

PRIVACY POLICY

OBVELO — Personal Data Masking Gateway

Version: 1.2 · **Published:** 2026-10-01 · **In force from:** 2026-10-01

1. Who we are

1.1 The controller of the personal data described in this Privacy Policy is **Luminote P.S.A.** (*prosta spółka akcyjna*), with its registered office at ul. Olszańska 7, 31-513 Kraków, Poland, entered in the Register of Entrepreneurs of the National Court Register (KRS) under number 0001223956, NIP 6751824986, REGON 543999032 ("**we**", "**us**" or the "**Provider**").

1.2 You can contact us about data protection by e-mail at security@obvelo.com or by post at the address above. We have not appointed a Data Protection Officer, as we are not required to do so; all data protection matters are handled at security@obvelo.com.

1.3 This Privacy Policy explains how we process personal data as a **controller**, in connection with the OBVELO website, the Accounts of our customers, billing, support and the security of the Service. Capitalised terms not defined here have the meanings given in the Terms of Service at <https://app.obvelo.com/legal/terms> and the Data Processing Agreement at <https://app.obvelo.com/legal/dpa> (the "**DPA**").

2. What this Privacy Policy does not cover: content sent through OBVELO

2.1 OBVELO detects and masks personal data in content that our customers send through the Service ("**Customer Content**"). For personal data contained in Customer Content, **we are not the controller**. We act as a **processor** on behalf of our customer, who decides why and how that data is processed. Our obligations in this respect are set out in the DPA.

2.2 If your personal data appears in content that one of our customers sent through OBVELO (for example, your name in a document or e-mail), please contact that

customer, who is the controller of your data and is responsible for informing you and handling your requests.

2.3 By design, the part of OBVELO that processes content (the data plane) stores nothing from that content: it is processed only in memory for the time needed to handle a request and return the response. The part that manages accounts (the control plane) stores contract data — accounts, plans, usage in numbers, and the settings a customer saves — and never sees content. As a result, we hold no copy of the content itself. If you contact us with a request concerning Customer Content, we will forward it to the relevant customer where we can identify them.

3. Whose data we process

We process personal data of:

- (a) **Users** — persons who register or use an Account on behalf of a customer (e.g. developers, administrators);
 - (b) **customer contact persons** — persons indicated for billing, security or other communication;
 - (c) **customers who are sole traders** — natural persons conducting business activity who conclude the Agreement in their own name;
 - (d) **persons contacting us** — by e-mail, including for support, complaints, security reports or sales enquiries;
 - (e) **website visitors** — persons visiting the OBVELO website, trying the public demo or using the customer panel.
-

4. Purposes, legal bases and retention periods

Purpose	Data	Legal basis (GDPR)	Retention
Registering and maintaining the Account, providing the Service	at registration: the User's e-mail address and chosen Plan; later, in the customer panel:	For sole traders: performance of the Agreement — Art. 6(1)(b). For Users and contact persons	For the duration of the Agreement, then until the expiry of the

Purpose	Data	Legal basis (GDPR)	Retention
	company name, VAT or registration number, country, address; Account settings; API key identifiers and labels	acting on behalf of a company: our legitimate interest in performing the Agreement with that company — Art. 6(1)(f)	limitation period for claims
Signing in to the customer panel	e-mail address, sign-in credentials (stored only as a hash), session data	As in the first row	For the duration of the Account; sessions end after 8 hours or at sign-out
Verifying the customer (VIES check of the VAT number, when you enter it in the customer panel)	company name, VAT number, verification result	Legitimate interest in verifying our business partners and preventing fraud — Art. 6(1)(f); for VAT purposes also Art. 6(1)(c)	As for the Account
Record of acceptance of the Terms of Service and the DPA	Account identifier, e-mail address, accepted document versions, date and time of acceptance	Legitimate interest in proving the conclusion and content of the Agreement — Art. 6(1)(f)	For the duration of the Agreement, then until the expiry of the limitation period for claims
Billing, invoicing, accounting and tax	company data, address, VAT number, Plan, usage counters, payment history, invoices	Legal obligation under tax and accounting law — Art. 6(1)(c)	5 years from the end of the calendar year in which the tax payment deadline expired

Purpose	Data	Legal basis (GDPR)	Retention
Usage metering and limits	Account and API key identifiers, number of characters and pages processed per period, limit settings	Performance of the Agreement — Art. 6(1)(b) / legitimate interest — Art. 6(1)(f), as in the first row	For the duration of the Agreement, then as billing data
Service communication (notices on changes to the Terms, DPA, Sub-processors, security incidents, payments)	e-mail address, content of messages	Performance of the Agreement — Art. 6(1)(b) / legitimate interest — Art. 6(1)(f); where required, legal obligation — Art. 6(1)(c)	For the duration of the Agreement, then until the expiry of the limitation period for claims
Support and complaints	e-mail address, name, content of correspondence	Legitimate interest in handling enquiries and complaints — Art. 6(1)(f); for sole traders also Art. 6(1)(b)	Until the matter is closed, then until the expiry of the limitation period for claims
Security of the Service and abuse prevention	IP address, kept in memory to limit repeated sign-in and registration attempts and never written to logs; for the public demo, a salted hash of the IP address that changes every day	Legitimate interest in ensuring the security of the Service — Art. 6(1)(f)	IP address: up to 1 hour in memory; demo hash: up to 24 hours in memory
Establishing, pursuing and defending claims	data necessary for the claim	Legitimate interest — Art. 6(1)(f)	Until the expiry of the limitation period for claims or the final conclusion of proceedings

Purpose	Data	Legal basis (GDPR)	Retention
Product updates and newsletter	e-mail address	Consent — Art. 6(1) (a), given in accordance with the Polish Electronic Communications Law	Until consent is withdrawn
Browser extension status records (Section 9.3)	random installation identifier, extension version, on/off and administered state, whether the organisation's browser policy sets any of its settings (yes or no), event type with at most a chat site's hostname, a file type, the names of changed settings or a count — never typed text, file names or file content	Legitimate interest of the Customer and ours in showing which installations of the extension are in use and in securing the Service — Art. 6(1)(f)	Up to 30 days in the gateway's memory (a restart clears it earlier); the log line written for each record until the gateway's log rotation overwrites it — logs are rotated by size, at most 5 × 10 MB per container, with no archive
Operation of the website and customer panel	browser data, session cookie; web server logs (address requested, time, response status — without IP addresses or request headers)	Legitimate interest in providing a working and secure website — Art. 6(1) (f)	Session cookie: up to 8 hours or until sign-out; server logs: up to 30 days

Limitation periods. Claims arising from business activity are generally time-barred after 3 years, with the period ending on the last day of the calendar year (Article 118 of the Polish Civil Code). Where a longer period applies, we retain data accordingly.

5. Where the data comes from

5.1 We obtain data directly from you when you register an Account, use the Service, contact us or visit our website.

5.2 If your employer or business partner registered an Account and indicated you as a User or contact person, we obtained your e-mail address and name from that customer.

5.3 We receive payment status information (e.g. whether a payment succeeded, failed or was refunded) from our payment provider. We do not receive or store payment card numbers.

5.4 We obtain the result of VAT number verification from the VIES system of the European Commission.

6. Is providing data required?

Providing an e-mail address is necessary to register an Account. Providing company and invoicing data is necessary before a paid Plan is paid for and is required by tax law. Providing other data is voluntary.

7. Who receives the data

7.1 We share personal data only to the extent necessary and only with the following recipients:

(a) **hosting provider** — OVH Sp. z o.o., ul. Powstańców Śląskich 9, 53-332 Wrocław, Poland (member of the OVHcloud group), which hosts our infrastructure in data centres in the EEA (currently France and Poland), acting as our processor;

(b) **payment provider** — Mollie B.V., Keizersgracht 126, 1015 CW Amsterdam, the Netherlands, which processes payments as an independent controller under its own privacy statement (<https://www.mollie.com/privacy>);

(c) **providers of IT and communication services** we use to run our business, such as e-mail, acting as our processors;

(d) **public authorities**, including tax authorities (for example through the National e-Invoicing System, KSeF), where required by law;

(e) **legal and professional advisers**, bound by professional secrecy, where necessary to establish, pursue or defend claims.

7.2 E-mails from the Service (such as confirmation of your address) are sent from our own mail server; we do not use an external e-mail delivery service. Sign-in to the customer panel runs on identity software we operate ourselves; no external identity provider receives your data.

7.3 We do not sell personal data and do not share it for advertising purposes.

8. Transfers outside the EEA

8.1 Our infrastructure is hosted in the EEA, and our website and customer panel do not load scripts, fonts or analytics from outside the EEA.

8.2 If a recipient listed in Section 7 (such as the payment provider, under its own privacy statement) transfers data outside the EEA as an independent controller, it does so under its own responsibility and in accordance with Chapter V GDPR.

9. Cookies and local storage

9.1 Our website and customer panel use only technologies that are **strictly necessary** for their operation: one session cookie that keeps you signed in to the customer panel (`HttpOnly` , `Secure` , `SameSite=Lax` , valid for up to 8 hours). Protection against forged requests uses a request header, not a cookie. We use no analytics, marketing or third-party cookies. The sign-in pages of our identity service (id.obvelo.com) set cookies that are strictly necessary for signing in and for protection against forged requests; they are not used for analytics or marketing.

9.2 The customer panel may keep a panel access token in your browser's local storage, and the `/app` page keeps the gateway address and the API key you enter there, so that you do not have to type them again. They stay on your device; you can delete them by clearing the site data in your browser.

9.3 The OBVELO **browser extension** stores its settings, the lists and dictionaries you keep in it and, where your organisation has set an administrator, a hash of the administrator's password (never the password itself) locally in your browser (browser extension storage). Where your organisation configures the extension through browser policy (for example Group Policy or a device-management profile), the

extension reads those settings from the browser and cannot change them. It sends to the OBVELO gateway configured in it:

- the text you type into a supported chat site, and files you attach there, so that they can be masked — also while you type, so that it can show you what will be masked before you send. This is content processed for the Customer under the DPA (Section 2), not by us as a controller;
- short **status records** about itself: a random installation identifier created at installation (not linked to your name or account by the extension), the extension version, whether it is switched on, whether an administrator manages it and whether your organisation's browser policy sets any of its settings (yes or no — never the settings themselves), and events such as a chat site added or removed (that site's hostname), a setting changed (the setting's name, never its value), a dictionary loaded (the number of entries) or a file sent without masking (its type, never its name or content). Status records never contain text you typed, file names or file content.

When the extension is removed, your browser opens a gateway address that records the removal of that installation. You can delete the data stored in your browser by removing the extension or clearing its data.

9.4 You can manage cookies in your browser settings. Blocking the session cookie prevents you from signing in.

10. Your rights

10.1 In accordance with the GDPR, you have the right to:

- (a) **access** your data and receive a copy of it (Art. 15);
- (b) **rectify** inaccurate data (Art. 16);
- (c) **erase** your data (Art. 17), subject to exceptions, e.g. where we must keep it under tax law;
- (d) **restrict** processing (Art. 18);
- (e) **data portability** — receive your data in a structured, commonly used, machine-readable format, where processing is based on consent or a contract and carried out by automated means (Art. 20);
- (f) **object** to processing based on our legitimate interest (Art. 21(1)), for reasons relating to your particular situation;

(g) **withdraw consent** at any time, where processing is based on consent, without affecting the lawfulness of processing before withdrawal.

10.2 To exercise your rights, contact us at security@obvelo.com. We respond without undue delay, and in any event within one month; this period may be extended by two further months where necessary, in which case we will inform you. We may ask for information needed to confirm your identity, e.g. by replying from the Account e-mail address.

10.3 You also have the right to lodge a complaint with the supervisory authority — in Poland, the **President of the Personal Data Protection Office** (*Prezes Urzędu Ochrony Danych Osobowych*), ul. Stawki 2, 00-193 Warszawa, www.uodo.gov.pl — or with the supervisory authority of your place of residence or work in the EU.

11. Automated decision-making

We do not make decisions about you based solely on automated processing, including profiling, that produce legal effects concerning you or similarly significantly affect you. The detection of personal data by OBVELO is carried out on Customer Content on behalf of our customers (Section 2), not to make decisions about you.

12. Security

12.1 We apply technical and organisational measures appropriate to the risk, including encryption in transit (TLS), strict separation between the part of the Service that processes Customer Content and the part that manages Accounts, restricted administrative access, key revocation, encrypted hourly backups of the account database kept for 30 days, and hosting exclusively in the EEA. A more detailed description of the measures is set out in Annex II to the DPA.

12.2 You can report security vulnerabilities to security@obvelo.com.

13. Children

The Service is intended exclusively for businesses and is not directed at persons under 18. We do not knowingly collect data of children in our role as controller.

14. Changes to this Privacy Policy

14.1 We may update this Privacy Policy, for example when we change recipients, introduce new features or when the law changes. We will notify Account holders of material changes by e-mail and in the customer panel before they take effect.

14.2 The current version is available at <https://app.obvelo.com/legal/privacy>, and each previous version, with its dates of validity, under its own address (for example <https://app.obvelo.com/legal/privacy-1.0.html>).