Security Policy

Technical and organizational security measures
Axess undertakes, respectively in its contract with the external computer center commissioned by Axess, to take the special requirements of data protection into account. Both the internal as well as the external computer centers are located in Austria. In this context Axess always makes an effort to take all measures, which are necessary for the execution of the order for the processing of the provided data on the data processing systems according to the GDPR as well as to design the inhouse organization so that the requirements of data protection are satisfied.

It is ensured that security zones and the group of authorized persons or persons with access authorization are stipulated, access routes are protected accordingly as well as that data carriers are controlled and stored in a secured manner.

It currently particularly concerns the following necessary measures:

1. Admission control:
Unauthorized persons are prohibited from gaining admission to data processing systems, with which data are processed or used. The computer rooms are located in an office building of a mixed region that is classified as earthquake-proof. The admission control – only employees of the IT, Facility and the management – is guaranteed by one of the following measures:
> Authorization /chip card

The presence in the security zone is recorded. Non-authorized personnel and persons who do not belong to the company (service technicians, consultants, cleaning staff, etc.) may only enter the rooms when accompanied by authorized persons. The admission control is supported by the following further organizational/technical measures:
> Alarm system
> Building surveillance
> Video technology

2. Entry control
A use of the data processing systems by unauthorized persons is prevented by the following measures:
> Password

Each authorized person has an own password that is only known to him/her, which must be changed at regular intervals. Automatic protocols (log files) are created with regard to all activities on the data processing and telecommunication system. The use of data processing systems with the help of equipment for data transmission by unauthorized persons is prevented by the following measures:
> VPN (Virtual Private Network)

3. Access control
It is guaranteed that the persons authorized to use a data processing system can exclusively access their data that are subject to access authorization and that data cannot be read, copied, changed or removed without authorization during the processing, use as well as storage. The restriction to the access possibility of the authorized person exclusively to the data subject to his access authorization is guaranteed by the following measures:
> Automatic examination of the access authorization (in the system)

4. Intended use control
It is guaranteed by the following measures that data collected for different purposes are processed separately:
> Software- based (e.g. client segregation)
> Segregation through access regulation (database principle)
> Segregation of test and current data
> Segregation of test and current systems (technology, programs)

5. Pseudonymization
Insofar as possible for the respective data processing the primary identification features of the personal data will be removed in the respective data application and stored separately.

6. Transfer control:
It is guaranteed that personal data with the electronic transmission or during their transport or their storage on data carriers cannot be read, copied, changed or removed without authorization and that it can be checked and determined, at which point a transmission of personal data by equipment for the data transmission is envisaged. The shipment of data carriers is documented and controlled by registration and accompanying documents. It is not permitted to bring and use private data carriers into the rooms. Data carriers are destroyed in the following manner:
> Magnetic data carriers by write-over and physical destruction (external service provider)

Insofar as the internet is used to forward personal data the following security measures will be used:
> Firewall
> Virtual Private Network (VPN)

7. Input control
It is guaranteed that it can be subsequently checked and determined whether and by whom personal data are entered in, changed or removed from data processing systems. The contractor will document or record inputs for this purpose.

8. Availability control
It is guaranteed by the following measures that personal data are protected against accidental destruction or loss:
> Daily/weekly/monthly/annual data backup
> Storage Area Network (SAN)
> Disk mirroring (RAID among others)
> Uninterruptible power supply (UPS)
> Overvoltage filter
> Emergency generator
> Outsourcing of data
> Fire prevention devices

9. Data protection management
It is ensured that a data protection management is set up and implemented. The data protection management is broken down into the following points:
> List of processing activities
> Contract data processing
> Data protection impact assessment
> Incident response management
> Report of breaches of data protection
> Training
> PDCA (Plan, Do, Check, Act): regular checks

10. Incident response management
Measures were taken concerning how the responsible persons should react to potential scenarios. These include data security breaches, DoS (Denial of Service), DDoS (Distributed Denial of Service), gaps in the firewall, outbreaks of viruses or malware and also threats by insiders.
The incident response management is divided into six important phases:
> Preparation: Both the users as well as the IT employees are trained or informed that potential incidents happen and which steps have to be initiated.
> Identification: Determination whether an event actually concerns a data protection incident.
> Containment: To limit the damages caused by the incident and isolate the affected systems in order to avoid further damages.
> Eradication: To find the cause or what triggered the incident off and to remove the affected systems from the productive environment.
> Recovery: To integrate affected systems into the productive environment again, after it has been ensured that no further threats exist.
> Gained knowledge: Completion of the incident documentation and analysis what the team or the company can learn from the incident. This way future responses can be improved under certain circumstances.

11. Privacy by Design & Privacy by Default
It is guaranteed that suitable technical and organizational measures were taken, which ensure that by corresponding pre-settings principally only personal data are processed of which the processing is necessary for the respective determined processing purpose:
> Personal data will only be collected if they are necessary for the processing of the contract (season tickets, etc.).
> The setting of cookies in web-shops is only possible with the consent of the user.
> The use of the personal data for marketing purposes is only permitted by the active consent of the user.

12. Order control
It is guaranteed that personal data, which are processed by order, are only processed in line with the instructions of the client. Contracts exist for the following types of contract 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 by order – only in line with the instructions of the client – is guaranteed by the following measures:
> Written instructions
> Offer and confirmation of order
> Pseudonymization

13. Sub-contract data processor
> CN Group CZ s.r.o.
> Agentur LOOP New Media GmbH
> conova communications GmbH