Version: 2.0
Version Date: 10th July 2025

Specific Technical and Organisational Measure

for SaaS Product Delivery via Microsoft Azure

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: Julian.handl@mscrm-addons.com

Table of contents

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

1 Introduction and general conditions

1.1 Introduction

This document outlines the technical and organisational measures (TOMs) of PTM EDV Systeme GmbH for services delivered via Microsoft Azure. It covers all security-related aspects of customer data processing in the context of our SaaS products. It does not include internal company measures unrelated to cloud-based service delivery.

If you require information on our internal TOMs, 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

PTM EDV-Systeme GmbH
Julian Handl (Office Manager)
Bahnhofgürtel 59
8020 Graz
Austria
Phone: +43 (316) 680 880 41
E-Mail: Julian.handl@mscrm-addons.com

1.3 Person of the company / authority responsible for data protection

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

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

2 Technical and organizational measures

Considering the state of the art, the costs of implementation and the nature, scope, circumstances 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 organizational measures to ensure a level of security appropriate to the risk, which shall include:

2.1 Ensuring the confidentiality

2.1.1 Access control (physical)

Suitable measures for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

Responsibility lies with Microsoft. Please refer to:

- https://learn.microsoft.com/en-us/azure/compliance/

2.1.2 Access control (digital)

Suitable measures for preventing data processing systems (computers, servers, services) from being used by unauthorized persons.

While Microsoft ensures infrastructure-level access control, PTM actively manages the application layer:

- User access roles defined and managed by PTM
- Minimum number of admin accounts (principle of least privilege)
- 2-factor user authentication and IP whitelisting for access to Azure resources
- Audit Logs in Azure AD enabled
- Automatic screen lock of Azure Virtual-Servers after 10 minutes
- Deployment of software firewalls for Azure virtual servers
- 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)
- Access management according to ISO27001 with quarterly review by the ISMS team

2.1.3 Data access control

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

Measures:

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

- PTM has no access to customer data unless explicitly authorized for support or debugging

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:

- Data of different customers is logically separated by service. Each environment requires its own service
- Debug files, if generated, are isolated and auto-deleted after 7 days

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

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:

- The cloud service communicates securely with Dynamics 365 web services using methods provided by the Dynamics 365 SDK (TLS 1.2, OAuth authentication).

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:

- Input control is the responsibility of the customer. PTM doesn't have any impact on the data provided by the customer.

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

2.3 Pseudonymization and encryption

2.3.1 Pseudonymization

Measures that ensure pseudonymization of data.

Measures:

- Pseudonymization is the responsibility of the customer. PTM doesn't have any impact on the data provided by the customer.

2.3.2 Encryption

Measures that ensure encryption of data.

Here we refer to the Microsoft Azure Services catalog of measures:

- https://learn.microsoft.com/en-us/azure/compliance/
- https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

2.4 Ensuring 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.

Here we refer to the Microsoft Azure Services catalog of measures:

- https://azure.microsoft.com/de-de/support/legal/sla/

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.

Here we refer to the Microsoft Azure Services catalog of measures:

- https://learn.microsoft.com/en-us/azure/compliance/

2.4.3 Recoverability (of the data / the systems)

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

Measures:

- PTM does not maintain persistent copies of customer data.
- Temporary files in exceptional cases (debugging, specific multi-part docs &customer-enabled file storage in PTMs Azure Blob) are automatically deleted after 7 days
- Azure offers robust recovery options for infrastructure

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

2.5 Procedures for regular review, assessment and evaluation

2.5.1 Order control

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

Measures:

- PTM provides a pre-defined Data Processing Agreement (DPA) in accordance with Art. 28 GDPR.
- Subprocessors are selected with due diligence and contractually bound in line with GDPR requirements.
- All PTM employees are contractually obligated to maintain data secrecy.
- The use of subprocessors is transparently documented and communicated.
- The level of data protection at subprocessors is reviewed both initially and regularly.
- Customers are granted effective audit and control rights as defined in the DPA.

2.5.2 Data protection management

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

Measures:

- ISO27001 certified ISMS
- Use of software solutions for data protection management
- Implementation of improvement proposals
- Documentation of all data protection procedures and regulations
- Access options for employees to data protection regulations (Wiki / Intranet)
- Review of the effectiveness of the TOMs (carried out at least annually)
- Appointment of an internal data protection officer
- Obligation of employees to maintain data secrecy
- Regular sensitization of employees on data protection and phishing.
- Compliance with the information requirements pursuant to Art. 13 GDPR
- Compliance with the information obligations pursuant to Art. 14 GDPR
- Data protection according to “Standard-Datenschutzmodell V3”
- The regulation of data subject rights takes place within the framework of the data processing contract
- Responsibility for data minimization lies on the customer side

2.5.2.1 Data protection audit

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

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.

- Internal Monitoring for all essential resources (e.g. Azure Virtual Machine Instances, SQL servers & flow components)
- External monitoring checks the availability of the Azure machines on the Internet every 10 minutes and sends out alarm emails if necessary
- Azure Health Monitoring sends SMS and email in case of problems
- Responsible and notified person are the senior developers in the company, with at least one person available at all times
- When problems occur, if the problem is not obvious, a support case is normally opened at Microsoft at the same time (via Business Critical Incident) if the internal problem-solving approaches are unsuccessful.

Furthermore, we refer to the Microsoft Azure Services catalog of measures.

- https://learn.microsoft.com/en-us/azure/compliance/
- https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

2.5.4 Data privacy-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.

(Main) Measures:

- No data is stored unless explicitly configured/triggered by the customer (e.g. debugging, multipart generation, optional Blob Storage).
- Temporary files are automatically deleted after 7 days.
- The customer selects the data center and therefore the processing location.
- Soley the customer defines what data is processed via template and service configuration.
- Solutions are fully integrated and run in the background as add-ons within the customer's environment.
- Roles and access to the solutions are managed entirely through the customer's Microsoft Entra ID (Azure AD).
- The Service Admin Account on the website supports Multi-Factor Authentication (MFA); credential management via Azure AD B2C
- Online payments are processed exclusively via certified external provider (Stripe and PayPal)

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0
Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at
Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815
Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403

- Azure-based services use TLS 1.2+ by default and enforce encryption transit (Microsoft SDK Standard)
- All services follow the “least privilege” principle; default configurations limit access to only what's technically required.

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria
Tel +43 (0)316 680 880-0

Fax +43 (0)316 680 880-25
office@ptm-edv.at
www.ptm-edv.at

Steiermärkische Sparkasse
Ktonr: 1100-811700
Blz: 20815

Gericht: Firmen-als Handelsgericht Graz
FN: 173442m
DVR: 978663
UID: ATU45695403