Technical and Organizational Measures (TOMs)

Fotografen Online Service GmbH (FOS) has implemented the following data protection measures to ensure the security of personal data while processed.

A. Pseudonymization Measures

Measures that reduce the direct reference to a person during processing in such a way that an assignment to a specific data subject is only possible with the use of additional information. The additional information is kept separate from the pseudonym by means of suitable technical and organizational measures.

B. Encryption Measures

Measures or processes in which a clearly readable text / information is converted into an illegible, i.e. not easily interpretable, character string (ciphertext) with the aid of an encryption process (cryptosystem):

- Symmetric / asymmetric encryption
- Block algorithms (e.g. AES, 3DES)

C. Measures to Ensure Confidentiality

1. Physical Access Control

Measures that physically deny unauthorized persons access to confidential files and data carriers, IT systems and data processing equipment used to process personal data:

Description of the access control system:

- Building and office doors are secured by card access system
- Access cards are personally assigned to employees
- Server rooms are secured by a physical lock; keys are held by the dedicated employees.

2. Data Access Control

Measures that prevent unauthorized persons from accessing, using or otherwise processing data protected under data protection law.

Description of the access control system:

- Login with username and password
- Login with 2-factor authentication
- Locking of the login process after a defined number of attempts
- Firewalls enabled on clients

- Network management device with firewall
- Locking of server room
- Encryption file system "clients" (notebook, desktop)
- Managing user permissions
- Central password assignment
- "Home office" policy

3. Data Usage Control

Measures to ensure that those authorized to use the data processing procedures can only access the personal data in accordance with their access authorization, so that data cannot be read, copied, modified or removed without authorization during processing and while stored.

Description of the access control system:

- Use of a central network-based authentication service for user.
- Use of password management systems
- Paper is securely destroyed (e.g. document shredder security level P-3)
- Data carriers that cannot be securely deleted are securely destroyed
- Use of authorization concepts
- Regulations for setting up and classifying user IDs, user groups and user rights
- User IDs and authorizations are assigned on the basis of actual need and necessity for task fulfillment ("need-to-know" principle)
- Each user ID is unique and assigned to one person
- Users and user IDs may only be set up and deleted via administrative roles
- Restrictive assignment of rights for third party service providers ("need-to-know" principle)

4. Separation Requirement

Measures to ensure that data collected for specific purposes is processed separately and segregated from other data and systems in a manner that precludes unplanned use of this data for other purposes.

Description of the separation control process:

- Separation of production and test environment (developer environment)
- Separate physical storage for customers and the databases used by customers
- Only administrators have access to administrative functions and interfaces
- Identity and authorization management is in place (authentication server with access to core system)
- User and group IDs are unique

D. Measures to Ensure Confidentiality

1. Data Integrity

Measures to ensure that stored personal data is not damaged by system malfunctions.

Description of data integrity:

- Installation of new releases and patches with release / patch management
- Functional testing of installation and releases/patches by the IT department

2. Transport Control

Measures to ensure that the confidentiality and integrity of data is protected during the transmission of personal data and during the transport of data media.

Description of transport control:

- Use of an encrypted communication protocol on the web server (https)
- Exclusion of physical transports of data carriers

3. Input Control

Measures to ensure that it is possible to check and establish at all times whether and by whom personal data has been entered into DP systems, changed or removed.

Description of the input control process:

- A separate table in the database is used to record which changes are made to the relevant data of a user account by FOS employees or the customer (photographer).

E. Measures to Ensure Availability and Resilience

1. Availability Control

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

Description of the availability control system:

- Data protection procedures
- Possibility of rollbacks
- UPS (Uninterruptible Power Supply)
- No sanitary connections in or above the server room

2. Quick Recoverability

Measures to ensure the ability to rapidly restore the availability of and access to personal data in the event of a physical or technical incident.

Description of the measures taken to ensure rapid recoverability:

- Data backup procedures
- Appropriate version management of the source code (developers)
- Automatic monitoring with email, SMS and phone notifications
- Emergency management
- Employees sensitized to emergency management

3. Reliability

Measures to ensure that all functions of the system are available and that any malfunctions that occur are reported:

Description of reliability measures:

- Automatic monitoring with email, SMS and phone notifications
- IT emergency service 24/7

F. Measures for the Regular Evaluation of the Security of Data Processing

1. Review Process

Measures to ensure data protection compliance and secure processing.

Description of the verification procedures:

- Data protection management
- External data protection officer (DPO) is appointed
- Employees receive regular training and are contractually bound to maintain confidentiality / data secrecy
- Regular employee awareness raising
- Formalized processes for data protection incidents (esp. regular involvement of data protection officer)
- Instructions from the customer are documented
- Formalized process for the engagement of subprocessors

2. Order Control

Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the customer's instructions:

Description of the order control measures:

- Before selection and during engagement of (potential) subprocessors, assessment of data protection and security measures taken and their documentation

- Conclusion of the necessary agreements for commissioned processing or EU standard contractual clauses
- Obligation of the subprocessor's employees to maintain data secrecy
- Obligation of subprocessor to appoint a data protection officer, if required by applicable law
- Agreement on effective control rights vis-à-vis the subprocessor
- Ensuring the destruction of data after completion or termination of a contract
- Instructions from the customer are documented
- Formalized process for the engagement of further subcontractors by subprocessor

Last update: 04/07/2024