Technical and organisational measures according to Art. 32 GDPR

Technical and organisational measures

PTM EDV Systeme GmbH –

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

PTM EDV-Systeme GmbH
Julian Handl (Administration)
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 framework

1.1 Introduction

Organisations that collect, process or use personal data themselves or on behalf of others shall take the technical and organisational measures necessary to ensure the implementation of the provisions of the data protection laws. Measures are only necessary if their effort is in a reasonable relation to the intended protective purpose

1.2 Company / Authority

The following specifications represent the data protection concept of the

PTM EDV-Systeme GmbH
Julian Handl (Administration)
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)
Am Eisernen Tor 2/III
8010 Graz
Austria
Phone: 0800224488
E-Mail: dpo@dpo.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 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:

- 2FA-Login for all projects
- Security guard service is provided by the building management
- Automated system of access control
- Chip cards / transponder systems
- Key control with a list
- Care in the selection of cleaning staff
- Monitored entrance area
- Visitors only accompanied by staff
- Alarm system monitors the offices and the server systems
- Access system nuki.io Nuki Smart Lock

2.1.2 Admission control

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

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

- Assignment of user rights
- Creation of user profiles
- Password assignment
- Assignment of user profiles to IT systems
- Anti-virus software
- Use of a software firewall
- Management of rights by a system administrator
- Login with username and password
- Management of user permissions
- Authentication with SSH Keys
- Logged access authorisations for the system admins and the management (LOG FILES)
- Storage in the building, locked with separate lock. Access authorisation see list
- Analogue visitor list, all external persons are recorded

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:

- 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.
- On any computer/PC/notebook

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

2.1.4 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

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:

- Functional responsibilities
- Provision of encrypted connections such as sftp, https
- 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.

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

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 Pseudonymisation and encryption

2.3.1 Pseudonymisation

Measures that ensure the pseudonymisation of data.

Measures:

- Internal instruction to pseudonymise personal data in case of disclosure
- Internal instruction to pseudonymise personal data after expiry of the deletion period

2.3.2 Encryption

Measures that ensure encryption of data.

Measures:

- No 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

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:

- Daily backups depending on the application
- Operation of high availability web servers
- SLA with hosting provider
- 99,95% availability of the network connection see documentation
- Availability of server hardware see documentation
- Weekly backups
- Backup & recovery concept
- RAID system / hard disk mirroring
- Data backup concept available
- Uninterruptible Power Supply (UPS)
- Monthly backups

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

2.4.3 Recoverability (of the data / systems)

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

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

Measures:

- Restoring databases and file systems from the web server backup
- Fire extinguisher in the server room
- Server room has no windows
- Server room is separate from workstations

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:

- Prior review of the safety measures taken by the contractor / documentation
- Selection of the contractor under due diligence aspects
- Provision of the necessary commissioned data agreement
- Provision of the necessary standard contractual clauses
- Obligation of the contractor's employees to maintain data secrecy
- Regulation on the use of subcontractors
- Review of the contractor's level of protection (initial)
- Review of the contractor's level of protection (continuous)
- Agreement on effective control rights vis-à-vis the contractor

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.

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

Measures:

- Use of software solutions for data protection management
- 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 officer
- Obligation of employees to data secrecy
- Regular sensitisation of employees on data protection
- Compliance with the information requirements pursuant to Art. 13 GDPR
- Compliance with the information obligations pursuant to Art. 14 GDPR

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:

- Use of a firewall and regular updates
- Use of spam filters and their regular updating
- Use of an Intrusion Prevention Systems (IPS)
- Use of virus scanners and their regular updating

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:

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

- Personal data is only collected for the purpose for which it is required
- Ensuring an easy exercise of the right of withdrawal of a data subject

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