Technical and organizational measures (Security Policy)

Preamble

Axess guarantees the following IT security measures within the framework of the Customer relationship.

1. General technical and organizational measures

Axess undertakes to take all necessary measures for processing the transmitted data in its data processing systems in accordance with the GDPR and ensures that its internal organization is designed to meet data protection requirements. The following provisions apply regardless of where the server is hosted.

1.1. Control of purpose of use

The following measures ensure that data collected for different purposes is processed separately:

- Software-based (e.g. customer segmentation)
- Separation through access control (database principle)
- Separation of test and current data
- Separation of test and running systems (technology, programs)

1.2. Pseudonymization

To the extent possible for the respective data processing, the primary identifying characteristics of the personal data will be removed from the respective data application and stored separately.

1.3. Input control

It is ensured that it can be subsequently verified and determined whether and by whom personal data is entered into, modified, or removed from data processing systems. Axess will document and record entries/log files for this purpose.

1.4. Privacy by Design & Privacy by Default

Through appropriate default settings within the framework of technical and organizational measures, it is ensured that, in principle, only personal data whose processing is necessary for the respective processing purpose is processed.

- Personal data is only collected if it is necessary for the processing of the purchase agreement (e.g. season tickets).
- The setting of cookies in Axess webshops is only possible with the user's consent.
- The use of personal data for marketing purposes is only permitted with the user's active consent.

2. Technical and organizational measures for Server-Hosting by Axess

If the Data Center Service is used as part of the purchase agreement, it is ensured that security zones and the circle of authorized persons and access rights are defined, access routes are secured accordingly, and data carriers are controlled and stored securely. The following measures apply only if the server is hosted by Axess.

2.1. Admission control

Unauthorized persons are prohibited from accessing data processing facilities where data is processed. The server rooms are located in an office building classified as earthquake-resistant. Only IT, facility management, and management staff have access to the premises. Access control is ensured by the following measures:

- Authorization/Chip Card

Presence in the security zone is registered. Unauthorized personnel and external individuals (service technicians, consultants, cleaning staff, etc.) may only enter the premises when accompanied by authorized personnel. Access control is supported by the following additional organizational/technical measures:

- Alarm system
- Building surveillance
- Video technology

2.2. Entry control

Unauthorized use of the data processing systems is prevented by the following measures:

- Password
  Each authorized person has their own password, known only to them, which must be changed at regular intervals. Automatic log files are created for all activities on the data processing and telecommunications system.

The unauthorized use of data processing systems via data transmission devices is prevented by the following measures:

- VPN (Virtual Private Network)

2.3. Access control

It is ensured that persons authorized to use a data processing system can only access their authorized data and that data cannot be read, copied, modified, or deleted without authorization during processing, use, and storage. The restriction of authorized access to data subject exclusively to their access authorization is guaranteed by the following measures:

- Automatic verification of access authorization (within the system)

2.4. Transfer control

It is ensured that personal data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage on data carriers, and that it can be verified and determined at what time the transmission of personal data by data transmission devices is intended. The shipment of data carriers is documented and monitored by registration and accompanying documents. It is not permitted to bring private data carriers into the premises and use them. Data carriers are destroyed in the following way:

- Magnetic data carriers by overwriting and physical destruction (external service provider)

To the extent that the internet is used for the transmission of personal data, the following security measures are employed:

- Firewall
- VPN (Virtual Private Network)

2.5. Availability control

The following measures ensure that personal data is protected against accidental destruction or loss:

- Daily/weekly/monthly/annual data backups
- SAN (Storage Area Network)
- Disk mirroring (RAID etc.)
- UPS (Uninterruptible Power Supply)
- Surge protection
- Emergency power generator
- Data off-site storage
- Fire protection equipment

2.6. Data protection management

It is ensured that a data protection management system is established and implemented. This system comprises the following points:

- Record of processing activities
- Data processing on behalf of a controller
- Data protection impact assessment

- Incident response management
- Data breach notification
- Training
- PDCA (Plan, Do, Check, Act): regular checks

2.7. Incident management

Measures have been put in place to determine how those responsible should respond to potential scenarios. These include data breaches, DoS (Denial of Service), DDoS (Distributed Denial of Service), firewall vulnerabilities, virus or malware outbreaks, and insider threats. Incident response management is divided into six key phases:

- Preparation: Both users and IT staff are trained or informed about potential incidents and the necessary steps to take.
- Identification: Determining whether an event constitutes a data breach.
- Containment: Limiting the damage caused by the incident and isolating the affected systems to prevent further damage.
- Eradication: Identifying the cause or trigger of the incident and removing the affected systems from the production environment.
- Recovery: Reintegrating affected systems into the production environment after ensuring that no further threats exist.
- Gained knowledge: Completing the incident documentation and analyzing what the team or organization can learn from the incident. This can help improve future responses.

3. Access to Customer data

In order to provide appropriate support in case of problems, Axess, as the data processor, reserves the right to access the Customer's system or data, provided that such access is covered by the purchase agreement between Axess and the Customer, or the Customer has consented to such access, or the reseller has forwarded the requested service request to Axess on behalf of the Customer. Axess guarantees that:

- physical access to the data center hardware will only occur if the Customer purchases the Data Center Service from Axess;
- access to the Customer's data via the remote maintenance tool will only occur in the case described above and with the consent or at the request of the reseller and/or the Customer;
- access to local devices will only be granted in support cases at the request of the Customer or the reseller.

4. Data processing control

Axess maintains contracts with external parties for the following types of data processing:

- Data processing by external parties
- Data carrier destruction/disposal by external parties
- Maintenance and remote maintenance by external parties
- Administration/remote administration by external parties

The processing of personal data is ensured by the following measures:

- Written instructions
- Offer and order confirmation
- Pseudonymization

Axess engages sub-processors only after prior review and approval, taking into account their suitability with regard to data protection and information security. Engagement is based on appropriate contractual arrangements, in particular through the conclusion of data processing agreements or comparable agreements. Before engaging a sub-processor and at appropriate intervals during the term of the contract, Axess verifies whether suitable technical and organizational measures have been implemented and monitors compliance with the agreed data protection and security standards.