

LiberUp privacy policy

Information about the personal data LiberUp processes, the purposes and legal grounds, and the rights of data subjects.

Version: 1.0-draft | Updated: 2026-08-31

Effective date: [EFFECTIVE DATE TO BE COMPLETED]

DRAFT: before this document takes effect, its effective date and actual accounting provider must be specified, and processor agreements, processing locations and any transfers outside the EEA must be verified.

1. Controller and contact

The controller is LIBERUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, UL. OZORKOWSKA 13A , 95-100 ZGIERZ, NIP: 7322232375, REGON: 54553560900000, KRS: 0001262265, referred to as “LiberUp” or the “Controller”.

Privacy contact: contact@liberup.pl; correspondence: UL. OZORKOWSKA 13A , 95-100 ZGIERZ. The Controller has not appointed a Data Protection Officer because, as of the effective date of this Privacy Policy, none of the conditions specified in Article 37(1) GDPR apply.

2. Scope and sources

Data is obtained from Users during registration, purchases, contact and Account management; automatically from devices and connections; and from the payment operator as transaction identifiers and status.

LiberUp does not intend to process special-category data. Such information should not be submitted unless necessary.

3. Data categories

- Account and profile: email, password hash, verification status, language, role and Account status, plus optional name, phone, company and Polish tax number.
- Orders and accounting: User, items, quantities, prices, statuses, dates, Licence parameters and refund information.
- Payments: amount, status, dates and Przelewy24 or Stripe session and transaction identifiers. LiberUp does not store full card or online-banking credentials.
- Licences and apps: Licence key, Product, type, seats, device limit, status, dates and event history.
- Devices: technical identifier, optional device name, app version, activation and last-contact timestamps.
- Security: IP address for Licence attempts, attempt type and result, hashed rate-limiting identifiers, and server and application logs.
- Contact: name, email, subject and message. The form forwards the message to email and does not store it in the application database.
- Consents: type, decision, source, document version and time, including Terms, newsletter and Product information preferences.

4. Purposes and legal grounds

- Accounts, Library, orders, subscriptions, Licences, devices, updates and complaints – contract performance or pre-contract steps (Article 6(1)(b) GDPR).
- Tax, accounting and authority obligations – legal obligation (Article 6(1)(c)).
- Security, abuse prevention, rate limiting, logs and legal claims – legitimate interests (Article 6(1)(f)).
- Pre-contract contact – Article 6(1)(b); other correspondence – legitimate interests under Article 6(1)(f).
- Newsletter, voluntary marketing, optional analytics and advertising cookies – consent (Article 6(1)(a) and applicable electronic communications law).
- Consent history – compliance obligations and legitimate interests (Article 6(1)(c) and (f)).

5. Required and optional data

Required fields are needed for the Account, contract, payment, activation or request. Without them, the relevant service may be unavailable. Optional profile fields are voluntary.

Marketing and optional-cookie consent is voluntary and does not affect purchased Products.

6. Recipients and providers

- OVHcloud — VPS 3 – service and database infrastructure; region and processor agreement must be confirmed.
- OVHcloud — Zimbra – system, verification, password-reset and contact messages.
- PayPro S.A. — Przelewy24; Stripe Payments Europe, Ltd. — Stripe (po aktywacji) – payments; PayPro S.A. also acts as an independent controller for payer data.
- OVHcloud — automatyczna kopia zapasowa VPS, przechowywana i trzykrotnie replikowana na innych serwerach w tym samym centrum danych co VPS w Warszawie, Polska. Retencja: 24 godziny..
- Zewnętrzne biuro rachunkowe — w zakresie niezbędnym do prowadzenia księgowości, rozliczeń podatkowych oraz realizacji obowiązków prawnych LiberUp..
- Authorised support and administration staff under role-based least privilege.
- Legal, security and IT providers where necessary and appropriately contracted.
- Public authorities where disclosure is legally required.

7. Google Analytics, Ads and AdSense

Google Analytics, Google Ads and Google AdSense are planned but currently inactive. Their scripts and identifiers must not be loaded before the required consent.

Before activation, this Policy and the Cookie policy must identify the exact configuration, retention, recipients, purposes, legal basis and any non-EEA transfer mechanism, with an easy withdrawal option.

8. Transfers outside the EEA

The website, database and automated backups are stored in OVHcloud infrastructure in Warsaw, Poland. Backups are stored in the same data centre as the VPS. OVHcloud Zimbra email data is hosted in European OVHcloud data centres. OVHcloud may use affiliated entities and approved subprocessors under its data processing agreement. Where processing involves a transfer outside the EEA, an adequacy decision or standard contractual clauses with the required safeguards will apply.

Planned Google services may involve non-EEA processing and will not be enabled before the transfer basis and safeguards are documented.

9. Local JPK processing

JPK tax files are processed locally on the User's device and are not sent to LiberUp servers. The server may receive only Account, Licence, version, ruleset and update data, without JPK file contents.

10. Retention

- Account and profile – data is retained while the Account remains active. After the Account is deleted, identifying and contact data are promptly erased or anonymised in the active database. Copies may remain in the automated VPS backup for up to 24 hours until the backup is automatically replaced. Data connected with Orders, payments, legal acceptances, complaints and claims is retained for the periods specified separately for those purposes.
- Orders, payments, refunds and accounting records – for at least five years from the beginning of the year following the financial year to which the records relate. Where data is required in connection with an audit, proceeding or claim, it may be retained until the proceeding is finally concluded or the applicable limitation period expires.
- Licences, Subscriptions, devices and events – data evidencing the scope of an entitlement is retained for the duration of the contract and for six years from the end of the calendar year in which the Licence or Subscription expired, was cancelled or revoked. Activated-device data that is no longer required for Licence operation or legal claims is erased or anonymised within 30 days after the Licence ends.
- Sessions and tokens – until they expire, are used or revoked, the password is changed or the User signs out. Inactive session records and used or expired tokens are deleted within 30 days.
- Licence attempts, IP addresses, logs and rate limiting – information concerning Licence activation, validation and deactivation attempts, including the IP address, attempt type and result, is retained for 90 days. Technical hashed identifiers used for rate limiting are retained for no longer than 48 hours. Standard application and server logs are retained for 30 days, while security logs are retained for 90 days. Data concerning a specific incident may be retained for longer, until its investigation is completed and for the period necessary to establish, exercise or defend legal claims.
- Contact messages and complaints – ordinary contact correspondence is retained for 12 months after the matter is closed. Correspondence concerning complaints, withdrawal, refunds or disputes is retained for six years from the end of the calendar year in which the matter was closed. Messages are then deleted from the OVHcloud Zimbra mailbox unless further retention is required by law or an ongoing proceeding.
- Consents – current consents are retained while they remain valid. Evidence that marketing or newsletter consent was granted or withdrawn is retained for three years after withdrawal or replacement. Acceptances of the Terms, EULA and other documents connected with an Order are retained for the retention period applicable to that Order or Licence.

- Backups – an automated backup of the entire VPS is created daily by OVHcloud and retained for 24 hours. It is triplicated on other servers in the same data centre in Warsaw, Poland. Access is restricted to authorised administrators through the secured OVHcloud Control Panel. LiberUp does not currently apply additional application-level encryption to the complete VPS backup. Each backup is automatically replaced by the next one, so data erased from the active system may remain in the backup for no longer than 24 hours.

11. Automated decisions and profiling

LiberUp does not currently make solely automated decisions producing legal or similarly significant effects. Security controls may temporarily rate-limit requests or reject an invalid activation; disputed cases can be reported to support.

Advertising profiling is inactive and will be described with consent controls before use.

12. Data-subject rights

- access and a copy;
- rectification;
- erasure where statutory conditions apply;
- restriction;
- portability for automated processing based on consent or contract;
- objection to legitimate-interest processing and at any time to direct marketing;
- withdrawal of consent without affecting prior lawful processing;
- a complaint to the President of the Polish Personal Data Protection Office.

13. Exercising rights

Requests may be sent to contact@liberup.pl. LiberUp may request only information needed to securely verify identity and will respond within the GDPR deadline.

Erasure does not always remove every record immediately where retention is required for law, accounting, security or claims.

14. Security

LiberUp uses risk-appropriate measures including role-based access, password hashing, server-side secret protection, encrypted connections, rate limiting, Licence event records, updates and backups. Measures are reviewed periodically.

No transmission or storage method guarantees absolute security. Suspected incidents can be reported to the privacy contact.

15. Children's data

LiberUp is not directed at children. Data found to have been supplied without a required legal basis or guardian consent will be deleted or investigated as appropriate.

16. Changes and versioning

The Policy has a version and effective date. Material changes to ongoing processing will be communicated appropriately before use. Archived versions will be available in the Legal centre.

Related documents in this version

[LiberUp terms of service — PDF](#) · [Cookie policy — PDF](#) · [End-user licence agreement — PDF](#) · [Complaints and withdrawal — PDF](#) · [Accessibility information — PDF](#)

liberup.pl/legal/archive