Technical - organizational measures
Status: 10/10/2022

1. Confidentiality

Storage & processing takes place at selected providers in data centers that guarantee high security and availability standards.

Access control: The processor shall prevent unauthorized persons from accessing data processing facilities with which personal data are processed or used by taking the following measures: Keys, electric door openers

In the data centers:

- placement of the server premises in a separate zone
- access is secured by an access control system
- video surveillance system
- only authorized persons are granted access (access protocols)

Entry control: The processor prevents the use of data processing systems by unauthorized persons by the following measures: secure passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers, remote access via Virtual Private Network (VPN), SSH keys.

Admission control: The processor shall ensure that persons authorized to use a data processing system have access only to the data to which they are authorized and that neither during processing nor after storage can personal data be read, copied, modified or removed without appropriate authorization, by the following measures: Authorization profiles, standard process for authorization assignment, logging of accesses as far as possible & permissible, periodic review of assigned authorizations, especially of administrative user accounts.

In the data centers:

- authorization system - only "named users" are used.
- the access authorizations are checked annually for their appropriateness.
- the access authorizations result from the order processing contracts.
- multi-factor authentication (MFA).

- Pseudonymization: If possible and reasonable for the respective data processing, the primary identifiers of the personal data in the respective data application are removed, and kept separately.
- Classification scheme for data: Due to legal obligations or self-assessment (secret/confidential/internal/public).
- Separation of purposes: The processor ensures that data collected for different purposes, in particular from different mandates, can be processed separately by the following measures: separate storage and processing of data according to mandate, authorization concept, minimum principle for the allocation of authorizations.

2. Integrity

- Transfer control: the processor shall ensure that personal data cannot be read, copied, altered or removed without authorization during electronic data transfer or storage and that it is possible to verify and determine to which entities personal data is intended to be transferred by means of data transfer equipment through the following measures: Encryption of the connection, VPN, electronic signature.
- Input control: The processor shall ensure that it is possible to subsequently verify and establish whether and by whom personal data have been entered into, modified or removed from data processing systems through the following measures: Logging, document management
- In the data centers: by keeping a "secure log" or by logging in the event log. These log files are used to detect unlawful data use and to defend against attacks. The logs are reviewed by the Chief Information Security Officer (CISO) in accordance with the audit plan.

3. Availability and resilience

- Availability control: protection against accidental or deliberate destruction or loss: backup, uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans, security checks at infrastructure and application level, standard processes in the event of employee changes/leavings
- Rapid recoverability
- Deletion periods: Both for data and backups themselves as well as metadata such as log files, etc.

In the data centers:

- redundant management of data center operations

4. Procedures for regular audit, assessment and evaluation

- data protection management, including regular employee training sessions
- incident response management
- privacy-friendly default settings
- privacy-friendly software development (privacy by design)
- implementation of penetration testing at regular intervals
- contract control: no commissioned data processing within the meaning of Art 28 DSGVO without corresponding instructions from the client, e.g.: clear contract design, formalized contract management, strict selection of the processor, prior conviction obligation, follow-up checks.

5. Supplementary Measures on behalf of Active Campaign / Postmark

In addition, the standard contractual clauses were supplemented by further (accompanying) assurances and clarification options on the part of the U.S. sub service provider to compensate for the disadvantages for the level of data protection identified by the ECJ.

- obligation to examine whether state measures are necessary.
- obligation to defend against government access to data of EU citizens until legal recourse is exhausted.
- obligation to pay a contractual penalty in the event of culpable breach of obligations under the standard contractual clauses.