Data Protection:

General technical and organizational measures

Contents

Document information

Short title	TOMs_EN
Edited by:	Philipp RUDI (PTV Group)
Version:	2.0.3
Author:	Bastian SCHNEIDER (PTV Group)
Created on:	19.06.2023

Technical and organizational measures (TOMs)

Organizations that collect, process or use personal data themselves or on behalf of others must take the technical and organizational measures necessary to ensure compliance with the provisions of the data protection laws (Art. 32 GDPR). The measures must be suitable to adequately protect the personal data according to their nature and category. The measures are only necessary if their effort is in a reasonable relation to the intended protection purpose.

In order to meet the requirements for data processing security, PTV Planung Transport Verkehr GmbH takes the following measures:

1 Confidentiality (Art. 32 Sect. 1 lit. b GDPR).

1.1 Physical Access Control

No unauthorized access to data processing systems

- Carefully selected security service
- Video surveillance of the entrance areas of the building and the data center
- Access to the building only via chip key (transponder system)
- Chip keys are assigned in accordance with the access authorization concept of the access management software. A list is kept of the assignment. Granting and changes of the authorization only in compliance with the 4-eyes principle.
- Within the building, Chip-Key grants access to specific areas only under consideration of the business hours and the authorization group.
- Staffed reception during business hours. Admission of visitors only after ringing the bell, opening of access door by receptionist
- Keeping of a visitor book with visitor log
- Visitors are only allowed in the building with a visitor's badge and in the company of a PTV employee.
- Securing sensitive areas with security locks, locking systems only with appropriate authorization by means of chip key (e.g. server room)
- Careful selection of external service providers, e.g. cleaning staff. Obligation to comply with data protection and confidentiality
- Stay of craftsmen only in the company of facility management staff.
- Securing of building shafts.

1.2 System Access Control

No unauthorized system use

- Login with user name and either password or pin
- Guidelines to: "Secure password", password can only be set if security requirements are met
- Anti-virus software for servers, clients, mobile devices
- Firewall
- Mobile device systems, policy on use and password assignment
- Time limit on password validity and password history
- Encryption of data media, notebook hard drives and smartphones
- Managing user permissions
- Policy and default setting "desktop lock", reactivation password protected

1.3 Authorization Control

No unauthorized reading, copying, modification or removal

- Authorization and administration concept in place, minimum number of administrators
- Concept for requesting and approving authorizations
- User roles / group concept
- Administration of user rights by administrators
- Access check by protocol for entry, modification and deletion
- External document shredder (DIN 32757) and secure storage of documents provided for destruction

1.4 Separation Control

Separate processing of data serving different purposes

- Processing of company data separately from the respective customer data
- Separation of relevant productive and test environments
- Multi-client capability of relevant applications

1.5 Pseudonymization

Priority of processing pseudonymized data, as far as this is possible

- Internal instruction to anonymize/pseudonymize personal data as far as possible in the event of disclosure
- Separate storage of pseudonymized data and assignment data in separate and secured system

2 Integrity (Art. 32 Sect. 1 lit. b GDPR)

2.1 Disclosure Control

No unauthorized reading, copying, modification or removal during electronic transmission or transport

- VPN use
- Encryption of notebook hard drives
- Logging of unauthorized external access attempts
- Provision via encrypted connections (sftp, https)

2.2 Input Control

Determination of whether and by whom personal data has been entered into systems, changed or removed

- Logging of all entries in relevant programs
- Overview of programs by means of which data can be entered, changed or deleted
- Traceability of input, modification and deletion through individual user names (not user groups)
- Assignment of rights for entering, changing and deleting data on the basis of an authorization concept
- Clear responsibilities for deletions

3 Availability and Resilience (Art. 32 Sect. 1 lit. b GDPR)

3.1 Availability Control

Protection against accidental or deliberate destruction or loss

- Fire and smoke detection systems
- Air conditioning and monitoring of the server room (temperature and humidity); video surveillance, CO2 fire extinguishers
- USV
- Protective socket strips in the server room
- RAID hard disk storage
- Backup and recovery concept (formulated)
- Control of the backup process
- Regular tests for data recovery and logging of results

- Storage of backup media in a safe place outside the server room
- Daily to annual backups, additional backups and tested backups,
- Tested emergency concept
- Virus scanner and multi-level firewalls
- Regular software updates
- Storage of backups in specially suitable data vaults

4 Procedures for regular Review, Assessment and Evaluation (Art. 32 Sect. 1 lit. d; 25 Sect. 1 GDPR)

4.1 Order Control (outsourcing, subcontractors)

Measures to ensure that personal data processed under contract can only be processed in accordance with the client's instructions:

- Prior review of the security measures taken by the contractor and their documentation.
- Selection of the contractor under due diligence aspects (in particular with regard to data protection and data security)
- Conclusion of the necessary contract agreement or EU standard contractual clauses
- Written instructions to contractor
- Obligation of the contractor's employees to maintain data secrecy
- Obligation to appoint a data protection officer by the contractor if an obligation exists
- Agreement on effective control rights
- Regulations on the use of further subcontractors
- Ensuring the destruction of data after completion of the order
- In the case of longer cooperation: Ongoing review of the contractor and its level of protection.

4.2 Data Protection Management

Together with the external data protection officer, a data protection management system (DSMS) is maintained in which all measures, procedures, activities, etc. are mapped. The DSMS contains the most important data protection requirements and a comprehensive structure for mapping data protection measures. The DSMS is maintained and updated on an ongoing basis. The data protection officer is supported by internal data protection coordinators.

- Our employees are obligated to comply with data privacy and confidentiality, training courses
- Implementation of data protection impact assessments (DPIA) as required

- Observance of the information obligations according to Art. 13, 14 GDPR for organization

4.3 Incident Response Management

An organizational and technical process for dealing with security incidents is defined and implemented. This also ensures a uniform response and proceduralized handling of detected and suspected security incidents/malfunctions. This also includes uniform follow-up and monitoring as part of a continuous improvement process.

- Use of firewall, spam filters and virus scanners. Regular updating
- IT ticket system in the event of an incident
- Involvement of data protection officers and information security officers.
- Data protection-friendly default settings
- In principle, only data that is appropriate and necessary for business purposes is collected and processed. Procedures for automated data collection and processing are designed in such a way that only the necessary data is collected.
- No more personal data is collected than is necessary for the respective purpose.
- Simple exercise of the data subject's right of revocation through technical measures.

5 Data protection officer

PTV Planung Transport Verkehr GmbH has appointed an external data protection officer (Art. 38 and 39 GDPR). He can be reached at:

data-protection@ptvgroup.com