Privacy Policy

of the viktor-global.com online platform

Viktor-global.com is an online platform (hereinafter referred to as the Platform or Viktor-global.com), a service for the comprehensive management and performance of professional tasks and the digitalisation of processes in occupational health and safety, fire safety and private security.

This Privacy Policy explains how personal data are processed when visiting, registering with and using the Platform, the roles of the User, the Provider and other entities involved, the types of data that may be processed, the purposes of processing and the legal bases relied upon, how data is protected and retained, and how individuals may exercise their rights.

Individual functionalities, modules, names and methods of technical implementation may change without requiring an amendment to this Privacy Policy, provided that this does not change the essential purposes, legal bases, categories of personal data, categories of individuals or other significant characteristics of the processing.

1.) Roles in personal data processing and contact details

To understand personal data processing correctly, a distinction must be made between data that the provider of the Viktor-global.com platform processes for its own contractual, business, security and support purposes and data that the User enters into its user environment for its own purposes or in the course of providing services to its client.

As a software service, the Platform is not a separate legal entity and therefore does not itself determine the purposes of personal data processing, the categories of individuals, the types of data entered by the User or their retention periods.

For personal data that the User enters into the Platform for its own purposes or in the course of providing services to its client, the Data Controller is the User or another entity that determines the purposes and essential means of processing. That entity must ensure an appropriate legal basis, notices to individuals, data limited to the minimum necessary, data accuracy, retention periods and appropriate management of access rights.

The Provider does not act as a Data Controller in respect of User Content, as it does not determine which personal or other data the User must enter, does not determine the legal basis for their processing, does not verify the accuracy of their content and does not decide on the professional, personnel, health, security, business or other purposes of their use.

Where, in ensuring the technical operation of the Platform, the Provider actually processes personal data on behalf of the User or another Data Controller and in accordance with its documented instructions, its rights and obligations in respect of that processing are, where necessary, regulated by a contract or other legal act governing personal data processing. Such a technical role does not mean that the Provider assumes the purposes of processing or the User's responsibility for the lawfulness of the data it enters into the Platform.

The Provider acts as an independent Data Controller for personal data of the contracting parties, their representatives, contact persons and authorised users that are necessary for registration, establishing

and performing the contractual relationship, managing user accounts, communication, billing, providing support, Platform security and pursuing or defending legal claims.

2.) Provider's contact details

Name: Viktor GLOBAL d.o.o.
Address: Cesta v Kleče 16, 1000 Ljubljana
Email: info@viktor-global.com
Company registration number: 9465006000
VAT identification number: SI 88170063
Contact of personal data protection officer: dpo@viktor-global.com

Requests concerning data in the user environment are generally dealt with most quickly if addressed to the User or organisation that entered the data or on whose behalf the data are processed. If the Provider receives such a request, it handles it in accordance with its actual role or forwards it to the responsible Data Controller without undue delay.

3.) Types of personal data, purposes and collection methods

The scope of data depends on the type of User, the functionalities provided by the Platform that are used, the contractual relationship and the data entered by the User or provided by the individual. The technical ability to enter a particular type of data does not mean that the Provider requires or recommends such entry or confirms it as necessary and lawful.

a) Data for registration, the contractual relationship and use of the Platform

- identification and contact details, such as first name, surname, organisation, position, email address and telephone number,
- data relating to the user account, organisation, role, rights granted, settings and account status,
- contractual, subscription, billing and payment data,
- data relating to communications, support requests, complaints, authorisations and other legally significant actions,
- technical and security data.

These data are processed for registering and managing user accounts, establishing and performing the contractual relationship, enabling functionalities, communication, billing, technical support, ensuring information security, preventing misuse and pursuing or defending legal claims. This list is illustrative and is not limited exclusively to the types of data listed.

b) Data in the user environment

Depending on the selected functionalities, the Platform may enable the processing of the following categories of data in particular:

- identification and contact details of the individual, such as first name, last name, date and place of birth, address, email address and telephone number,
- data relating to the employer, organisational unit, job and duties,
- data relating to certificates, records and records of proceedings,
- data relating to inspections of work equipment, devices, machinery, facilities, firefighting equipment and other objects of professional procedures,

- data from quotations, pro forma invoices, invoices, reports and other business documents that the User creates with the aid of the Platform,
- documents, attachments, timestamps, electronic signatures, digital certificates, graphical facsimiles and other data that the User enters or creates.

The Platform is not intended for storing medical records, diagnoses, therapies, treatment data or other special categories of personal data that are unnecessary for the intended service. Where the Platform enables free-text entries or document uploads, the User must itself assess whether each entry is necessary, proportionate and lawful.

c) Illustrative purposes for the use of modules and functionalities

Depending on the selected modules and functionalities, personal data may be processed in particular for:

- ordering and providing professional services, inspections and measurements,
- maintaining records, creating and signing certificates, records of proceedings, reports and other documentation,
- checking document validity, managing deadlines and sending notifications and reminders,
- maintaining data on organisations, equipment, devices, facilities and other objects of professional procedures,
- preparing quotations, pro forma invoices, invoices, overviews and reports,
- online storage, archiving, export, transfer, restoration and deletion of data and documents,
- using the User's own digital certificates, electronic signatures, timestamps, graphical signatures and other means of validating documents.

The list is illustrative and not exhaustive. The precise purpose, scope of data and legal basis for each procedure are determined by the User or another responsible Data Controller in accordance with the service used and its statutory or contractual obligations.

4.) Legal bases for processing personal data

a) Performance of the contractual relationship or User Relationship

The Business Cooperation Agreement or User Relationship provides the contractual basis for supplying the ordered services and for processing personal data of the contracting parties, their representatives, contact persons and authorised users that are necessary for registration, establishing and performing the contractual relationship, managing user accounts, communication, billing, providing services and supporting Users. The Provider may also process these personal data to fulfil tax, accounting, security and other statutory obligations, and on the basis of a legitimate interest in ensuring the security and reliability of the Platform, preventing misuse, maintaining audit trails and pursuing or defending legal claims.

b) The User's legal basis for data in the user environment

For personal data that the User enters into the Platform for its own purposes or in the course of providing services to its client, the User itself or another Data Controller must ensure an appropriate legal basis for processing personal data no later than the time of entry into the Platform. Such a basis may include, in particular, compliance with a legal obligation, performance of a contract, a legitimate interest or valid consent, where consent is appropriate in the circumstances and freely given.

c) Consent

Where processing is based on consent, that consent must be freely given, specific, informed and unambiguous. The individual may withdraw it at any time without affecting the lawfulness of

processing before its withdrawal. Withdrawal may mean that certain optional functionalities are no longer available. This does not affect the lawfulness of processing before consent was withdrawn.

5.) Protection of personal data

The Provider establishes, maintains and improves a system of administrative, organisational and technical measures to manage information risks and ensure the confidentiality, integrity, availability and traceability of information. Measures are determined according to the nature of the services, types of data, identified risks, state of the art and reasonable implementation costs, and comprise:

- periodic maintenance, updating and security checks of information systems and software,
- management of user and privileged access, allocation of rights according to roles, and regular review and revocation of unnecessary rights,
- use of appropriate authentication methods, including the option of multi-factor authentication where introduced or required,
- encryption of communications and use of appropriate cryptographic and other safeguards according to the technical architecture and risks,
- separation of user environments and restriction of access to entitled Users,
- logging of significant access events, changes, exports, deletions, security events and other relevant actions to the extent necessary and technically feasible,
- backups, restoration procedures and measures to ensure availability and resilience,
- management of vulnerabilities, changes, security events and incidents, and performance of security reviews and testing,
- contractual confidentiality and security obligations for persons and external service providers who may be involved in providing the services,
- procedures for business continuity, service restoration and supplier management.

Detailed measures, procedures and records are governed by internal policies, contracts, technical documentation and other documented information and are not published in full in order to safeguard information security.

Routine technical support does not generally include access to the content of User data. Where such access is exceptionally necessary to remedy a specific fault, provide requested support or address a security event, it is undertaken at the request of or with the approval of an entitled User, limited to the minimum necessary scope and duration, and made traceable, unless a different course of action is necessary due to a statutory obligation or to prevent immediate harm.

No information system can guarantee absolute security or entirely uninterrupted operation. The Provider therefore regularly adapts its measures to the risks and endeavours to ensure reliable operation, but cannot completely rule out the possibility of unauthorised access, disclosure, alteration, loss or destruction of data.

6.) Security breaches and notification

The Provider has procedures in place for detecting, assessing, containing, documenting and remedying security events and personal data breaches.

Where a breach concerns data for which the User or another entity is the Data Controller, the Provider will notify that Data Controller without undue delay and provide the available information necessary to assess the risk and fulfil its obligations. If not all circumstances are known at the time of the initial notification, further information may be provided in stages.

The obligation to notify the competent supervisory authority and individuals is assessed according to the role of each entity, the nature of the breach, the likelihood and severity of the risk and the applicable legislation.

7.) Retention of personal data

Personal data are retained as follows:

- personal data are retained only for as long as necessary for the purpose for which they were collected, or for as long as required by the applicable legislation, the contractual relationship, legitimate interests or documented instructions from the responsible Data Controller,
- registration and user data are retained for the duration of the active User Relationship and for a further reasonable period necessary for account closure, security and legal claims,
- contractual, billing and accounting data are retained for the periods required by the applicable legislation and evidential needs,
- communications and support requests are retained until the matter is resolved and thereafter for as long as reasonably necessary to demonstrate the support provided and defend legal claims,
- security and audit logs are retained for a period determined according to security risks, evidential needs and technical settings,
- digital certificates, graphical facsimile data, data and documents in the user environment are retained until deletion by an entitled User, cessation of use, expiry of the agreed retention period, another documented instruction from the responsible Data Controller or account deletion,
- archived documents are retained for the duration of the ordered archiving service or until a lawful instruction to delete them is received.

The User or another Data Controller is responsible for determining and applying the retention periods for User Content required under substantive law. The Provider cannot itself assess the statutory or professional retention period for each individual document belonging to the User.

8.) Deletion of data, quarantine and backups

Within the scope of its rights and the technical capabilities available, the User may delete individual data, documents or the user account. Before closing the account, it must retrieve the data and documentation it needs for statutory, evidential or business purposes.

Following account closure or a request for account deletion, the data are placed in quarantine for 30 days. During this period, they are not intended for ordinary use but may be restored upon a timely and justified request to prevent accidental loss. At the end of the quarantine period, the data are irreversibly deleted from the active environment.

If the User has not logged into its user account at least once during a consecutive two-year period, the system sends three warnings to the User's email address about deletion of the user account, one per month during the final three months before account deletion. During this time, the User may save its data at any point. Once this period expires, the data are placed in quarantine for 30 days, during which they may still be restored at the User's request. If the User logs into the account again, the two-year reference period starts afresh. At the end of the 30-day quarantine period, the system irreversibly deletes the data and notifies the User by email. Data in backups are deleted or overwritten as part of the regular backup retention cycle. Until then, they are not intended for ordinary use, but solely for restoration and ensuring system integrity.

The Provider may, on request and within reasonable limits, issue confirmation that deletion has been carried out.

9.) Archive

The Archive is a separate paid service of the Platform. It enables the User to continue storing selected documents and data electronically after their active use or validity has ended, provided that the User orders such storage and has an appropriate legal basis for it.

The User itself determines which documents to archive and how long they must be retained. Retention in the Archive continues until expiry of the ordered archiving service, deletion by an entitled User, termination of the contractual relationship or another lawful ground for ending retention. Before the archiving service ends, the User has the option of exporting or retrieving the documentation in formats supported by the Platform.

10.) Digital certificates, electronic signatures and graphical facsimiles

The Platform enables the use of the User's digital certificate, electronic signature or graphical facsimile to sign or validate documents. The User is responsible for the validity and lawful use of the digital certificate, protecting the private key, password and other credentials, and assessing the legal effects of the chosen signature method.

The Provider is not the issuer of the digital certificate, a certifier of the content or a signatory to the User's documents. Automated creation or signing of a document is carried out on the basis of the User's settings and instructions.

Digital certificates, passwords and other credentials are protected by appropriate technical measures according to the Platform's architecture. The User may remove a stored digital certificate, credentials or graphical facsimile in the settings or request their deletion. Upon account deletion or after extended inactivity, they are deleted in accordance with the rules on retention and deletion.

11.) Age restriction and minors' data

The Platform is intended for business and professional use by business entities and other legal persons and their authorised persons. Natural persons may use it only within the framework of a lawful relationship with a User, for the provision of an individual service or where they are otherwise lawfully granted access.

A person aged at least 15 may use the Platform independently. When processing minors' data, the User must ensure an appropriate legal basis, notices, data limited to the minimum necessary and suitable safeguards.

12.) Automated procedures and decision-making

The Platform automates individual procedures that the User would otherwise perform manually, such as calculating a test result, creating a document, checking a validity period, sending a reminder or carrying out another preconfigured action.

Such procedures do not constitute decision-making based solely on automated processing that produces legal effects or similarly significantly affects an individual. The User determines the criteria and purpose of the procedure, carries out the final professional assessment, and approves and signs the document.

13.) Individuals' rights

Depending on the circumstances and legal basis, an individual may exercise, in particular:

- the right to information and access to personal data,
- the right to rectification of inaccurate or incomplete data,
- the right to erasure where the statutory conditions are met,
- the right to restriction of processing,
- the right to data portability where applicable,
- the right to withdraw consent with effect for the future where processing is based on consent,
- the right to lodge a complaint with the competent supervisory authority.

These rights are not absolute. Before a request is acted upon, the applicant's identity and entitlement are verified. A request may be refused or restricted where permitted by the applicable legislation, for example because of the rights of other persons, a statutory obligation or the pursuit of legal claims.

14.) Exercising rights and cooperating with the Data Controller

For data in the user environment, the User or another responsible Data Controller is responsible for deciding on an individual's request. Within the scope of its actual role and technical capabilities, the Provider assists that Data Controller in locating, exporting, rectifying, restricting or deleting data.

If the Provider receives an individual's request concerning data in the user environment, it forwards the request to the responsible Data Controller without undue delay, unless its role requires it to handle the request itself. It rectifies, restricts or deletes data in the user environment on the basis of a documented instruction from the responsible Data Controller, a binding decision of a competent authority or another appropriate legal basis.

Requests concerning registration, contractual, contact, billing, support or security data for which the Provider is an independent Data Controller may be sent to dpo@viktor-global.com. Requests will be answered without undue delay and within the time limits prescribed by the applicable legislation.

15.) Access to personal data

Access to personal data is restricted to the User, its authorised persons and other entitled recipients in accordance with the rights granted, the purpose of the service and the applicable legislation.

The Platform's primary cloud infrastructure is provided through Microsoft Azure services in data centres in the European Union or European Economic Area. Where the Platform enables connections or data exchanges with external systems or service providers, the third-party provider's terms and privacy policies may also apply to the use of those services. Before transmitting data, the User is responsible for verifying the recipient's entitlement, the purpose of transmission and the appropriate legal basis.

Personal data may also be disclosed or made available to competent authorities or other entitled recipients where required by law or a binding decision, or where disclosure is necessary to protect the rights, security or property of the Provider, the User or other persons.

16.) Transfers of personal data to third countries

Data processing and storage take place in the European Union or European Economic Area. Personal data are therefore not disclosed to third parties or transferred outside the European Economic Area

for purposes other than those set out in the General Terms and Conditions, this Privacy Policy or agreed in the Business Cooperation Agreement.

The User is solely responsible for transfers it carries out by exporting, sending, integrating or granting access to recipients outside the European Union or European Economic Area.

17.) Complaint to a supervisory authority

An individual may lodge a complaint with the competent supervisory authority for personal data protection, in particular in the country of their habitual residence, place of work or the alleged infringement. Details of the competent supervisory authority are available on the official websites of national data protection authorities or the European Data Protection Board.

Before lodging a complaint, the individual may also contact the User or another responsible Data Controller, or the Provider's data protection contact, to seek a direct resolution of the matter.

18.) Updates to the Privacy Policy

The Provider reserves the right to update the Privacy Policy from time to time due to changes in legislation, contractual roles, providers, security measures, business processes or significant aspects of processing. Important changes are communicated to Users in an appropriate manner before they become applicable, where required by the nature of the change. Amendments to the Privacy Policy take effect on the date of publication on the Platform's web pages.

Changes to the user interface, technical architecture, module names, list of functionalities, authentication methods, encryption, logging or other technical measures do not require amendment of this Privacy Policy, provided that they do not change the essential purposes, legal bases, categories of data, categories of recipients or individuals' rights.

Continued use of this website or the Platform's service after amendments to the Privacy Policy have been published constitutes agreement to those amendments. The Privacy Policy takes effect on the date of publication.

Published on:

14.10.2026