

Ozeon Privacy Policy

Last updated: 01 July 2026 **Website:** <https://ozeon.com> **Controller:** Ozeon OÜ (Registry Code 17484775) **Registered address:** Tornimäe tn 5, 10145 Tallinn, Kesklinna linnaosa, Harju maakond, Estonia **Contact:** privacy@ozeon.com

Contents

1. Introduction
 2. Who We Are
 3. Scope of This Policy
 4. Personal Data We Collect
 5. Why We Use Personal Data
 6. Legal Bases Summary
 7. Cookies, Consent & Analytics
 8. Third-Party Services and Processors
 9. International Data Transfers
 10. Data Retention
 11. User Rights
 12. Right to Complain
 13. No Sale of Personal Data
 14. Email Communications
 15. Security
 16. Children and Young People
 17. Automated Decision-Making
 18. Future Platform Features
 19. Related Policies
 20. Changes to This Privacy Policy
 21. Contact
-

1. Introduction

This Privacy Policy explains how Ozeon collects, uses, stores, shares, and protects personal data through the Ozeon website.

Ozeon is a regenerative innovation platform being developed to connect knowledge, learning, publishing, projects, organisations, Open Calls, funding, governance, and verification across ocean, climate, land, and sustainability-related work.

This policy applies to the current public website, including early access forms, waitlist forms, language selection, contact or enquiry forms, cookie preferences, consent-based analytics, website performance tools, and current restricted internal/editor functionality where applicable.

It does not yet fully cover future public platform features such as logged-in user accounts, organisation accounts, payments, project funding, subscriptions, bounties, DAO participation, Progress tokens, \$OZN utility, NFTs, IP-NFTs, OCIS, dMRV services, AI Footprint, or project verification workflows. Before those features launch publicly, Ozeon will update this Privacy Policy and provide additional privacy notices where needed.

2. Who We Are

For the purposes of data protection law, the controller of personal data collected through this website is:

Ozeon OÜ (17484775) Tornimäe tn 5, 10145 Tallinn, Kesklinna linnaosa, Harju maakond, Estonia Email: privacy@ozeon.com

Ozeon OÜ decides why and how personal data is processed through the current website.

Ozeon's holding company is:

Ozeon Pte. Ltd. (202535133H) 133 New Bridge Road, #08-01, Chinatown Point, Singapore 059413

Ozeon Pte. Ltd. may support strategic, commercial, operational, technical, or group-level activities connected to the wider Ozeon ecosystem. Unless otherwise stated, Ozeon OÜ is the controller for personal data collected through the current website.

If Ozeon appoints a Data Protection Officer, EU representative, or additional privacy contact in the future, the relevant details will be added here.

3. Scope of This Policy

This Privacy Policy covers personal data collected when users:

- visit the Ozeon website
- submit an early access or waitlist form
- contact Ozeon through the website
- select language preferences
- interact with pages where Analytics consent has been given
- manage cookie and privacy preferences
- request information about Ozeon, partnerships, or platform access
- receive transactional or confirmation emails
- receive early access or waitlist communications
- use restricted Ozeon Studio or editor functionality, where applicable

This policy should be read together with Ozeon's [Cookie Policy](#), which explains cookies, local storage, Google Consent Mode v2, analytics preferences, and cookie categories in full detail.

4. Personal Data We Collect

Ozeon aims to collect only the personal data needed for the purposes described in this policy.

4.1 Data Provided Directly by Users

When users submit an early access, waitlist, contact, partnership, or enquiry form, Ozeon may collect:

- name
- email address
- organisation name, if provided
- role, background, or professional area, if provided
- country or general location, if provided
- selected interests or interest tags
- message content, if provided
- communication preferences
- date and time of submission

The exact data collected depends on the form used.

4.2 Early Access and Waitlist Data

When a user joins the early access list or waitlist, Ozeon may process:

- email address
- name, if collected
- selected interest tags
- signup source, date, and time
- subscription status
- email engagement data, where enabled by the email provider
- unsubscribe or communication preference status

Waitlist and email-list data may be stored in Mailchimp and in Ozeon's own database, where needed for platform operations, signup validation, and record keeping.

4.3 Cookie and Consent Preference Data

Ozeon stores information about cookie and consent choices, including whether the user has accepted or rejected Strictly Necessary, Functional, and Analytics cookies. The current consent model is stored under **version 2** and includes [\(necessary\)](#), [\(functional\)](#), and

analytics fields. Strictly Necessary is always active; Functional and Analytics are optional and disabled by default. Full detail is in the [Cookie Policy](#).

4.4 Technical and Usage Data

When users visit the website, Ozeon and its service providers may process limited technical information, including:

- IP address, browser type, device type, operating system
- approximate region or country
- pages visited, referral source, date and time of visit
- request metadata and user-agent information
- website interaction information and language selection
- cookie consent status
- website performance information
- security and abuse-prevention signals

Some of this information may be processed by hosting, infrastructure, analytics, security, rate-limiting, and performance providers.

4.5 Analytics and Performance Data

Ozeon currently uses:

- **Google Analytics 4** — consent-gated; only runs where Analytics consent is given
- **Vercel Analytics and Speed Insights** — aggregate website usage and performance measurement

Neither tool is used for advertising, retargeting, or behavioural marketing.

4.6 Google Analytics Event Data

Where Analytics consent has been given, the website tracks two custom events:

- **join_waitlist** — fires on successful early access/waitlist submission; may include selected interest tags
- **select_language** — fires when a user selects a language; may include language code and name

Neither event intentionally sends personally identifiable information — names, email addresses, phone numbers, or message content — to Google Analytics.

4.7 Restricted Studio, Editor, or Administrative Account Data

Where restricted Ozeon Studio, editor, or administrative functionality is used by authorised team members or collaborators, Ozeon may process:

- account email address, login or verification information

- role and permission metadata, authentication events
- content records, uploaded files or images, file metadata
- editor activity, security logs, technical request data

Authentication is handled through Better Auth, self-hosted on Ozeon's own infrastructure and database. Because it is self-hosted, Better Auth is not a separate third-party processor — the underlying infrastructure and database providers are disclosed in Section 8.

4.8 File and Image Upload Data

Where authorised users upload files or images through Ozeon Studio or related internal tools, Ozeon may process uploaded files and images, file names and metadata, storage paths, upload timestamps, and associated account or editor metadata. Files and images are stored using Vercel Blob. This functionality is intended for authorised Studio, editor, administrative, or internal workflows unless otherwise stated.

4.9 Rate Limiting and Abuse Prevention Data

To protect the website from abuse, spam, repeated form submissions, and automated misuse, Ozeon may process request metadata, timestamps, IP-derived or request-derived rate-limit keys, one-time send guards, and temporary operational data. Ozeon uses Upstash for Redis-based rate limiting, abuse prevention, and ephemeral operational storage.

4.10 Data We Do Not Intentionally Collect

The current public website does not intentionally collect special category data — information about health, religion, political opinions, trade union membership, genetic or biometric data, sex life, sexual orientation, or racial or ethnic origin. Users should not submit sensitive personal data through general website forms unless Ozeon specifically requests it through an appropriate, protected process.

5. Why We Use Personal Data

5.1 Website Operation and Security

Technical data and Strictly Necessary technologies are used to operate, secure, maintain, and deliver the website — page delivery, reliability, security, consent storage, TLS, CDN delivery, edge protection, abuse prevention, and debugging. *Legal basis: legitimate interests; necessity to provide a requested service.*

5.2 Cookie Consent Management

Consent preference data is processed to remember user cookie choices and allow users to update or withdraw consent. *Legal basis: legal obligation; legitimate interests in maintaining a compliant consent system.*

5.3 Early Access and Waitlist Management

Used to process signups, understand user interest, organise onboarding, assign interest tags, manage email lists, and communicate with people who have asked to hear from Ozean. *Legal basis: consent; legitimate interests; steps taken at the user's request.*

5.4 Responding to Enquiries

Used to respond to user messages, partnership requests, collaboration enquiries, and other user-initiated communications. *Legal basis: legitimate interests; steps taken at the user's request.*

5.5 Communications and Updates

Contact details may be used to send early access updates, launch information, partnership discussions, verification emails, confirmation emails, welcome emails, or enquiry responses. Users can unsubscribe from optional communications at any time; transactional emails (e.g. verification codes) may still be sent where necessary to provide a requested service or protect account security. *Legal basis: consent; legitimate interests; steps taken at the user's request.*

5.6 Website Analytics and Improvement

Where Analytics consent is given, Google Analytics data is used to understand website usage and improve page content, structure, language support, design, and user experience. *Legal basis: consent.*

5.7 Aggregate Performance Analytics

Vercel Analytics and Speed Insights are used to understand performance, page speed, route-level experience, and technical reliability — never for advertising or retargeting. *Legal basis: legitimate interests; consent where required by applicable law.*

5.8 Functional Preferences

Where Functional consent is given, optional preferences such as language or personalisation settings may be stored. *Legal basis: consent.*

5.9 Studio, Editor, and Administrative Functionality

Account, authentication, content, upload, and permission data is processed to manage authorised access, protect content workflows, support publishing, and maintain website operations. *Legal basis: legitimate interests; contractual necessity where applicable; steps taken at the request of the authorised user.*

5.10 Rate Limiting and Abuse Prevention

Limited technical data is processed to prevent spam, abuse, excessive submissions, automated misuse, and security threats. *Legal basis: legitimate interests in protecting the website, users, and infrastructure.*

6. Legal Bases Summary

Purpose	Example Data	Legal Basis
Website operation and security	IP address, request metadata, technical logs	Legitimate interests; service requested by user
Cookie consent storage	Consent preferences	Legal obligation; legitimate interests
Early access and waitlist	Name, email, interests, signup metadata	Consent; legitimate interests; user-requested steps
Email-list management	Email address, tags, subscription status	Consent; legitimate interests
Transactional email	Email, verification codes, confirmations	Legitimate interests; service requested by user
Responding to enquiries	Contact details, message content	Legitimate interests; user-requested steps
Optional communications	Email, communication preferences	Consent; legitimate interests
Google Analytics 4	Consent-gated usage data and events	Consent
Vercel Analytics / Speed Insights	Aggregate performance and usage data	Legitimate interests; consent where required
Functional preferences	Language or preference settings	Consent
Studio/editor accounts	Account email, auth events, role metadata, content	Legitimate interests; contractual necessity
File and image storage	Uploaded files/images and metadata	Legitimate interests; contractual necessity
Rate limiting and abuse prevention	Request-derived keys, timestamps, signals	Legitimate interests

Where Ozeon relies on legitimate interests, it considers whether the processing is necessary, proportionate, and balanced against the rights and freedoms of users.

7. Cookies, Consent & Analytics

Ozeon uses cookies, local storage, and similar technologies across three categories —

Strictly Necessary (always active), **Functional**, and **Analytics** (both optional and off by default). Optional categories are governed by Google Consent Mode v2: `functionality_storage` and `personalization_storage` follow Functional consent, and `analytics_storage` follows Analytics consent — all denied until the user opts in.

Ozeon does not currently use advertising cookies, retargeting pixels, behavioural advertising tools, or third-party marketing tracking technologies. If that changes, this Privacy Policy, the Cookie Policy, and the cookie banner will be updated before those tools are activated.

Users can accept, reject, or change cookie preferences at any time via the **Cookie Settings** link in the site footer, or through their browser settings. Full detail — including the current cookie table, consent versioning, and Google Analytics event structure — is in the Cookie Policy.

8. Third-Party Services and Processors

Ozeon uses selected third-party providers to operate the website, manage signups, send email, store data, prevent abuse, and measure performance. Each processes personal data only as necessary for the purposes in this policy, and only in its capacity as a service provider or processor.

Provider	Role	Location
Vercel Inc.	Hosting, serverless infrastructure, CDN, edge security, TLS, delivery, Vercel Blob file storage, Vercel Analytics, Speed Insights	United States
Google Analytics 4	Consent-gated website analytics	United States
Mailchimp (The Rocket Science Group LLC, an Intuit company)	Waitlist and subscriber-list management, interest tags, segmentation, marketing email	United States
Resend	Transactional email delivery (verification codes, confirmations, welcome emails)	United States
Neon	Serverless Postgres hosting for subscriber, account, and content records	Region documented internally; available on request
Upstash	Redis-based rate limiting, abuse prevention, ephemeral operational storage	United States

Ozeon's own `/api/subscribe` route on Vercel receives and validates waitlist submissions before passing relevant data to the systems above; Ozeon does not currently use a third-party form tool such as Typeform for waitlist submissions.

Ozeon maintains an internal record of processing for each provider — its role, the data categories involved, location of processing, applicable data processing agreement, transfer safeguard, and retention setting — available on request.

9. International Data Transfers

Several providers listed in Section 8 are based in, or may process data in, the United States, Singapore, or other countries outside the European Economic Area, the United Kingdom, or Switzerland.

Where personal data is transferred internationally, Ozeon relies on appropriate safeguards, which may include:

- an adequacy decision, where applicable
- the EU-U.S. Data Privacy Framework, where the provider is certified and the transfer is covered
- Standard Contractual Clauses
- the UK International Data Transfer Addendum or equivalent UK safeguards
- data processing agreements and supplementary safeguards, where required

Users may contact privacy@ozeon.com for more information about the transfer safeguards in place for a specific provider.

10. Data Retention

Ozeon keeps personal data only as long as necessary for the purposes described in this policy, unless a longer period is required by law.

- **Consent preferences** — until the user changes preferences, clears browser storage, or the consent model version is updated.
- **Early access and waitlist data** — for as long as necessary to manage early access, launch communications, and onboarding; deleted or anonymised sooner where the user unsubscribes, requests deletion, or withdraws consent, unless Ozeon has a lawful reason to retain it longer.
- **Email marketing and subscriber records** — retained while the user remains subscribed, or while Ozeon has a lawful reason to retain consent, unsubscribe, or suppression records. Users can unsubscribe at any time.
- **Contact and partnership enquiries** — retained as long as necessary to respond to the enquiry, manage the relationship, and maintain appropriate business records.
- **Google Analytics data** — governed by the applicable GA4 property retention settings, and only where Analytics consent has been given.
- **Vercel Analytics / Speed Insights data** — retained per Vercel's applicable product settings and service terms; used for aggregate performance insight only, never advertising or retargeting.

- **Technical logs** — retained for a limited period needed for security, debugging, reliability, fraud and abuse prevention, and operational maintenance.
- **Studio, editor, and account data** — retained while the account is active or as long as necessary for content history, security records, auditability, and access management.
- **Uploaded files and images** — retained as long as necessary for the relevant content, operational, or archival purpose, then deleted or archived per internal content-management practice.

11. User Rights

Depending on location and applicable law, users may have the right to:

- access their personal data
- request correction of inaccurate personal data
- request deletion of personal data
- restrict or object to certain processing
- withdraw consent at any time (without affecting processing carried out before withdrawal)
- data portability
- not be subject to decisions based solely on automated processing that produce legal or similarly significant effects
- complain to a data protection authority

Users can exercise these rights by contacting privacy@ozeaon.com. Ozeaton may need to verify a user's identity before responding to certain requests.

12. Right to Complain

Users who believe their personal data has been processed unlawfully have the right to complain to a data protection authority. As Ozeaton OÜ is established in Estonia, the relevant supervisory authority is:

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) Tatari 39, 10134 Tallinn, Estonia Website: <https://www.aki.ee>

Users may also contact the supervisory authority in their own EU or EEA country.

13. No Sale of Personal Data

Ozeaton does not sell personal data, and does not currently share personal data with third parties for behavioural advertising or retargeting.

14. Email Communications

Ozeaton may send email to users who sign up for early access, join the waitlist, request updates, or make contact — including early access updates, launch information,

onboarding communications, partnership responses, verification codes, confirmations, and welcome emails.

Mailchimp is used for waitlist and email-list management; Resend is used for transactional email delivery. Users can unsubscribe from optional marketing or update emails at any time via the unsubscribe link or by contacting privacy@ozeaon.com. Transactional or service-related emails may still be sent where necessary to provide a requested service, confirm an action, or protect account security.

15. Security

Ozean uses reasonable technical and organisational measures to protect personal data against unauthorised access, loss, misuse, alteration, or disclosure, including:

- secure website delivery, TLS encryption, CDN and edge security
- access controls, including role-based access for restricted Studio or editor functionality
- limited access to form submissions
- use of reputable service providers and data minimisation
- consent-based analytics and rate limiting / abuse prevention
- avoidance of unnecessary tracking — no advertising or retargeting trackers in the current implementation

No website or online service can guarantee absolute security, but Ozean aims to apply privacy-conscious practices as the platform develops.

16. Children and Young People

The current website is not intentionally directed at children under the age required by applicable data protection law for independent consent. If Ozean becomes aware it has collected personal data from a child without appropriate consent, it will take steps to delete that data where required. Future educational or community features involving young people will be reviewed separately for child privacy, safeguarding, age-appropriate design, and consent requirements.

17. Automated Decision-Making

The current website does not use personal data for automated decision-making that produces legal or similarly significant effects on users. Future features involving OCIS, Project Integrity Scoring, dMRV, verification workflows, governance, funding, token activity, or AI-supported reporting may require additional notices explaining automated or AI-assisted processing.

18. Future Platform Features

This policy describes the current public website, early access implementation, and restricted internal/editor functionality. Future Ozean platform features may involve

additional processing, including: public user and organisation accounts, payments, project publishing and funding, subscriptions, article/media/tutorial publishing, bounties, DAO participation, educational resources, Progress tokens, \$OZN utility, NFTs and IP-NFTs, OCIS climate intelligence, dMRV monitoring, AI Footprint, project verification workflows, and public platform file or media uploads.

Before launching these features publicly, Ozeon will update this Privacy Policy, the Cookie Policy, the Terms of Use, and any relevant platform-specific notices.

19. Related Policies

This Privacy Policy should be read alongside Ozeon's [Cookie Policy](#), which covers cookies, consent, and analytics in full detail, and its [Terms of Service](#), which govern use of the website more broadly.

20. Changes to This Privacy Policy

Ozeon may update this Privacy Policy if it adds website features, changes analytics tools or cookie categories, adds third-party providers, changes hosting, database, storage, or email providers, launches account-based or payment features, launches DAO, token, NFT, OCIS, dMRV, or AI Footprint features, changes retention periods, changes the responsible legal entity, or changes international transfer safeguards. Where changes are material, Ozeon will update the policy date, notify users, and request renewed consent where required.

21. Contact

Questions about this Privacy Policy or Ozeon's use of personal data: [**privacy@ozeon.com**](mailto:privacy@ozeon.com)

Inspiring regenerative innovation for a sustainable future
through Open Science, Crowdfunding, and Transparency.

