VIMS — VARILO INTEGRATED MANAGEMENT SYSTEM

Privacy and cookie policy

Version: 1.0 | Last updated: 2026-09-26

This document explains what personal data we process in connection with the v-ims.pl website and the VIMS platform, on what legal basis, how long we keep it, and which cookies and browser storage mechanisms we use.

Vesta Usługi i Szkolenia Marcin Makowski, ul. Wrzosowa 33, 84-300 Lębork, Poland · NIP/VAT ID: 841-161-18-09 · kontakt@varilo.eu · v-ims.pl

1. Controller and contact details

The controller of personal data processed in connection with the v-ims.pl website and the Provider's own processes is Vesta Usługi i Szkolenia Marcin Makowski, ul. Wrzosowa 33, 84-300 Lębork, Poland, VAT ID (NIP) 841-161-18-09.

For all matters concerning data protection, including the exercise of the rights described below, you may contact us at kontakt@varilo.eu or in writing at the registered address.

No data protection officer has been appointed. Data protection requests are handled by the business owner at the contact address indicated above.

2. Two roles: controller and processor

With regard to website visitors, people contacting us through the form, and representatives of customers and business partners, we act as the controller — we decide on the purposes and means of processing.

With regard to data entered into the VIMS platform by a customer organization — for example employee data, training participants, people involved in incidents or subcontractors — the customer is the controller. We process that data as a processor, solely on the customer's instruction and within the scope set out in the data processing agreement.

This distinction matters in practice: if you are an employee of an organization using VIMS and wish to exercise your rights regarding data held in the system, the correct recipient of your request is your employer as controller. We will forward such requests to the relevant organization.

3. Purposes, legal bases and scope of processing

- Handling enquiries from the contact form — name, e-mail address, organization name, message content. Basis: Art. 6(1)(b) GDPR (steps prior to a contract) and Art. 6(1)(f) GDPR (our legitimate interest in business correspondence).
- Creating and maintaining platform user accounts — e-mail address, account identifiers, authentication data, trusted device information. Basis: Art. 6(1)(b) GDPR (performance of a contract).
- Ensuring the security of the service — a security event log covering sign-in code delivery and verification, permission changes, data exports and reveals of specially protected data. Basis: Art. 6(1)(f) GDPR (protecting data and the service against unauthorized access).
- Billing, invoicing and accounting — customer billing data and contact persons. Basis: Art. 6(1)(c) GDPR (tax and accounting obligations) and Art. 6(1)(b) GDPR.

- Recording acceptance of legal documents — the person, document version and date of acceptance. Basis: Art. 6(1)(c) and (f) GDPR (accountability).
- Handling support requests and complaints — contact details of the reporting person and the description of the request. Basis: Art. 6(1)(b) and (f) GDPR.
- Website visit statistics based on analytics cookies — aggregated traffic data, without profiling and without linking to identifying data. Basis: Art. 6(1)(a) GDPR (your consent given in the cookie banner).
- Establishing, pursuing and defending claims — data required to evidence the course of the cooperation. Basis: Art. 6(1)(f) GDPR.

4. Retention periods

- Contact form correspondence — up to three years from the end of the correspondence, unless a contract results from it.
- User account data — for the term of the agreement with the organization and then up to thirty days after it ends, unless the data processing agreement provides otherwise.
- Security event log — for the term of the agreement and afterwards for the period required for accountability, no longer than twenty-four months.
- Billing and accounting documents — five years from the end of the year in which the tax obligation arose.
- Data processed for claims — until the statutory limitation periods expire.
- Analytics data from cookies — as stated in the cookie table, no longer than twenty-four months.

5. Recipients and processors

Data may be transferred to providers of services necessary to operate the website and platform: cloud and database infrastructure providers, e-mail and transactional messaging providers, website hosting providers and — to the extent required by law — our accounting office and legal advisers.

Every processor acting on our behalf operates under a data processing agreement and only to the extent necessary to deliver the service.

We do not sell personal data, do not share it with advertising networks or data brokers, and do not use it to build marketing profiles.

6. Processing location and transfers outside the EEA

VIMS platform and website data is processed in infrastructure located within the European Economic Area.

We do not envisage routine transfers to third countries. Should such a transfer become necessary, it will only take place under a mechanism provided for in Chapter V GDPR and this document will be updated accordingly.

7. Your rights

- The right of access to your data and to obtain a copy of it.
- The right to rectification of inaccurate or incomplete data.
- The right to erasure where we have no basis for further processing.
- The right to restriction of processing.
- The right to data portability for data processed under a contract or consent.

- The right to object to processing based on legitimate interest.
- The right to withdraw consent at any time — without affecting the lawfulness of processing carried out before withdrawal.
- The right to lodge a complaint with the President of the Personal Data Protection Office, ul. Stawki 2, 00-193 Warsaw, Poland.

8. Automated decisions and profiling

We do not take decisions based solely on automated processing that would produce legal effects for natural persons.

Algorithm-assisted functions in the platform — such as pre-reading the content of a safety data sheet — are supportive only. Their output is presented for human verification and is not recorded as a final finding without user confirmation.

9. What cookies and browser storage are

Cookies are small text files saved on your device by your browser. Alongside them we use browser local storage, which works similarly and is used to remember settings and the sign-in session.

Essential items are required for the website and platform to work — without them signing in and retaining basic settings is impossible. Their use does not require consent.

Analytics and preference items going beyond essential functions are used only after you give consent in the cookie banner. You can change or withdraw that consent at any time via the “Cookie settings” link in the site footer.

We do not use advertising cookies, social network pixels or tools that track user behaviour across other websites.

10. List of cookies and browser data used

- Platform authentication session items (essential) — keep the user signed in to app.v-ims.pl; expire at the end of the session or when the device session validity period lapses.
- Trusted device marker (essential) — reduces how often the one-time sign-in code is required; stored for up to thirty days.
- Cookie banner choice (essential) — stores your consent decision; stored for up to twelve months.
- Language preference (pl/en) and light/dark theme (essential for interface operation) — stored in browser local storage until cleared.
- Visit analytics (optional, consent required) — aggregated measurement of visits and most-visited pages, without identifying individuals; stored for up to twenty-four months.

11. Managing cookies yourself

You can change the scope of your consent at any time via the “Cookie settings” link in the site footer. Withdrawing consent does not affect essential items.

Independently of the banner, every browser lets you delete stored cookies and block new ones in its privacy settings. Blocking essential items will prevent you from signing in to the VIMS platform.

12. Data security

We apply technical and organizational measures proportionate to the risk: encryption in transit, mandatory two-step authentication for platform accounts, database-level isolation of each organization's data, role-based access control, protection of attachments against access that

bypasses permission checks, and a security event log.

A detailed description of the architecture and safeguards is published on our “Security and IT architecture” page, including an explicit list of functions we do not currently offer.

In the event of a personal data breach we act in accordance with Art. 33 and 34 GDPR and, when acting as processor, notify the controller without undue delay.

13. Changes to this policy

We update this policy when the scope of our services, the tools we use or applicable law change. The date of the last update and the version number are stated at the top of the document.

The current version is published at v-ims.pl/en/privacy-policy together with the downloadable files.