Technical and organisational measures

in accordance with the GDPR

Table of Contents

Data processor

InterMedia Solutions GmbH
(hereinafter referred to as IMS)
Ahornstr. 7, 82041 Oberhaching near Munich

Contact person: Robert Holzer
Phone: +49 89-244 151 51
Email: datenschutz@intermedia-solutions.de

1.0 Confidentiality

1.1 Entry control

Measures that are appropriate to prevent unauthorised access to data processing equipment
with which personal data is processed or used.

Technical measures: bell system with camera, security locks, manual locking system, alarm system, video surveillance of the entrances.

Organisational measures: visitors are accompanied by employees, cleaning services are carefully selected, key regulation

1.2 Data access control

Measures that are appropriate to prevent data processing systems from
being used by unauthorised persons.

Technical measures: login with username + password, anti-virus software server, anti-virus software clients, firewall, use of VPN for remote access, encryption of data carriers, automatic desktop lock, encryption of notebooks,

Organisational measures: creation of user profiles, central password assignment, "secure password" policy, general Privacy Policy

1.3 Physical access control

Measures to ensure that those authorised to use
a data processing system can only access
data subject to access authorisation, and that
personal data during processing, use and after storage
can not be read, copied, altered or removed by any unauthorised persons.

Technical measures: access logging

Organizational measures: no unauthorised reading, copying, modifying or removing within the system, e.g.: authorisation concepts and access rights according to requirements

1.4 Separation control

Measures to ensure that data collected for different purposes
can be processed separately.

Technical measures: separation of productive and test environment, physical separation (systems/databases/data carriers)

Organisational measures: control via authorisation concept, definition of database rights

2.0 Integrity

2.1. Disclosure control

Measures to ensure that personal data
cannot be read, copied, altered or removed without authorisation
during electronic transmission or during transport or storage on data carriers
and that it is possible to verify and establish to which bodies
personal data is transmitted through data transmission facilities.

Technical measures: technical logging of the entry, modification, and deletion of data, manual or automated control of the logs

Organisational measures: granting of rights to enter, change and delete data based on an authorisation concept, storage of forms from which data was transferred to automated processing

2.2 Entry control

Measures to ensure that subsequent checks and determinations can be made
whether and from whom personal data has been
entered into, modified, or removed from data processing systems
Technical measures: email encryption, use of VPN, logging of access and retrieval, provision via encrypted connections such as sftp and https, electronic signatures

Organisational measures: documentation of the data recipients and the duration of the planned transfer or the deletion periods, disclosure in anonymous or pseudonymised form, careful selection of transport personnel and vehicles

3.0 Availability and reliability

3.1 Availability control

Measures to ensure that personal data is protected against accidental destruction or loss.

Technical measures: fire and smoke alarm systems, fire extinguishers, server room surveillance, air-conditioned server room, RAID system/hard drive mirroring, uninterruptible power supply
Organisational measures: backup strategy (online/offline; on-site/off-site), control of the backup process, separate partitions for operating systems and data

4.0 Procedures for periodic review, assessment and evaluation

4.1 Data protection measures

Technical measures: data protection management, verification of effectiveness of the technical protective measures is carried out at least once a year

Organisational measures: employees are trained and committed to confidentiality/data secrecy, regular sensitisation of
employees, the organisation meets the information requirements under Art. 13 and 14

of the GDPR.

4.2 Incident response management

Technical measures: use of firewalls and regular updates, use of spam filters and regular updates, use of virus scanners and periodic update

Organisational measures: procedure for dealing with security incidents, documentation of security incidents and data breaches

4.3 Data protection-friendly presettings

Technical measures: no more personal data is collected than is necessary for the respective purpose, easy use of the right of withdrawal of the data subject through technical measures

4.4 Order control (outsourcing to third parties)

Measures to ensure that personal data processed in the order can only be processed according to Client's instructions.

Organisational measures: no order data processing within the meaning of Art. 28 of the GDPR without corresponding instructions of the Client, e.g., clear contract design, formalised order management, strict selection of the service provider, compulsory pre-compilation, follow-up checks.