Technical and organisational measures – overview

Personio has taken the following technical and organisational measures within the meaning of Article 32 of the GDPR in order to ensure confidentiality, encryption, pseudonymisation, integrity, availability, resilience, recoverability and corresponding audit procedures.

1. Confidentiality

1.1 Organisational management

The aim is to ensure that the internal organisation meets the specific requirements of data protection.

Personio implemented the requirements as follows:

X	Organisational instructions (as per 5 and 6 ISO/IEC 27002/2017)	X	Appointment of a data protection officer
X	Obligation to maintain confidentiality and data protection	X	Data protection training
X	Restrictions on personal and business use of communication devices	X	Reliability of staff (as per 7 ISO/IEC 27002:2017)

1.2 Encryption and pseudonymisation of personal data

It is ensured that personal data is only stored in the system in a manner that prevents third parties from identifying the data subjects.

Personio implemented the requirements as follows:

X	Key management (as per 10.1.2 ISO/IEC 27002:2017)	X	Database and storage encryption

X	Data transmission via encrypted data networks or tunnel connections (data in transit)	X	Encryption of mobile storage media
X	Encryption of storage devices on laptops	X	Encrypted exchange of information and files
X	Email encryption		

1.3 Physical access control

Access by unauthorised persons to the IT system and processing facilities, by means of which the processing is carried out, is prohibited.

Personio implemented the requirements as follows:

X	Electronic door locks	X	Controlled and documented key distribution
X	Supervision and accompaniment of strangers	X	Securing rooms with an increased need for protection
X	Closed doors and windows	X	Physical and environmental security of server systems in data centres
X	Deployment of security staff	X	Other: Use of employee ID cards to identify authorised persons and to open locked doors Video surveillance in sensitive areas (data centre)

1.4 Authorisation check

The use and processing of data protected under data protection law by unauthorised persons is prevented.

Personio implemented the requirements as follows:

X	Use of authentication procedures	X	Authorisation determination and assignment following approval by administration
X	Use of secure passwords	X	Prohibition of sharing passwords and use of shared accounts
X	Automatic lockout in the event of inactivity	X	Use of antivirus software

X	Clean desk policy	X	VPN connection to public wireless networks and connection to company network

1.5 Access control

It shall be ensured that persons authorised to use an automated processing system only have access to the personal data for which they have access authorisation.

Personio implemented the requirements as follows:

X	Role and authorisation concept	X	Control of access rights to customer systems by the contracting entity
X	Assignment of access rights	X	Host-based intrusion detection system (IDS)
X	Grid security	X	Logging of processes relating to logging in and logging out

1.6 Separability

It is ensured that personal data collected for different purposes can be processed separately and separated from other data and systems in such a way as to prevent unplanned use of such data for other purposes.

Personio implemented the requirements as follows:

X	Separation of development, test and operating environments (as per 12.1.4 ISO/IEC 27002:2017)	X	Separation of networks (as per 13.1.3 ISO/IEC 27002:2017)
X	Client separation on the software side		

2. Integrity

2.1 Transmission control

It is ensured that the confidentiality and integrity of private data are protected during the transmission and transport of the storage media.

Personio implemented the requirements as follows:

X	Transmission encryption (data in transit)	X	Prohibition of disclosure to unauthorised third parties

2.2 Input control

The aim is to ensure that it is possible to subsequently check and determine which personal data has been entered or changed into automated processing systems at what time and by whom.

Personio implemented the requirements as follows:

X	Logging of system activities in admin and customer systems as well as evaluation		

3. Availability

3.1 Availability control

Ensure personal data is protected against accidental destruction or loss.

Personio implemented the requirements as follows:

X	Data backup procedures/backups	X	Geo-redundancy with respect to the server infrastructure of productive data and backups
X	Capacity management	X	Warning systems to monitor the availability and condition of server systems
X	IT fault management (as per 16 ISO/IEC 27002:2017)	X	Fire detection and firefighting system
X	Uninterruptible power supply		

3.2 Restorability

It is ensured that systems can be reliably recovered in the event of a physical or technical failure.

Personio implemented the requirements as follows:

X Disaster recovery concept

4. Review and evaluation

Description of the procedures for regularly reviewing, assessing and evaluating the effectiveness of technical and organisational measures.

Personio implemented the requirements as follows:

X	Establishment of the Data Protection and Information Security Team	X	Risk management
X	Independent review of information security (as per 18.2.1 ISO/IEC 27002:2017)	X	Carrying out internal audits
X	Verification of compliance with security policies and standards (as per 18.2.2 ISO/IEC 27002:2017)	X	Verification of compliance with technical specifications (as per 18.2.3 ISO/IEC 27002:2017)

X	Procedures for continuous improvement of the data protection and information security management system	

4.1 Contract monitoring

It is ensured that private data processed on behalf of the customer can only be processed in accordance with the customer's instructions.

Personio implemented the requirements as follows:

X	Data processing pursuant to Article 28 of the GDPR	X	Careful selection of suppliers
X	Carrying out regular checks/requesting evidence		