

Security Policy

The Processor utilises third party data centres that maintain current ISO 27001 certifications and/or SSAE 16 SOC I Type II or SOC 2 Attestation Reports. The Processor will not utilise third party data centres that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations.

Upon the Controller's written request (no more than once in any 12 month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Solutions or Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the MSA between the parties.

The following descriptions provide an overview of the technical and organisational security measures implemented. It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available, however additional information regarding technical and organisational measures may be requested. It is acknowledged and agreed that the technical and organisational measures described herein will be updated and amended from time to time, at the sole discretion of the Processor, however the updated technical and organisational measures will not fall short of those measures herein in any material, detrimental way.

1. Entrance Control

Technical or organisational measures regarding access control, especially regarding legitimisation of authorised persons:

The aim of the entrance control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Personal Data.

Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorisations. They are monitored by security personnel. Access for employees is only possible with an encoded ID with a photo on it. All other persons have access only after having registered before (e.g. at the main entrance).

Access to special security areas for remote maintenance is additionally protected by a separate access area. The constructional and substantive security standards comply with the security requirements for data centres.

2. System Access Control

Technical and organisational measures regarding the user ID and authentication:

The aim of the system access control is to prevent unauthorised use of data processing systems being used for the processing of Customer Data.

Remote access to the data processing systems is only possible through the Processor's secure VPN tunnel. If the users first authenticate to the secure VPN tunnel, after successful authentication authorisation is executed by providing a unique user name and password to a centralised directory service. All access attempts, successful and unsuccessful are logged and monitored.

Additional technical protections are in place using firewalls and proxy servers and state of the art encryption technology that is applied where appropriate to meet the protective purpose based on risk.

3. Data Access Control

Technical and organisational measures regarding the on-demand structure of the authorisation concept, data access rights and monitoring and recording of the same:

Measures regarding data access control are targeted on the basis that only such data can be accessed for which an access authorisation exists and that data cannot be read, copied, changed or deleted in an unauthorised manner during the processing and after the saving of such data.

Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.

To maintain data access control, state of the art encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.

4. Transmission Control

Technical and organisational measures regarding the transport, transfer, transmission, storage and subsequent review of Personal Data on data media (manually or electronically).

Transmission control is implemented so that Personal Data cannot be read, copied, changed or deleted without authorisation, during transfer or while stored on data media, and so that it can be monitored and determined as to which recipients a transfer of Personal Data is intended.

The measures necessary to ensure data security during transport, transfer and transmission of Personal Data as well as any other company or Customer Data are detailed in the Security Policy. This standard includes a description of the protection required during the processing of data, from the creation of such data to deletion, including the protection of such data in accordance with the data classification level.

For the purpose of transfer control, an encryption technology is used (e.g. remote access to the company network via two factor VPN tunnel and full disk encryption). The suitability of an encryption technology is measured against the protective purpose.

The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred to companies located outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the Standard Contractual Clauses.

5. Data Entry Control

Technical and organisational measures regarding recording and monitoring of the circumstances of data entry to enable retroactive review.

System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.

6. Data Processing Control

Technical and organisational measures to differentiate between the competences of principal and contractor:

The aim of the data processing control is to provide that Personal Data is processed by a commissioned data processor in accordance with the Instructions of the principal.

Details regarding data processing control are set forth in the MSA and DPA.

7. Availability Control

Technical and organisational measures regarding data backup (physical/logical):

Data is stored in triplicate across 2 data centres, with 2 separate cross connections. The data centres can be switched in the event of flooding, earthquake, fire or other physical destruction or power outage protect Personal Data against accidental destruction and loss.

If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.

8. Separation Control

Technical and organisational measures regarding purposes of collection and separated processing:

Personal Data used for internal purposes only e.g. as part of the respective customer relationship, may be transferred to a third party such as a subcontractor, solely under consideration of contractual arrangements and appropriate data protection regulatory requirements.

Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.

Customer Data is stored in a way that logically separates it from other customer data.

The Controller is assigned a unique encryption key, generated using a FIPS 140-2 compliant crypto library, which is used to encrypt and decrypt all of the Controller's archived data. In addition to the unique encryption keys, all data being written to the storage grid includes the Controller's unique account code. The Processor's systems that write data to the storage grid retrieve the encryption key from one system and the customer code from another, which serves as a cross check against two independent systems. The Controller's encryption key is further encrypted with a Processor key stored within a centralised and restricted key management system. In order for the Processor to access Customer Data via the master key, the key management system provisions individual keys following a strict process of approval that includes multiple levels of executive authorisation. Use of these master encryption keys is limited to senior production engineers and all access is logged, monitored, and configured for alerting by security via a centralised Security Incident and Event Management ("SIEM") system. The Controller's archived data is encrypted at rest using AES256 bit encryption and data in transit is protected by Transport Layer Security ("TLS").