Technical and Organizational Measures
pursuant to Art. 32 GDPR
Fotografen Online Service GmbH (GOTPHOTO)

1. Introduction

Fotografen Online Service GmbH (GotPhoto) implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk in accordance with Art. 32 GDPR. These measures are designed to ensure the confidentiality, integrity, availability and resilience of processing systems and services, and to ensure the ongoing ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.

The measures described below apply to all systems and services used to process personal data.

2. Confidentiality

2.1 Physical Access Control

GotPhoto primarily uses certified cloud infrastructure providers for hosting its production systems. No on-premise server infrastructure is operated for core production services.

Cloud data centers used for processing personal data are protected by state-of-the-art physical security measures, including access control systems, surveillance, and restricted access procedures. The cloud provider maintains internationally recognized security certifications (e.g., ISO 27001).

Access to GotPhoto office premises is restricted to authorized personnel. and controlled via electronic badges. Entry to the office is logged electronically and access records can be retrieved when required for security or compliance purposes. All visitors are accompanied by GotPhoto personnel at all times during their visit to ensure adherence to GotPhoto security and data protection standards.

2.2 Logical Access Control (System Access)

Access to internal systems and production environments is granted only to authorized personnel.

The following measures are implemented:

- Individual user accounts for all employees
- Strong password requirements
- Multi-factor authentication (MFA) for administrative and privileged access

- Centralized identity and access management
- Role-based access control
- Immediate deactivation of accounts when employment or assignment ends
- Encrypted communication protocols (e.g., TLS) for system access

Administrative access to infrastructure and cloud services is managed via centralized identity management system with session-based authentication and least-privilege principles.

2.3 Data Access Control (Authorization Control)

Access to personal data is restricted according to the need-to-know principle.

The following safeguards are implemented:

- Role-based authorization concepts
- Separation of duties where appropriate
- Formalized process for granting, modifying and revoking access rights
- Regular review of access rights
- Restrictive assignment of administrative privileges
- Unique user IDs assigned to individuals

Access to source code repositories, databases and administrative interfaces is limited to authorized personnel only.

2.4 Separation Control

Data collected for different purposes and customers is logically separated.

The following measures are implemented:

- Logical separation of development, test and production environments
- Controlled access to administrative functions
- Segregation of customer data within application architecture
- Separation of infrastructure components according to security requirements

3. Integrity

3.1 Data Integrity and Change Control

GotPhoto ensures that personal data cannot be altered or deleted without authorization.

Measures include:

- Role-based permissions

- Logging of access and relevant system activities
- Controlled deployment processes
- Formalized release and change management procedures
- Version control systems for source code
- Secure configuration management

3.2 Secure Transmission

Personal data transmitted over public networks is protected by encryption.

Measures include:

- Encrypted communication via HTTPS (TLS 1.2 or higher)
- Encrypted administrative access protocols
- Prohibition of unencrypted transmission of personal data

3.3 Input Control and Logging

It is possible to determine whether and by whom personal data has been entered, modified or deleted within systems.

Measures include:

- Logging of authentication events
- Logging of administrative activities
- Logging of relevant application-level changes
- System based log management
- Defined log retention periods

Logs are reviewed on demand and in the context of security incident investigations.

4. Availability and Resilience

4.1 Availability Control

GOTPHOTO protects personal data against accidental destruction or loss.

Measures include:

- Hosting in certified cloud environments
- Redundant infrastructure components
- Regular automated backups
- Versioned backups
- Periodic restoration tests

- Continuous system monitoring

4.2 Rapid Recovery

GOTPHOTO maintains processes to restore availability and access to personal data in a timely manner.

Measures include:

- Documented backup and recovery procedures
- Defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Incident and emergency management procedures
- 24/7 monitoring of production systems
- Defined escalation procedures

4.3 Business Continuity

A documented Business Continuity Plan (BCP) is in place. Employees are informed about emergency procedures. The effectiveness of the BCP is reviewed periodically.

5. Data Protection Management and Governance

5.1 Data Protection Organization

GOTPHOTO has appointed:

- An external Data Protection Officer (DPO)
- An internal Information Security Officer (ISO)

Documented policies and procedures are maintained, including:

- Data protection policy
- Information security policy
- Identity and access management policy
- Backup and recovery policy
- Incident response plan
- Remote work and mobile device policies
- Deletion and destruction policy

Employees are contractually bound to confidentiality and receive regular data protection and security awareness training.

5.2 Incident Response Management

GOTPHOTO maintains documented procedures for detecting, reporting and responding to security and data protection incidents.

Measures include:

- Monitoring systems for detecting security-relevant events
- Formalized internal incident reporting procedures
- Involvement of the DPO in data protection incidents
- Documentation and follow-up of incidents
- Procedures for assessing notification obligations

6. Secure Software Development

GOTPHOTO applies secure software development principles.

Measures include:

- Secure system architecture and engineering principles
- Separation of development, test and production environments
- Use of secure coding standards
- Peer review processes
- Prohibition of hard-coded passwords
- Controlled use of third-party components
- Secure repository management
- Access to source code based on need-to-know
- Continuous integration and deployment processes including security checks
- Secure secrets management
- Application of least-privilege and zero-trust principles where appropriate

Security testing (e.g., vulnerability scans and penetration tests) is conducted on a regular basis.

7. Subprocessor Management (Order Control)

Where subprocessors are engaged, GOTPHOTO ensures that processing takes place only on documented instructions.

Measures include:

- Careful selection of subprocessors under data protection and security criteria
- Conclusion of data processing agreements pursuant to Art. 28 GDPR
- Use of EU Standard Contractual Clauses where required
- Review of subprocessor security measures
- Contractual confidentiality obligations for subprocessor personnel

- Ongoing monitoring of subprocessor compliance

8. Regular Review and Evaluation

GOTPHOTO regularly reviews and evaluates the effectiveness of its technical and organizational measures.

This includes:

- Periodic internal assessments
- Review of access rights
- Review of policies and procedures
- Updates of measures in response to technological developments
- Documentation of relevant security measures

9. Privacy by Design and by Default

GOTPHOTO implements the principles of privacy by design and privacy by default.

Measures include:

- Collection of personal data limited to what is necessary for the defined purpose
- Configuration of systems to ensure data minimization
- Technical support for the exercise of data subject rights
- Consideration of data protection requirements during system design and development

Version: March 2026