lack of consent to optional cookies

1. Refusal of consent to optional cookies should not prevent the use of basic Service functions, unless a given function technically requires a specific necessary technology.

2. Refusal of consent to analytical, advertising or marketing cookies must not block access to the Service if those cookies are not necessary to provide the service requested by the User.
3. The Administrator should not use mechanisms forcing consent to optional cookies as a condition of access to the Service if this is not compliant with applicable law.
4. Optional cookies should be as easy to reject as to accept where consent is required for their use.

§ 14. Updating the cookie list

1. Technologies used in the Service may change along with the development of the Service, Next.js updates, Supabase configuration, Lemon Squeezy configuration or implementation of new functions.
2. The Administrator should periodically verify the actual list of cookies, LocalStorage keys, SessionStorage data and similar technologies used in the Service.
3. In the event of implementing new categories of cookies, in particular analytical, marketing, advertising or remarketing cookies, the Administrator should:
 - a) update this Cookie Policy,
 - b) update the cookie banner or preferences panel,
 - c) ensure the possibility to give or refuse consent before optional cookies are activated,
 - d) supplement the Privacy Policy if personal data is processed for a new purpose.
4. The User may check currently saved cookies and site data through browser settings.

§ 15. Security and technical limitations

1. The Administrator makes reasonable efforts to ensure that cookies and similar technologies used in the Service are limited to the scope necessary to achieve specified purposes.
2. The Administrator should apply appropriate technical and organizational measures to protect data processed through cookies and similar technologies.
3. The use of cookies and similar technologies should not lead to the collection of data excessive in relation to the purposes specified in this Cookie Policy.
4. The User should regularly update the web browser and operating system, as outdated software may increase security risks.
5. The User should use trusted devices and networks, particularly when logging in to the Account or making payments.

§ 16. Changes to the Cookie Policy

1. The Administrator may amend this Cookie Policy in the event of:
 - a) changes in law,
 - b) changes in technologies used in the Service,
 - c) changes in external providers,
 - d) implementation of new Service functions,
 - e) implementation of new cookies or similar technologies,
 - f) changes in payment processing,
 - g) the need to clarify information provided to Users.
2. The current version of the Cookie Policy is published in the Service.
3. If the changes are significant for User privacy, the Administrator may inform Users additionally, for example through a message in the Service or by e-mail.

§ 17. Contact

1. In matters relating to this Cookie Policy, the User may contact the Administrator at: support@zetasignals.pl.

2. The Privacy Policy of Zeta Signals also applies to matters concerning personal data processing in connection with cookies and similar technologies.

§ 18. Final provisions

1. This Cookie Policy applies from [date].
2. The Cookie Policy is available free of charge in the Service in a manner enabling its acquisition, reproduction and recording.
3. In matters not regulated by this Cookie Policy, applicable Polish and European Union law shall apply.
4. This Cookie Policy should be interpreted together with the Terms of Service and the Privacy Policy of Zeta Signals.