



Technical and organisational measures **(TOM)**

Organisations processing personal data (PII) whether collecting, processing, or using such data have to implement technical and organisational measures to ensure compliance with applicable data protection requirements. Measures are only required if the effort involved is proportionate to the intended protective purpose.

movingimage EVP GmbH
Tempelhofer Ufer 1
10961 Berlin

complies with this requirement by the following measures:

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

1.1 Access Control I

Physical measures that are suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data is processed or used

Technical Measures

Alarm system

Automatic access control system with card reader (magnetic/ chip card)

Door security

Security locks

Transponder locking system

Doorbell system with camera

Video surveillance of the entrances

Fireproof doors

Motion detector

Security doors/ windows

Organizational Measures

Key policy

Reception with registration

Guest book

Guest passes/ badges

Guests are accompanied

Careful selection of cleaning staff

Information security guidelines

Work instructions for access control

Work instructions for occupational safety

Employee and authorisation badges

1.2 Access Control II

Logical measures that are suitable for preventing data processing systems from being used by unauthorised persons

Technical Measures

Minimum requirement for password assignment
 Authentication with at least username and password
 Use of 2-factor authentication for all compatible systems
 Use of VPN
 Automatic locking of workstations after period of inactivity
 Use of anti-virus and anti-malware software
 Use of firewalls
 Encryption of data carriers and servers
 Encryption of devices
 Single Sign-On
 Use of separate privileged user IDs for administrative activities
 Logging of access to systems

Organizational Measures

User rights management
 Individual user accounts
 Information security policies
 Work instructions for access control
 Policy on the use of mobile devices
 Least privilege principle (need-to-know) in role assignment
 Segregation of duties (SoD) in authorisation management

1.3 Access Control III

Measures that 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, changed or removed without authorisation during processing, use and after storage.

Technical Measures

Use of data destruction service providers under consideration of DIN 66399
 Proper deletion of data carriers before their destruction
 Encryption of data carriers and servers
 Secure storage of data carriers
 Deletion concept and policy on retention and deletion periods for data
 Mobile device management system with remote wipe capability

Organizational Measures

Use of an authorisation concept
 Management of user accounts and their authorisations by administrators
 Number of administrators reduced to a necessary minimum
 Information security guidelines
 Approval routines for requesting access rights
 Multiple-eyes principle
 Logging of the destruction of data carriers

1.4 Separation Control

Measures that ensure the separate processing of data collected for different purposes

Technical Measures

Separation of production, test and development systems
Physical separation of systems, databases and carriers
Logical client data separation within the application
Network segmentation

Organizational Measures

Use of an authorisation concept
Definition of database authorisations
Division of tasks
Information security guidelines
Guidelines for the secure development of software

1.5 Pseudonymisation (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

The processing of personal data is done in a way that personal references of data is not accessible without further additional information, in particular an identification key

Technical Measures

Logical separation of real and pseudonymized data
Encryption and protection of real data
Log files are pseudonymised or anonymised

Organizational Measures

Instruction to pseudonymise and anonymize data insofar as this is functionally possible
Encryption guidelines
Information security guidelines
Guidelines for the secure development of software
Privacy Policy
Data protection training for employees

1.6 Encryption (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

The processing of PII is done in a way that the data is amended via cryptographic measures in a way that they are – in particular during transit – not readable without the respective key so that access by an unauthorized third party is excluded

Technical Measures

Encryption and protection of real data
Use of modern encryption technologies

Organizational Measures

Key management guidelines
Encryption guidelines
Information security guidelines
Guidelines for the secure development of software
Data classification guidelines

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

2.1 Transfer Control

Measures to ensure that PII cannot be read, copied, amended, or erased by unauthorized third parties during transfer of such data. Furthermore, such measures ensure the controlling and assessment of the addressees of such transfers

Technical Measures

Use of VPN

Access and retrieval logging

Use of encrypted connections and protocols, e.g. HTTPS for data transmission

Use of encrypted e-mail communication

Secured Wi-Fi

Secured data transport

Secured file transfer

Mobile device management system with remote wipe capability

Logging of the copying, modification or removal of data

Use of secured wide area network (WAN) connections

Organizational Measures

Transmission of data in pseudonymised or anonymised form where possible

Encryption of the data carrier before physical transport

Careful selection of transport personnel and vehicles for physical transport

Logging of the physical handover

Information security guidelines

Data classification guidelines

Regulation on the handling of mobile storage media

Physical transport security

2.2 Input Control

Measures to ensure the retrospective check of whether and by whom PII have been inserted, amended, or erased

Technical Measures

Logging the entry, modification or removal of data

Manual or automated evaluation of the logs

Organizational Measures

Review of the applications that can be used for entering, changing or removing data

Creation and assignment of authorisation profiles for entering, changing or removing data

Information security guidelines

Processes for the secure deletion of data

Functional responsibilities and organisationally defined competencies

Multiple-eyes principle



2.3 Documentation Control

Measures to ensure that the procedural methods of the processing of PII are documented in a way that they are traceable

Technical Measures

Version control for source code and configuration changes
Use of infrastructure as code for traceable management of infrastructure changes

Organizational Measures

Use of an architecture diagram
Data classification guidelines
Information security guidelines

3 Availability and resilience (Art. 32 para. 1 lit. b GDPR)

3.1 Availability Control

Measures to ensure that PII are protected against random destruction or loss

Technical Measures

Use of a cloud provider for all data managed by customers certified according to:

- CSA STAR,
- ISO 9001,
- ISO 22301,
- ISO 27001 and
- ISO 27018

Physical and geographical redundancy of data
Physical separation of operating and file systems
Suitable archive storage facilities for paper documents

Organizational Measures

Disaster concept in place
Maintenance processes
Data classification guidelines
Information security guidelines
Backup processes with regular review, incl. retention process and storage of backups at geographically separate locations



3.2 Resistance & resilience of services/systems

Measures to ensure that the technical systems do not fail completely in case of incidents and/or partial failure, but that main system services continue to run

Technical Measures	Organizational Measures
Use of a cloud provider with data and services recovery option for all data managed for customers certified according to: • CSA STAR, • ISO 9001, • ISO 22301, • ISO 27001 and • ISO 27018	Restore procedures with regular review
Physical and geographical redundancy of data	Information security guidelines
Automation of infrastructure management	Emergency plan with regular emergency drills
System design with a high-availability approach	Risk-based deployment of security updates
Automation of failure scenarios	Designated Business/ Service Continuity Manager role
Use of a CDN for caching media content	
Security concept for software and IT applications	

4 Procedures for regular review, assessment, and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

4.1 Data Protection Management

Technical Measures

Centralized documentation of all
Data protection procedures and regulations
with access for employees as required
Regular vulnerability scans and annual
penetration tests by an independent third
party

Organizational Measures

Appointment of the external
DPO: Charlotte Schieler, ISiCO Datenschutz
GmbH, Am Hamburger Bahnhof 4, 10557
Berlin
Training of employees in the area of data
protection
Inclusion of the data protection aspect in the
planning and development of applications
Appointment of the internal Information
Security Officer
If required, a Data Protection Impact
Assessment (DPIA) is performed
Compliance with the information obligations
according to
Art. 13 & 14 GDPR
Process for handling requests for
information from data subjects
Data protection principles
Maintaining records of processing activities
(Art. 30 GDPR)
External review/ audit of information
security, e.g. as part of the ISO 27001
certification
Formal change management process with
mandatory review and approval of changes
to software, infrastructure and IT services
Guidelines and instructions for ensuring
technical and organisational measures for
data security
Compliance with the internal guidelines and
processes for the certifications listed under
section 5

4.2 Incident-Response-Management

Support for reacting on security breaches

Technical Measures

Use of firewalls

Use of spam filters

Use of anti-virus and anti-malware software

Intrusion Detection System (IDS)

Intrusion Prevention System (IPS)

Organizational Measures

Process for recognizing and reporting security incidents

Process for dealing with security incidents

Involvement of the data protection officer and information security officer in security incidents

Process for notifying the controller of personal data breaches without undue delay (Art. 33 para. 2 GDPR)

Documentation of security incidents

Process for the follow-up of security incidents

Dedicated playbook for responding to phishing incidents

4.3 Data protection-friendly default settings (Art. 25 para. 2 GDPR)

Measures to implement data protection requirements, i.e. data protection by default and data protection by design

Technical Measures

Reduction of the collection of personal data to an appropriate minimum
Simple exercise of the data subject's right of withdrawal of consent through technical measures

Organizational Measures

Inclusion of data protection in the planning and development of applications

Guidelines for the secure development of software

4.4 Processor Control

Measures to ensure that PII processed on behalf of a controller that the processing of such data is done according to the controller's instructions

Technical Measures

Organizational Measures

Inspection of the security measures taken by the contractor and their documentation

Documented procedure for the selection of contractors based on due diligence

Conclusion of the necessary agreement on order processing or EU standard contractual clauses

Written instruction to the contractor

Obligation of the contractor's employees to maintain data secrecy

Obligation to appoint a data protection officer by the contractor if the contractor is subject to a corresponding legal obligation

Agreement of effective control rights vis-à-vis the contractor

Regulation on the use of additional subcontractors

Ensuring the destruction of data after completion of the order

Periodic review of the contractor and its level of protection

Formalised management of processing orders

Process for receiving and following the controller's instructions

Designation of contact persons and/ or responsible employees

Control/ review of processing in accordance with instructions

Standardised testing of the suppliers used

5 Certifications

5.1 Transfer Control

Both the Quality Management System according to ISO 9001 and the Information Security Management System according to ISO 27001 of movingimage, including the data centre operation, underwent several external certifications:

Measures	PwC (TISAX „special data“)	TÜV Nord (ISO 9001, 20000-1, 22301, 27001)
Access Control I	Evaluated on 29.11.2024	Certified on 5.10.2025
Access Control II	Evaluated on 29.11.2024	Certified on 5.10.2025
Access Control III	Evaluated on 29.11.2024	Certified on 5.10.2025
Separation Control	Evaluated on 29.11.2024	Certified on 5.10.2025
Pseudonymisation	Evaluated on 29.11.2024	Certified on 5.10.2025
Encryption	Evaluated on 29.11.2024	Certified on 5.10.2025
Transfer Control	Evaluated on 29.11.2024	Certified on 5.10.2025
Input Control	Evaluated on 29.11.2024	Certified on 5.10.2025
Documentation Control	Evaluated on 29.11.2024	Certified on 5.10.2025
Availability Control	Evaluated on 29.11.2024	Certified on 5.10.2025
Load capacity	Evaluated on 29.11.2024	Certified on 5.10.2025
Data Protection Management	Evaluated on 29.11.2024	Certified on 5.10.2025
Incident-Response-Management	Evaluated on 29.11.2024	Certified on 5.10.2025
Privacy-friendly default settings	Evaluated on 29.11.2024	Certified on 5.10.2025
Processor Control	Evaluated on 29.11.2024	Certified on 5.10.2025