**Technical and Organisational Measures**
Status: 10/13/2021

## 1. Confidentiality

Storage and processing is carried out by selected providers in data processing centres that guarantee high standards of security and availability.

**Entry control:** The data processor uses the following measures to prevent the ingress of unauthorized persons to data processing facilities in which personal data is processed or used: keys, electric door openers.

In the APA–IT data processing centres:

- Installation of server rooms in a separate area
- Ingress is regulated by an entry control
- Video surveillance equipment
- Entry is possible for authorised persons only

**Admission control:** The data processor uses the following measures to prevent use of data processing systems by unauthorised persons: secure passwords; automatic locking mechanisms, two-factor authentication, encryption of data carriers, remote access via a virtual private network (VPN), SSH keys.

In the APA–IT data processing centres:

- Server passwords and access codes are given to the Client when the processing systems are first started up.
- Once responsibility for the systems has passed to the Client, the Client resets the passwords at its discretion and chooses a strong password that meets universal standards.

**Access control:** The data processor uses the following measures to guarantee that persons authorised to use a data processing system have access to no other data than that for which they have authorisation and that personal data cannot be read, copied, altered or deleted without the relevant authorisation either during processing or following its storage: authorisation profiles,

standard process of authorisation allocation, access logging insofar as this is possible and permitted, periodical verification of allocated authorisations, especially of administrative user accounts.

In the APA–IT data processing centres:

- Authorisation system: only named users are used.
- An annual check of access rights is carried out to determine their continued appropriateness.
- The access rights are derived from the third-party processor agreements or contracts.

- Pseudonymisation: Insofar as it is possible and advisable for each data processing case, the primary identifying attributes of the personal data in each data application are removed and kept separately.
- Classification scheme for data: this has as its basis legal obligations or own assessment (secret/confidential/public).
- Separation according to purpose: The data processor uses the following measures to guarantee that data collected for different purposes, and especially for different clients, can be processed separately: separate storage and processing of data from different clients/jobs; authorisation concepts; principle of minimum authorisation allocation.

**2. Integrity**

- Transmission control: The data processor uses the following measures to guarantee that personal data cannot be read, copied, altered or deleted without authorisation during electronic data transmission or storage and that it is possible to check and ascertain the locations to which personal data is to be transmitted by means of data transmission systems: connection encryption; VPN; electronic signature.

- Data entry control: The data processor uses the following measures to guarantee that it is possible to retrospectively check and ascertain whether and by whom personal data has been entered into a data processing system, altered or deleted: logging; document management.

In the APA–IT data processing centres: by maintaining a secure log or by entries in the event log. These log files serve to detect unlawful use of data and to repel attacks. The protocols are examined by the Chief Information Security Officer (CISO) in accordance with the audit plan.

**3. Availability and Resilience**

- Availability control: Prevention of accidental or wilful destruction or loss: backup; uninterruptible power supply (UPS); virus protection; firewall; reporting procedures and contingency planning; security checks at infrastructure and application levels; standard processes in the event of transfers/departure of personnel.
- Rapid recovery
- Erasure periods: for both data and backups as well as for metadata such as log files, etc.
  In the APA–IT data processing centres: redundant running of data processing centre operations

**4. Procedures for regular testing, assessment and evaluation**

- Data protection management, including regular staff training
- Incident response management
- Data protection-friendly default settings
- Data protection-friendly software development (privacy by design)
- Order or contract control: No processing as defined by Art. 28 GDPR without corresponding instructions from the Client, e.g. clear and unambiguous contractual arrangements, formalised order management, strict controls on the selection of the data processor, duty of pre-evaluation, supervisory follow-up checks.

**5. Supplementary Measures by Postmark**

Apart from the Standard Contractual Clauses there are additional measures by the US sub-contractor to account for the shortcomings of data transfer to the US as stated by the ECJ.

- Obligation to check whether government measures are necessary
- Obligation to defend against state access to data of EU citizens until the legal process is exhausted
- Obligation to pay a contractual penalty in case of culpable breach of obligations under the standard contractual clauses