Privacy Policy – SMM Protocols

Effective date: 1 May 2026

This Privacy Policy describes how VIPO a.s., with its registered office at Gen. Svobodu 1069/4, 958 01 Partizánske, Slovakia ("we", "our", "us", or the "Company"), collects, processes, stores, and protects personal data in connection with the SMM Protocols mobile application ("the App").

1. **Purpose of the Application**

SMM Protocols is an internal application used exclusively by authorized employees, contractors, and service technicians of VIPO a.s. for documenting, managing, and reporting service protocols related to prophylactic maintenance activities.

The App is not intended for public use. It does not allow public user registration, and user accounts are created and managed exclusively by a system administrator.

2. **Data Controller**

The data controller responsible for the processing of personal data is:

VIPO a.s.
Gen. Svobodu 1069/4
958 01 Partizánske
Slovakia
Email: info@smartmaintenance.sk

Privacy and data protection requests may be submitted using the contact details above.

3. **Categories of Personal Data We Process**

Depending on the user's role and use of the App, we may process the following categories of personal data:

a) Identification and Account Data
This may include:

- username;
- password;
- work email address.

b) Operational and Service Data

This may include operational and service-related information that is created, entered, uploaded, or processed through the App and that may be linked to an authorized user or may otherwise contain personal data, including:

- service protocols and inspection records;
- maintenance reports;
- technical notes, findings, and recommendations;
- machine-related data linked to service activities;
- photographs, attachments, and supporting documentation uploaded as part of service records;
- timestamps of service actions;
- identification of the user who created, modified, reviewed, uploaded, or submitted a service record;
- information entered into the App by authorized users as part of maintenance documentation.

c) Technical, Security, and Log Data
This may include technical, server-side, security, and log data necessary for the operation, protection, maintenance, and troubleshooting of the App and related backend systems, including:

- device type and operating system;
- app version;
- IP address;
- login timestamps;
- logout timestamps, where available;
- authentication logs;
- user-agent strings, which may include information about the browser, application, operating system, device, or client used to access the App;
- server access logs;
- system activity logs;
- error logs and diagnostic data;
- security logs;
- performance data;

- technical data necessary for system integrity, troubleshooting, prevention of unauthorized access, and protection against misuse.

Some of this data may be linked to a specific user account and may therefore constitute personal data.

d) Photographs, Attachments, and File Metadata

The App may allow authorized users to upload photographs or other attachments as part of service protocols, inspection records, maintenance reports, or other service documentation.

Such files may contain personal data or metadata, including:

- photographs of machines, equipment, workplaces, defects, service activities, or related technical conditions;
- information visible in the photograph or attachment;
- file name and file type;
- date and time when the file was created, modified, uploaded, or attached to a service record;
- device-related metadata, such as camera or device model, where included in the file;
- GPS location coordinates or other location metadata, where such metadata is enabled on the user's device and included in the uploaded file.

Users should avoid uploading photographs or attachments containing unnecessary personal data unless such information is required for the relevant service, maintenance, documentation, or reporting purpose.

The App does not collect personal data for advertising or marketing purposes.

4. Legal Basis for Processing

Personal data is processed in accordance with Article 6 of Regulation (EU) 2016/679, the General Data Protection Regulation ("GDPR"), on the following legal bases:

- Article 6(1)(b) GDPR – processing necessary for the performance of a contract, including an employment or contractor relationship;
- Article 6(1)(f) GDPR – processing necessary for the legitimate interests of VIPO a.s., including efficient maintenance operations, internal reporting, system security, business continuity, and protection of company assets;
- Article 6(1)(c) GDPR – processing necessary for compliance with legal obligations, where applicable.

5. Purposes of Processing

We process personal data solely for internal business and operational purposes, including:

- documenting and managing maintenance activities;
- creating, storing, and reviewing service protocols;
- documenting machine condition, defects, service findings, repairs, inspections, or maintenance activities using photographs or attachments;
- assigning and managing service tasks;
- operational planning and analysis;
- internal reporting;
- ensuring system functionality, security, and reliability;
- recording and reviewing login activity, authentication events, and server access logs;
- 9detecting, preventing, and investigating unauthorized access, misuse, technical errors, or security incidents;
- troubleshooting technical issues;
- protecting the App, users, and company systems against unauthorized access or misuse;
- complying with applicable legal, contractual, audit, or regulatory obligations.

We do not process personal data for advertising, marketing, or user tracking purposes.

6. Data Sharing and Recipients

VIPO a.s. does not sell personal data.

Personal data is not disclosed to third parties for advertising or marketing purposes.

Personal data may be accessed only by:

- authorized employees and personnel of VIPO a.s.;
- authorized contractors or service technicians, where access is necessary for their assigned tasks.

Any external service providers act as data processors or authorized service providers and are required to comply with confidentiality, security, and data protection obligations.

7. International Data Transfers

Personal data is primarily processed within the European Union or the European Economic Area.

If any transfer of personal data outside the European Union or European Economic Area occurs, such transfer will be carried out only in accordance with applicable GDPR requirements, including appropriate safeguards such as Standard Contractual Clauses or other legally recognized transfer mechanisms.

8. Data Retention

Personal data is retained only for as long as necessary to fulfil the purposes described in this Privacy Policy or as required by applicable legal, contractual, audit, security, or operational obligations.

In particular:

- account data is generally retained for the duration of the user's employment, contractor relationship, or authorized access to the App;
- service protocols, inspection records, and maintenance reports may be retained for the period necessary for operational, warranty, contractual, audit, technical, or legal purposes;
- photographs, attachments, and related file metadata uploaded as part of service documentation are retained together with the relevant service protocol, inspection record, maintenance report, or operational record, unless earlier deletion is required or permitted under applicable retention rules;
- server logs, authentication logs, IP addresses, login timestamps, user-agent strings, error logs, diagnostic logs, and security logs are retained only for the period necessary for system operation, security, troubleshooting, audit, and investigation of security or technical incidents, unless a longer retention period is required by applicable legal, contractual, or operational obligations.

When personal data is no longer required, it will be deleted, anonymized, or securely archived in accordance with applicable retention requirements.

9. Data Security

VIPO a.s. implements appropriate technical and organizational measures to protect personal data against unauthorized access, loss, misuse, alteration, disclosure, or destruction.

These measures may include:

- access control and authentication mechanisms;

- role-based authorization;
- administrator-managed user accounts;
- secure data storage;
- encrypted communication where applicable;
- monitoring and logging of system activity;
- restriction of access to authorized personnel only;
- internal confidentiality and data protection obligations;
- logging and monitoring of authentication events, server access, and security-relevant activity;
- regular maintenance and security review of the App and related systems.

Although we take appropriate measures to protect personal data, no system can be guaranteed to be completely secure.

10. User Accounts

User accounts are created, modified, and deactivated by a system administrator. Public self-registration is not available.

Access to the App is granted only to authorized users who require access for internal business, service, maintenance, or operational purposes.

Users are responsible for keeping their login credentials confidential and for using the App only in accordance with applicable internal rules, security requirements, and authorization levels.

11. Rights of Data Subjects

Under the GDPR, users may have the following rights in relation to their personal data:

- the right of access to personal data;
- the right to rectification of inaccurate or incomplete personal data;
- the right to erasure of personal data, where applicable;
- the right to restriction of processing;
- the right to object to processing based on legitimate interests;
- the right to data portability, where applicable;
- the right to lodge a complaint with a supervisory authority.

Requests may be submitted to VIPO a.s. at:

info@smartmaintenance.sk

Deletion or restriction requests will be assessed in accordance with applicable legal, contractual, audit, security, and operational retention requirements.

Users also have the right to lodge a complaint with the competent supervisory authority, in particular the Office for Personal Data Protection of the Slovak Republic:
Budova Park one
Námestie 1. mája 18
811 06 Bratislava
Slovak Republic
Email: statny.dozor@pdp.gov.sk

12. Automated Decision-Making and Profiling

The App does not use automated decision-making or profiling that would produce legal effects or similarly significant effects on users.

13. Marketing and Tracking

The App is not used for marketing, advertising, or behavioral tracking.

VIPO a.s. does not use the App to track users across third-party applications or websites for advertising purposes.

14. Children's Privacy

The App is intended exclusively for authorized employees, contractors, and service technicians. It is not intended for children or for public consumer use.

15. Changes to This Privacy Policy

This Privacy Policy may be updated from time to time to reflect changes in the App, legal requirements, or internal data protection practices.

The latest version of this Privacy Policy will always be made available to users.

16. Contact Information

For any questions, requests, or concerns regarding this Privacy Policy or the processing of personal data, please contact:

VIPO a.s.
Gen. Svobodu 1069/4
958 01 Partizánske
Slovakia
Email: info@smartmaintenance.sk