LiberUp privacy policy

How LiberUp processes data for its website, licensing, correspondence and communications. The EULA governs software use; the Cookie policy covers browser technologies.

Version: 2.4-draft-2026-10-07 | Updated: 2026-10-07

Planned effective date: 2026-10-07

DRAFT: Planned date: 2026-10-07. Outstanding matters, approval and publication must be completed; this remains a draft and does not amend existing contracts. Later publication requires an appropriate effective date. The date alone does not activate sales or renewals.

---

1. Controller and contact

The controller is LIBERUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, UL. OZORKOWSKA 13A , 95-100 ZGIERZ, Poland; KRS 0001262265, NIP 7322232375, REGON 54553560900000. Send data requests and questions to contact@liberup.pl or that address. An authorised LiberUp representative handles them. The assessment of whether a data protection officer is required under GDPR Article 37 must be documented before this policy takes effect.

This policy also covers accounts and test orders at staging.liberup.pl. Provider tests may use fictional payment details, but real email addresses, account identifiers and activation information remain personal data. The test environment verifies functionality and does not receive local JPK files or accounting clients' data.

2. Data and its sources

Data comes from the person registering, purchasing or contacting us, an authorised customer representative, device communication with the service, and the selected payment provider. It includes email, password hash, verification and account security, language and preferences, purchaser and billing details, order items and history, transaction status and identifiers, licences and their dates.

Licensing requires a technical device identifier, user-provided device name, app version, activation and validation times, and security events. The service processes IP addresses, technical request information and attempt results. Contact handling includes an address, case content and necessary verification and delivery records. Consents and acceptances are recorded with versions and timestamps.

We do not request banking passwords, complete card data or KSeF secrets. Payment credentials are submitted directly to the provider. Do not include special-category data or accounting clients' records in correspondence.

If we receive a representative's or employee's contact details from a customer instead of directly from that person, we provide the required information, including the source and categories of data, within one month at the latest, or at the first communication or disclosure to another recipient if earlier. An exception is applied only where a ground under Article 14(5) GDPR applies and is documented. Publishing this policy in the footer alone does not replace providing the information to that person.

3. Purposes and grounds

Accounts, purchases, licensing, devices, delivery and contract administration: GDPR Article 6(1)(b). For a customer's employee or representative, communication and relationship management rely on legitimate interests under Article 6(1)(f). Accounting and legally required responses: Article 6(1)(c).

Security, abuse prevention and establishing or defending specific claims rely on Article 6(1)(f), subject to necessity and individual rights. Pre-contract correspondence uses point (b); other correspondence uses (f). Voluntary marketing and future optional tracking use Article 6(1)(a) and, where applicable, Articles 398–399 of the Electronic Communications Law.

Required data enables the requested action; without it an account, purchase, activation or response may be impossible. Optional fields remain voluntary. Purchased services do not depend on marketing consent. Security, contractual price, expiry and billing notices do not require newsletter subscription.

The application privacy notice describes JPK_VAT data and connections, local history and logs. Required contractual communications, security notices and conformity updates do not depend on newsletter consent or optional messages about new features.

4. Local files and processing boundaries

JPK applications process files and save results on the user's computer. LiberUp does not receive file contents during ordinary use. The KSeF summary application is designed to connect directly from the computer to the Ministry of Finance without sending invoices, tokens or KSeF authorisations to LiberUp. This must be tested before release.

Licensing local software alone does not entrust accounting clients' documents to LiberUp. Account and activation data are processed separately. We do not offer remote-desktop support and accept only synthetic or effectively anonymised samples. An accidentally received real document is restricted and assessed for deletion and possible incident handling; it does not automatically become authorised diagnostic material.

A cloud feature, remote processing or content telemetry requires prior reassessment of flows, documentation and, where applicable, a processing agreement. Future operations are not covered by blanket consent.

5. Recipients and providers

OVHcloud provides the website VPS and database and OVHcloud Zimbra email. Hosted data is covered by its applicable processing agreement; its privacy policy describes its own purposes. Using Zimbra through OVHcloud does not itself mean all mail is separately transferred to the software manufacturer. Relevant service documents are linked below.

The selected active provider Stripe, Przelewy24 (PayPro S.A.) or Paynow (mElements S.A.) receives data necessary for payment. Its own payment obligations follow its documents. The contracting entity, roles, countries and identifier scope must be approved for each integration before activation. Mentioning a planned provider does not mean it already receives data.

Authorised LiberUp personnel and necessary IT, accounting and legal providers may access data under appropriate obligations. Authorities receive data where required by law. The accounting firm's identity and contractual evidence must be completed in the vendor register before publication.

6. Locations and transfers

LiberUp's confirmed configuration places the VPS in Warsaw and uses OVHcloud Zimbra email. OVHcloud describes European email hosting. This does not establish that every support operation and subcontractor acts only in Poland. Subcontracting and locations must be matched against the agreement actually assigned to LiberUp's account.

Transfers outside the EEA require a GDPR Chapter V basis, such as Article 45 or 46, and assessment of safeguards. Before a new flow is enabled we document the recipient, country and mechanism. Information on applicable safeguards and obtaining copies is available at contact@liberup.pl. Future transfers are not presented as already approved.

7. Retention

Account data supports the service while used; closure leaves only what is necessary for obligations and specific claims. Unverified accounts without purchases or entitlements become eligible for deletion after 30 days. Cleanup provides 90 days for licence attempts, up to 7 days buffer for expired session and token records, and up to 24 hours for expired rate limits and nonces. The schedule and its operation must be monitored.

Tax records follow applicable periods, generally linked to 5 years from the end of the year in which tax payment became due, subject to events affecting limitation (Tax Ordinance Articles 70(1) and 86(1)). Accounting records follow Accounting Act Article 74. These periods do not all run from the order date.

Contracts, acceptance evidence, licences and disputes are retained for performance and as necessary for specific claims under the applicable Civil Code Article 118 limitation period. Consent evidence does not authorise marketing after withdrawal. The content of ordinary contact and technical-support messages is deleted 12 months after the case closes. Messages documenting a complaint, contract performance or a specific dispute are retained only as needed under the applicable category and claim period. Backups and accounting evidence follow separate rules; their actual configuration must match the published information.

Maximum retention in VPS and mailbox backups must be checked in configuration. We do not assert an unverified 24 hours. Backups are excluded from ordinary processing and rotated; deletion instructions must be reapplied after restoration. A case-specific hold needs a basis, scope, owner and review date.

Manual retry history records the operator identifier, task kind and identifier, time and result code; it does not store email bodies, passwords or tokens. Completed entries are deleted after 90 days and failed verification and password-recovery email entries after 7 days. An active task may be retained until its outcome is established; complaints, disputes and contract evidence follow the separate periods described in this policy.

8. Account closure and statistics

Closing an Account and disabling renewal are separate operations under the Terms. After closure we restrict processing and delete or anonymise unnecessary data; legally required settlement records and evidence remain with limited access. Encrypting data alone does not fulfil an erasure request.

Statistics remain indefinitely only after effective anonymisation, without identification or reconstruction of links. Pseudonymous identifiers and encrypted data remain subject to GDPR and limited retention.

9. Rights and requests

Subject to GDPR conditions, rights include access and copies, rectification, erasure, restriction, portability and objection to legitimate-interest processing. Direct marketing can be objected to at any time. Consent can be withdrawn without affecting prior lawful processing. Complaints may be lodged with the President of UODO.

We respond without undue delay, generally within one month; a further two-month extension requires Article 12(3) conditions and notice of the reason. Identity verification is proportionate. Erasure may be subject to Article 17(3) exceptions. Closing the Account is not required to ask about data.

10. Security and automation

Risk-appropriate measures include access control, secret protection, encrypted connections, password hashing and event records. Automated payment, licence-validity and device-limit checks may refuse an operation; disputed outcomes can be reviewed by a person via contact@liberup.pl. Advertising profiling is not active. Any decision-making covered by GDPR Article 22 requires a separate assessment and notice before implementation.

Report suspected breaches without sharing secrets or real client documents. LiberUp assesses incidents and fulfils applicable GDPR Articles 33–34 obligations. We do not promise that incidents are technically impossible.

11. Newsletter, cookies and social profiles

The newsletter is optional and requires appropriate consent. Unsubscribe through settings or contact. Essential contractual notices are not newsletter messages. Google Analytics, Google Ads and AdSense remain inactive; enabling them requires updated information, configuration and any required consent. The Cookie policy contains the technology inventory.

Facebook, X, YouTube and Instagram publish updates. LiberUp uses ordinary website links, without pixels or embedded players. Once followed, the platform applies its own documents. LiberUp processes visible profile

information, comments and messages to communicate under Article 6(1)(f). Do not send account disputes, payment details or client documents in public comments.

Facebook Page statistics and potential joint controllership require an Article 26 assessment and applicable platform terms. Insights documentation and configuration remain to be confirmed before active use. Following a profile does not subscribe the user to the newsletter.

12. Versions and connections

This policy describes processing, does not replace the contract and does not consent to every future use of data. Material changes in purposes, providers or scope are assessed and communicated before application. Current and archived versions appear in the Legal centre; language versions and PDFs use the same source content.

Legal references and useful documents

RODO / GDPR — art. 5–7, 12–22, 25–28, 32–34, 37, 44–49; motyw / recital 26

Prawo komunikacji elektronicznej — art. 398–399

Ordynacja podatkowa — art. 70 § 1, 86 § 1

Ustawa o rachunkowości — art. 74

Kodeks cywilny — art. 118

OVHcloud — umowa powierzenia / processing agreement (PDF)

OVHcloud Zimbra — warunki usługi / service terms (PDF)

OVHcloud — polityka prywatności / privacy policy

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 · Subscription and payment rules — PDF · Support and continuity rules — PDF · Withdrawal form — PDF · JPK_VAT product specification — PDF · Application privacy — PDF · Social profile privacy — PDF · JPK_VAT use and safety — PDF

liberup.pl/legal/archive