STILL

Technical and Organizational Measures according to GDPR

I. Confidentiality (Art. 32 para. 1 lit. a + b GDPR)

1. Access Control of Processing Areas *(Physical Access)*

- Maintaining a physical security concept for the locations in scope incl. physical security zones
- Ensuring adequate access control measures to buildings and areas located in different physical security zones
- Restricting physical access to the required minimum (least privilege principle)
- Ensuring physical protection of perimeter, buildings, and rooms using fencing, secured doors, and secured windows
- Managing keys and access cards
- Limiting access to server rooms to a highly restricted group of authorized persons, including intrusion detection measures
- Managing visitors at the locations

2. Access Control to Data Processing Systems *(Authentication)*

- Ensuring strong user authentication (MFA) for the operational personnel working on the application
- Authenticating technical users by means of secure authentication protocols
- Ensuring network authentication between systems or system components by means of a machine certificate (interfaces)
- Enabling other applications to authenticate using technical users by means of secure authentication protocols
- Ensuring that clear-screen, clean-desk, and clean-wall principles are ensured at locations and by persons in scope of the data processing services
- Ensuring a DMZ and application gateway for access from external networks (e.g., the Internet)
- Implementing malware protection (incl. EDR on clients and servers)

3. Access Control to Use Specific Areas of Data Processing Systems *(Authorization)*

- Documenting the roles and permissions concept
- Restricting access to the required minimum (least privilege principle)
- Using personalized user accounts for the operational personnel working on the application
- Preventing access to the application through default or test accounts
- Using a process for regularly checking and withdrawing authorizations
- Creating separate administrator accounts for managing systems

- Ensuring that information (both data and physical documents) is securely deleted or disposed of, when no longer needed
- Ensuring that applications provide multi-tenant capabilities or using dedicated systems to process data for different purposes

4. Separation of Processing for Different Purposes

- Using separate development, test/quality assurance and production environment

5. Pseudonymization

- Ensuring that personal data is removed (anonymized) from data sets, before these are used for another purpose than for which they were initially obtained

6. Encryption

- Using state-of-the-art encryption for securing data at rest

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

1. Input Control

- Recording when users log in and make a failed attempt at logging in
- Logging user management actions
- Defining deadlines for storing and deleting logging data
- Ensuring input validation

2. Transmission Control

- Coordinating interface agreements
- Using state-of-the-art transport layer security (authentication and encryption) for data transfer
- Decoupling direct external access to the application
- Logging inbound and outbound data communications
- Ensuring output encoding

III. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

1. Availability Control

- Implementing malware protection (incl. EDR on clients and servers)
- Obtaining/requesting information about software vulnerabilities regularly
- Correcting vulnerabilities according to defined remediation times, based on criticality
- Identifying and correcting weaknesses regularly
- Implementing backups according to a backup concept
- Ensuring that backup restore tests are performed regularly
- Performing regular security scanning for vulnerabilities and weaknesses during development (static and dynamic security analysis)

- Performing regular security analysis for vulnerabilities and weaknesses for major releases or major feature changes (penetration testing)
- Fixing identified vulnerabilities and weaknesses based on their criticality
- Establishing a cold stand-by system
- Ensuring adequate physical business continuity measures are established for data centers and other relevant IT infrastructure (incl. redundant power supply, network connections, water protection, fire suppressant)
- Operating a central vulnerability management organization for all systems in scope

IV. Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the data processing (Art. 32 para. 1 lit. d GDPR)

1. Data Protection Management

- Confirming the protection need (Information Security Classification for the involved Information Assets)
- Checking compliance with service requirements on a regular basis
- Taking security specifications into account in the development of the application (security by design)
- Taking data protection requirements into account in the development of the service or application (privacy by design)
- Ensuring compliance requirements and rules when using open- source software
- Planning and documenting the application’s software life cycle
- Raising awareness of application administrators to IT security
- Operating an information security management system (ISMS) with dedicated information security roles, who are responsible for ensuring that adequate information security measures are implemented and their effectiveness is regularly assessed and the measures are adapted, if needed
- Operating a data protection management system (DPMS) with dedicated data protection roles, who are responsible for ensuring that data processing activities are documented, adequate data protection measures are implemented, their effectiveness is regularly assessed, and the measures are adapted, if needed

2. Incident Response Management

- Defining information security events in relation to user activities
- Using synchronized time stamps when logging user activities

- Conducting regular analysis of logging data to check whether any Information Security Events or Incidents have occurred
- Operating a 24/7 incident response organization that ensures that information security events are analyzed and responded to in a timely manner
- Maintaining information security incident response plans for relevant information security incidents

3. Data Protection by Default (Art. 25 para. 2 GDPR)

- Ensuring that only the personal data that is required for a certain purpose is made mandatory, when collecting and using personal data

4. Job Control

- Ensuring that subcontractors are carefully chosen, data processing agreements are concluded with them, and the technical and organizational measures are also passed on to subprocessing
- Ensuring that all personal data used in the role as processor are deleted at the end of the service contract, unless there is a legal obligation to keep them longer
- Ensuring regular information security training, including acceptable use when handling information, for all employees that have access to application data
- Ensuring that all employees that have access to personal data have been committed to an obligation of confidentiality