Appendix 3: Technical and organisational measures pursuant to Art. 32 DSGVO

In the course of obtaining this information, the Contractor shall provide the Customer with the following information on the technical and organisational measures set up:

Confidentiality [Art. 32 para. 1 lit. b DSGVO]

a) Entry Control

Measures to deny unauthorized persons access to the server systems used to process or use personal data:

The data centers are staffed 24/7. Access to the security areas is protected by an electronic access control system with logging.
The output of keys for the office locking system for the employees is centrally managed, monitored and documented. The access areas are secured by video surveillance. Visitors must identify themselves at the reception and will only be guided to their contact persons in the respective areas if accompanied.

b) Access Control

Measures to prevent the use of data processing systems by unauthorized persons:

The data processing systems are protected in particular by anti-virus software, firewall systems (software) and proxy servers. The administration of the security software is regularly ensured and is carried out only by authorized personnel. The authorization of the personnel is ensured by assigned user rights or user profiles. These profiles can be used to log on to the respective IT systems using two-factor authentication. This is done using a username and password (at least 8 digits, 1 lowercase letter, 1 uppercase letter, 1 number) and a 6-digit one-time code, which is sent to the user's smartphone via an app or via SMS.
Access to data processing systems is via secure connections (e.g. SSL certificates). The electronic data traffic between client and contractor is secured by encryption technology.

c) Access Control

Measures which guarantee that those authorized to use a data processing system only access data subject to their access authorization and that personal data cannot be processed, used and stored without authorization, read, copied, changed or removed:

The assignment of rights is implemented according to the authorization concept and administration is the responsibility of the system administrators. The concept and the rights granted are subjected to an annual self-assessment and the procedure is monitored.

In principle, the number of administrators is limited to the "most necessary". To ensure that only authorized persons have access to data, data carriers and data are encrypted and access is regulated via user rights. Access to systems and applications is password-protected by two-factor authentication and depends on user rights - each employee can only access the functions necessary to perform his or her tasks within the scope of his or her area of responsibility. Illegal access to systems or data integrity via vulnerabilities in programs is prevented by regular monitoring of the infrastructure and immediate resolution of problems found. Both external and internal accesses are recognized and their effects minimized.
Customer data on the servers of the hosting service provider are stored AES256-encrypted and are therefore not readable by the hosting service itself.

d) Pseudonymization

Pseudonymization (Art. 32 para. 1 lit. a, Art. 25 para. 1 DSGVO) guarantees that identification features of personal data, insofar as this is necessary to protect the data subjects or is required from the point of view of data protection law, are replaced by identifiers for certain or identifiable persons and can therefore not be assigned to the data subject without additional information.

Consequently, data can no longer be attributed to a specific data subject without additional information. This additional information must be kept separately and be subject to appropriate technical and organizational measures.

Customer data on the servers of the hosting service provider are stored AES256-encrypted and are therefore not readable by the hosting service itself.

Integrity [Art. 32 para. 1 lit. b DSGVO]

e) Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data carriers and that it is possible to check and establish to which points personal data is to be transmitted by data transmission devices:

The electronic data exchange is monitored by security systems, where all data is transmitted SSL-encrypted (TLS 1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES_128_GCM (cipher)). Unauthorized removal of data carriers in the data center is restricted by security areas and access control. Guidelines have been issued for the respective areas to prevent unauthorized removal of data carriers. Discarded data carriers will be destroyed according to specifications.
In addition, an authorization concept is used to assign rights to enter, change and delete data on the servers. All employees are contractually bound to data secrecy.

f) Input Control

Measures to ensure that it can be subsequently verified whether and by whom personal data have been entered, modified or removed in data processing systems:

The restrictive assignment of rights by individual users restricts the entry, modification or removal of personal data in data processing systems. Every entry, modification and removal of data is recorded.

Availability [Art. 32 Par. 1 lit. b DSGVO]

g) Availability Control

Measures to ensure that personal data is protected against accidental destruction or loss:

To limit accidental destruction or loss during job-related data processing, a backup & recovery concept was created, implemented and the recovery was regularly tested. The data backups are stored in a secure, outsourced location. An uninterruptible power supply (UPS) is used to ensure regular and safe operation of the systems even in the event of faults in the power grid. The server room is secured by various monitoring and alarm systems, in particular devices for monitoring temperature and humidity as well as fire and smoke detection systems.

Control measures [Art. 32 para. 1 lit. d, Art. 25 para. 1 DSGVO]

h) Order Control

Measures to ensure that personal data processed on behalf of the contracting authority can only be processed in accordance with the contracting authority's instructions:

The Processor shall process the data submitted in accordance with the contract concluded and shall comply with the statutory provisions and requirements defined by contract within the framework of the instructions of the Controller. This contractually excludes the disclosure of data to unauthorized third parties and defines the framework of instructions. The mandatory contents of § 28 DSGVO are also taken into account in the determination. The Processor shall allow the client to inspect the documentation of the "technical/organizational measures" in advance or, if necessary, to inspect the data processing equipment on site. A possible examination of the Processor as well as his activities

carried out in the context of data processing is thereby made possible and supported by the Processor.

i) Separation requirement

Measures to ensure that data collected for different purposes can be processed separately:

The separation requirement is ensured by logical client separation on the software side. Test environments are managed independently of the production system - customer data is not transferred to these test systems.

j) Data security management

Procedures to ensure regular review, analysis and evaluation of the effectiveness of technical and organizational measures:

The security measures described are regularly reviewed, analyzed and evaluated and adapted to the technical standard in order to ensure the effectiveness of the technical and organizational measures.

k) Privacy-friendly presetting

Measures to prevent unauthorized or unlawful data processing by presetting data processing for a specific purpose. The amount of data collected, the scope of processing, the storage period and accessibility must be taken into account. In particular, measures must be taken to prevent personal data from being made available automatically (without human intervention) to an indefinite number of natural persons:

By default settings and warnings within the products, the user is instructed on how to use them in compliance with data protection regulations. In addition, the access possibilities are personalized and password-protected.

l) Risk management

Procedures for determining the risk to the rights and freedoms of natural persons and needs-based analysis of the appropriate level of protection, taking into account the state of the art, implementation costs, the nature, scope, circumstances and purposes of processing and the different likelihoods and severity of the risk.

The risks to the rights and freedoms of natural persons are continuously examined and evaluated and the level of protection is adjusted accordingly if necessary.

Status: January 2024