

## Checklist: "Technical and organisational measures"

*This document provides additional information on how to answer the questions regarding the technical and organisational measures that are to be described as part of the "Data Processing Agreement". Please answer the questions and describe all measures that are in place to guarantee the security of data processing and how they are implemented. The following topics, subtopics and related questions are designed to help you in identifying all relevant measures. Please be as precise as possible.*

### I. Confidentiality [Article 32 (1) (b) EU-GDPR]

#### 1. Access control to premises and facilities

How are unauthorised persons prevented from gaining access to data processing facilities where personal data is processed or stored?

- **Building security:** What kind of entry control system is used; are buildings locked outside working hours; are processing zones and visitor's zones separated?
- **Admission to the buildings:** Are entries logged and checked; how is this done?
- **Setting up the computer centre as a security sector:** How are the servers secured (e.g. are they located in a specifically dedicated secured and locked server room with access control) ; what kind of locking system is being used; is backup media stored in a safe co-location?
- **Specifying persons with access authorisation:** Are admissions and uses of keys logged; are there special access regulations for other persons?
- **Securing the networks:** How are distribution boxes, router, switches and network components secured against unauthorised access?

#### 2. Access control to systems

How are unauthorised persons prevented from using data processing systems which contain personal data?

- **Internal authorisation procedure for users:** What is the process for user authentication with respect to files and systems (e.g. user accounts with individual access rights); who may access files and systems; is there a documented organisational procedure for issuing, securing, changing and deleting user accounts; what happens to user accounts of staff members who have left the company?
- **Logging of access to applications (e.g. Content Management Systems, CMS) and systems:** How long may the access be traced back?
- **Encryption routines for log-in and password:** What are the settings of the global password policy; what is the procedure if lost passwords need to be reset; how many generations may old passwords not be re-used for?
- **Standard set up for PC:** Is there an automatic keyboard and monitor lock if PCs are not used; after how many minutes will they be locked; how are the PCs reset?

- **Firewall installation and virus protection:** Which networks are protected by which firewall systems; are there several; are IDS/IPS (Intrusion Detection Systems/Intrusion Prevention Systems) being used; which antivirus software is being used; is the virus protection automatically updated constantly; are e-mails automatically checked for malicious software; are indexed websites blocked?
- **Data storage media:** Are data storage media examined for malicious software before being used?

### 3. Access control to data

How is ensured that persons authorised to use a data processing system have access only to those data they are authorised to access, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording?

- **Security policy, authorisation concept and usage rights:** Is a differentiated authorisation system for use of files, system and application programmes in place; how are accessions to security-relevant data documented?
- **Controlled destruction of data storage media:** Are data storage media which are no longer for use rendered unusable; are they physically destroyed; are secured document containers or document shredding bins used for confidential documents; are certified disposal companies used?
- **Special regulations for mobile terminals:** Is hard disk encryption used on mobile PCs; how are they secured outside working hours (e.g. locked away)?

### 4. Separation control

How is ensured that personal data collected for different purposes is processed and stored separately?

- **Separated processing/File management for each order:** Is separation by client and project ensured; is ensured that the data may only be used for the purpose agreed?
- **Function separation:** Are test data and programs saved in different directories (e.g., are data stored on different network drives); are test data pseudonymised (key-coded)?

## II. Integrity [Article 32 (1) (b) EU-GDPR]

### 5. Disclosure/transmission control

How is ensured that personal data cannot be read, copied, altered or removed without authorisation during electronic transfer or physical transport or while storage on data storage media? And how is ensured that it is possible to check and determine the destination to which personal data are sent via data transfer systems?

- **Data transmission:** How are the data transmitted; are transmissions logged; are all addresses along the transmission chain documented; is there a documentation of PCs, software and files with personal data in the network; are transmitted data checked for correctness and completeness?

- **Transmission security:** Is data being transmitted encrypted with password protection only; what encryption algorithm is being used; how is data transmitted internally and externally (e.g. internal network/secure exchange portal/VPN)?

## 6. Input control

How is ensured that it is possible to retroactively check and ascertain whether and by whom personal data has been entered, changed or removed in/from data processing systems?

- **Systems for logging and logging evaluation:** Is there an automatic logging of file use/file changes/file erasure; how long are logs for security-relevant data stored for evaluation; who may access/change/evaluate this data?

## III. Availability and resilience [Article 32 (1) (b) EU-GDPR]

### 7. Availability control

How is ensured that personal data is protected against accidental destruction or loss?

- **Data security concept:** What backup system is being used; who is authorised to access the system; how often are changed databases saved; how often are they fully backed up; where are backup-copies stored; what emergency plans exist; are IT continuity tests performed on a regular basis?
- **Fire protection systems:** Are there fire protection zones and doors; are the server rooms air-conditioned; are smoke and fire alarms installed; is fire extinguisher equipment available; do plans for escape, rescue and fire protection exist?
- **Power supply:** Are an emergency power generator and UPS systems installed?

## IV. Job Control [Articles 28 (3) (a) (b) and 32 (4) EU-GDPR]

### 8. Job control

How is ensured that personal data that is processed on behalf of others is processed strictly in accordance with the instructions of the controller?

- **Conformity with instructions of client and data protection requirements:** Is there a clear regulation of the competences and responsibilities; is there a documentation of the different process stages and a work step control; how is ensured that all employees are aware of all the data protection requirements relevant to them before starting their work (in particular, this includes client's instructions for performing the agreed services)?

## V. Procedures for regular reviews, assessment and evaluation [Articles 32 (1) (d) and 25 (1) EU-GDPR]

How are the regular procedures for reviews/assessment/evaluation of the effectiveness of the technical and organisational measures for ensuring the security of the processing defined?