Version: 3.1
Version Date: 11th July 2025

General Technical and Organisational Measures

for internal business operations

Art. 32 GDPR

PTM EDV Systeme GmbH

https://www.mscrm-addons.com/

https://www.poweraddons.com/

PTM EDV-Systeme GmbH
Julian Handl (Office Manager)
Bahnhofgürtel 59
8020 Graz
Austria
Phone: +43 (316) 680 880 41
E-Mail: gdpr@ptm-edv.at

Table of contents

1 Introduction and general framework

1.1 Introduction

This document outlines the internal technical and organisational measures (TOMs) of PTM EDV Systeme GmbH. It describes safeguards implemented within the company's own infrastructure and operations. It does not cover the processing of customer data via our SaaS products or any services delivered through Microsoft Azure.

If you require information on the TOMs related to our SaaS delivery, please contact our Data Protection Coordinator.

This document is structured in accordance with Art. 32 GDPR and aligned with established security frameworks, including ISO/IEC 27001:2022, which PTM has been certified against since April 2024.

1.2 Company / Authority

The following specifications represent the data protection concept of the

PTM EDV-Systeme GmbH
Julian Handl (Office Manager)
Bahnhofgürtel 59
8020 Graz
Austria
Phone: +43 (316) 680 880 41
E-Mail: gdpr@ptm-edv.at

1.3 Person of the company / authority responsible for data protection

DPO Consult GmbH
Karl Pusch (Data Protection Officer)
Joanneumring 18
8010 Graz
Austria
E-Mail: gdpr@ptm-edv.at

2 Technical and organisational measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the following:

2.1 Ensuring the confidentiality

2.1.1 Access control

Suitable measures suitable for preventing unauthorised persons from gaining access to data processing systems where personal data are processed or used.

Measures:

- Security service provided by the building management
- Chip cards / transponder systems
- Key management with a list
- Careful selection of cleaning personnel
- Monitored entrance area
- Visitors only accompanied by staff
- Alarm system monitors the office premises outside of business hours
- Video surveillance system configured for office premises outside of business hours
- Video surveillance system configured for server room 24/7
- Server room equipped with nuki.io access system (Nuki Smart Lock)
- Designated security areas with their own protective measures
- Key management with E-Lock secured key boxes
- Storage within the building, locked with a separate lock.
- Analog visitor list, recording all non-employee individuals

- Clear policy on the acceptable use of office facilities according to ISO27001

2.1.2 Admission control

Suitable measures for preventing data processing systems (computers) from being used by unauthorised persons.

Measures:

- 2FA-Login for access off-premises
- Creating user profiles with least-privilege user permissions
- Password requirement with password policies (must contain at least 10 characters, 8 alphanumeric characters, uppercase and lowercase letters, a number, and a special character)
- Secure Password Management (KeePass)
- Annual requirement of password change
- Brute-Force protection of user accounts
- Anti-virus and anti-malware software
- Use of software firewall
- Automatic screen lock after 10 minutes
- Management of user permissions by a system administrator
- Login with username and password
- Authentication with SSH keys
- Logged access control for all users (log files)

2.1.3 Data access control

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

Measures:

- Access management according to ISO27001 with quarterly review by the ISMS team

- Use of the minimum number of administrators
- Management of user rights by administrators
- Secure storage of data carriers and documents
- Use of document shredders of service providers
  There is a box with data carriers in the server room - a certified shredder from the company Reisswolf destroys the data at regular intervals.

2.1.4 Separation control

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Measures:

- Separation of productive and test environment
- Control via an authorisation concept
- Setting database rights
- Anonymization/pseudonymization of personal data on test system

2.2 Ensuring the integrity

2.2.1 Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or during their transport or storage on data media. Furthermore, it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

Measures:

- Functional responsibilities
- Provision of encrypted connections such as sftp, https and SSH
- Provision of encrypted storage media (hard disks encryption)
- Logging of accesses and requests
- Ext. data transfer via USB sticks is blocked. In exceptional cases, with the approval of the management, the USB port will be activated for a limited period of time.
- Clear policy on acceptable use of sensitive data according to ISO27001
- Data-loss-prevention measures implemented for devices and cloud-services

2.2.2 Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into, modified or removed from data processing systems.

Measures:

- Use of access rights
- Logging in the server log files
- Technical logging if data is changed
- Technical logging if the data is deleted
- Clear responsibilities for the deletion of data

2.3 Pseudonymisation and encryption

2.3.1 Pseudonymisation

Measures that ensure the pseudonymisation of data.

Measures:

- Pseudonymization of personal data on test systems if necessary

2.3.2 Encryption

Measures that ensure encryption of data.

Measures:

- Local backups, daily and weekly with AES 256-bit encryption
- Cloud backups, daily and weekly with AES 256-bit encryption (encryption from the side of PTM-EDV and the cloud provider Microsoft, also AES 256-bit encryption)
- All company computers are encrypted using Bitlocker
- External access to company resources via SSL VPN tunnel + 2FA
- The encryption protocol TLS 1.2 or higher is used.

2.4 Ensuring the availability, resilience and recoverability

2.4.1 Availability (of the data)

Measures to ensure that personal data is protected against accidental destruction or loss - ensuring availability of the data.

Measures:

- Business continuity and disaster recovery policy according to ISO27001
- Daily, weekly, or monthly backups depending on the importance of the application
- SLA with hosting service provider
- 99.95% availability of network connection
- Backup & recovery concept in place
- RAID system / disk mirroring
- Uninterruptible power supply (UPS)

2.4.2 Resilience (of the systems)

Measures to ensure that personal data is protected against accidental destruction or loss - ensuring resilience of the systems.

Measures:

- Installation of current security updates on all application servers
- Use of software firewalls
- Backup & Recovery Plans
- Vulnerability Management according to ISO27001

2.4.3 Recoverability (of the data / systems)

Measures to ensure that personal data is protected against accidental destruction or loss - ensuring recoverability of the data and systems.

Measures:

- Backup & Recovery Concept available and tested annually
- Fire extinguisher in the server room
- Temperature & Humidity alerting system in the server room
- Maintenance Plan for server executed and reviewed annually

2.5 Procedures for regular review, assessment and evaluation

2.5.1 Order control

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Measures:

- Vendor Management according to ISO27001
- Prior review of the safety measures taken by the contractor / documentation
- Selection of the contractor under due diligence aspects (all critical-risk vendors are at least ISO27001 or SOC2 certified)
- Provision of the necessary commissioned data processing agreement
- Provision of the necessary standard contractual clauses
- Obligation of the contractor's employees to maintain data secrecy
- Review of the contractor's level of protection (initial)
- Review of the contractor's level of protection (continuous)
- Agreement on effective control rights

2.5.2 Data protection management

Measures to ensure that the methods have been evaluated to systematically plan, organise, manage and control the legal and operational requirements of data protection.

Measures:

- Use of software solutions for data protection management

- Use of a ISMS Management Tool according to ISO27001
- Implementation of improvement proposals
- Documentation of all data protection procedures and regulations
- Access options for employees on data protection regulations (Wiki / Intranet)
- Review of the effectiveness of the TOMs (carried out at least annually)
- Appointment of an internal data protection coordinator
- Appointment of an external data protection officer (certified)
- Obligation of employees to data secrecy
- Regular sensitisation of employees on data protection (mandatory yearly cyber-security and phishing trainings)
- Compliance with the information requirements pursuant to Art. 13 GDPR
- Compliance with the information obligations pursuant to Art. 14 GDPR

2.5.2.1 Data protection audit

To ensure a high and up-to-date level of security and compliance, PTM EDV Systeme GmbH undergoes an annual ISO27001 audit as part of its certified ISMS. The certificate can be provided upon request.

2.5.3 Incident-Response-Management

Measures that ensure that security incidents can be prevented or in the case of security incidents that have already occurred, that data and systems can be protected and that rapid analysis and remediation of the security incident can be carried out.

Measures:

- Incident Response Management according to ISO27001
- Existing incident report form for all employees with accompanying process
- Use of a firewall and regular updates
- Use of spam filters and their regular updating
- Use of an Intrusion Prevention Systems (IPS)

- Use of an Intrusion Detection System (IDS)
- Use of virus scanners and their regular updating
- Use of SIEM Tool (Wazuh) implemented on both internal and external resources

2.5.4 Data protection-friendly default settings

Measures that ensure that a certain level of data protection already exists in advance through the appropriate technical design (privacy by design) and factory settings (privacy by default) of a software.

Measures:

- Personal data is only collected for the purpose for which it is required
- Ensuring the easy exercise of data subjects' rights, including the right to:
  - Information
  - Correction or deletion
  - Restriction of processing
  - Data portability
  - Withdrawal