VIMS — VARILO INTEGRATED MANAGEMENT SYSTEM

Data Processing Agreement

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

A template agreement concluded under Art. 28 GDPR between an organization using the VIMS platform (the controller) and the platform provider (the processor). The document is an annex to the main agreement and is ready for signature.

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. Parties and subject matter

Processor: Vesta Usługi i Szkolenia Marcin Makowski, ul. Wrzosowa 33, 84-300 Lębork, Poland, VAT ID (NIP) 841-161-18-09, data protection contact address: kontakt@varilo.eu.

Controller: the organization using the VIMS platform under the main agreement, identified in this agreement together with its registration details and a data protection contact address.

The subject matter of this agreement is the entrusting of personal data processing to the extent necessary to provide access to the VIMS platform. It is concluded under Art. 28(3) GDPR and applies for the term of the main agreement.

2. Nature, purpose and duration of processing

Processing is automated, carried out in the information system made available by the processor, and covers operations such as collection, recording, storage, organization, modification, consultation, disclosure to the controller's authorized users, erasure and backup.

The purpose of processing is to enable the controller to run occupational safety, environmental, fire safety, quality and compliance processes in the system — in particular incident registers, risk assessments, training and qualification records, the chemical register, inspections and audits, and corrective actions.

Processing lasts for the term of the main agreement and for the period necessary to return or delete the data after it ends.

3. Categories of data subjects

- Employees and collaborators of the controller holding user accounts in the system.
- Employees of the controller covered by registers kept in the system — training and qualification records, medical examinations, risk assessments and workplace assignments.
- People involved in incidents and near misses: injured persons, witnesses, persons conducting the investigation.
- Employees of subcontractors and external companies admitted to work on the controller's premises.
- People designated as organizational contacts: safety function representatives, managers, approvers of permits and change requests.
- Where an occupational safety service company serves multiple clients — also data subjects on the side of clients served by the controller, provided the controller has established a legal basis for processing their data.

4. Types of personal data entrusted

- Identification and contact data: name, job title, organizational unit, business e-mail address and phone number.
- Employment and competence data: workplace and zone assignment, scope of authorizations, training, qualifications and their renewal dates.
- Incident data: description of the circumstances, the person's role in the event, investigation findings, attachments including photographic documentation.
- Data related to occupational health care within the scope kept by the controller: type of examination, date performed, next due date, information on the fitness-for-work certificate. The controller undertakes not to enter health data into the system beyond what labour law requires.
- Technical account and sign-in data: account identifier, e-mail address, trusted device information, security event timestamps.
- The parties agree that the controller does not enter special categories of data other than those indicated above, nor data relating to criminal convictions, unless separately agreed in writing with the processor.

5. Obligations of the processor

- Processing data only on the controller's documented instructions, which include the controller's configuration and use of the system, and in accordance with this agreement.
- Ensuring that persons authorized to process the data have committed to confidentiality, including after the cooperation ends.
- Implementing and maintaining the technical and organizational measures referred to in Art. 32 GDPR and described in section 6 of this agreement.
- Assisting the controller in responding to data subject requests, including promptly forwarding requests mistakenly addressed to the processor.
- Assisting the controller in meeting its obligations under Art. 32–36 GDPR, in particular data protection impact assessments and breach handling.
- Making available to the controller the information necessary to demonstrate compliance and allowing audits on the terms set out in section 8.
- Informing the controller if, in the processor's opinion, an instruction infringes data protection law.

6. Technical and organizational measures

- Encryption of data in transit between the user's browser and the system.
- Mandatory two-step authentication for accounts: password plus a one-time code sent to the account e-mail address, with limited validity and a capped number of attempts.
- Passwords and one-time codes stored only as cryptographic hashes.
- Isolation of each organization's data enforced at database level, row by row, independently of interface filters.
- Role-based access control, with organization membership approved by the organization owner or administrator and permissions stored outside the user profile.
- Protection of attachments, including incident photographs, against access bypassing permission checks — files are not reachable at a public address.
- A security event log covering sign-ins, permission changes, data exports and reveals of specially protected data.

- Automated backups of the data layer performed within the cloud provider's infrastructure, together with a restore procedure.
- Processing of data in infrastructure located within the European Economic Area.
- Separation of platform administrative permissions from permissions inside a customer organization, and least-privilege access for support staff.

7. Sub-processing

The controller grants the processor general authorization to engage sub-processors necessary to deliver the service, provided they are bound by data protection obligations no less strict than those arising from this agreement.

As at the date of this agreement the processor engages the following categories of sub-processors: a cloud infrastructure and managed database provider including attachment storage, a transactional e-mail and notification delivery provider, and a hosting and application delivery provider.

The processor informs the controller of any intended change or addition of a sub-processor at least thirty days in advance. The controller may raise a reasoned objection; if the parties fail to agree on a solution, the controller may terminate the main agreement in the manner provided for therein.

8. Audit and demonstrating compliance

The controller is entitled to verify how this agreement is performed, including by conducting an audit, upon at least fourteen days' prior notice, during business hours and in a manner that does not interrupt the continuity of the service.

An audit may not extend to data of other organizations using the platform, nor to information constituting a trade secret of the processor or its sub-processors.

The processor may demonstrate compliance by providing a description of its security measures, responses to a security questionnaire and documentation obtained from its infrastructure sub-processors.

9. Personal data breaches

The processor notifies the controller of any breach of the entrusted personal data without undue delay and no later than forty-eight hours after becoming aware of it, at the controller's contact address indicated in this agreement.

The notification includes the available information on the nature of the breach, the categories and approximate number of data subjects and records, the likely consequences and the measures taken or proposed. Information not available at the time of notification is provided in phases.

Notifications to the supervisory authority and to data subjects are made by the controller. The processor provides the necessary assistance.

10. Return and deletion of data after termination

At any time during the agreement, and before it ends, the controller may download an archive of its organization's data directly from the system. This right is available to the organization owner and administrator, and each export is recorded in the security event log.

After the main agreement ends, the processor deletes the entrusted data within thirty days of termination, or returns it to the controller in line with the controller's written request submitted no later than the termination date.

Deletion also covers copies of the data, save for backups, which are deleted as their retention cycle expires, and data whose storage is required by law.

11. Liability and final provisions

Each party is liable for the consequences of infringing data protection law within the scope of its own obligations. The controller is responsible in particular for the legal basis of processing, the scope of data entered into the system and providing information notices to data subjects.

Amendments require written form or an equivalent electronic form with a qualified signature, except for updates to the sub-processor list made under section 7.

Matters not covered by this agreement are governed by the GDPR, Polish law and the provisions of the main agreement and the VIMS platform terms of service.

Version 1.0 of this template applies from 2026-09-26 and is published at v-ims.pl/en/dpa.