SECONOS
IT & Data Services GmbH

Anlage zum Auftrag gemäß Art. 28 DS-GVO
Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

1. Zutrittskontrolle
Der Zutritt zu den Räumen ist nur per Schlüssel möglich und ist entsprechend dokumentiert. Des Weiteren werden die Zu- und Abgänge durch entsprechende technische Vorkehrungen überwacht, sodass der Zugang von Unbefugten Alarm auslöst.

Die Daten auf den stationären Computern sind durch Verschlüsselung geschützt.
Die Computer sind auch durch entsprechende Hardening Maßnahmen abgesichert.

Im Rechenzentrum gelten die technisch organisatorischen Maßnahmen des Subunternehmens Hetzer Online GmbH.

2. Zugangskontrolle
Der Zugang zu den Systemen ist durch starke Passwörter und Zweifaktor-Authentifizierung geschützt. Die Wahl einfacher Passwörter wird durch den Einsatz von Passwortfiltern unterbunden.
Datenträger werden durch sichere Löschvorgänge bereinigt und werden anschließend grundsätzlich mechanisch zerstört.

Die Schlüssel-und Passwortverwaltung erfolgt an zentraler Stelle und untersteht ausschließlich der Geschäftsleitung und dem Verantwortlichen der IT-Technik.

3. Zugriffskontrolle

- Durch Begrenzung, Dokumentation und regelmäßige Prüfung Zugangsberechtigter und Protokollierung der Zugriffe
- Regelmäßige Sichtung der Protokolle zum Dateizugriff
- Regelmäßige Sichtung der Protokolle zum Datenbankzugriff
- Umsetzung Need-to-know Prinzip
- Feingranulare Zugriffsrechte begrenzen den Zugang auf die notwendigsten Daten
- Geschäftsleitung ist verantwortlich für die Ausgabe und Verwaltung von Zugriffssicherungscodes

4. Weitergabekontrolle
Weitergabe von Daten erfolgt durch Pseudonymisierung bzw. in verschlüsselter Form. Je nach Grad der Schutzwürdigkeit der Daten wird abgewogen wie zu Verfahren ist bspw. verschlüsselter Mailversand oder persönliche Übergabe eines verschlüsselten Datenträgers.
Durch die strenge Berechtigungsstruktur wird die Datensparsamkeit systemweit begrenzt.
Im Falle von ungewöhnlichen Aktivitäten bspw. zu hohes Datenaufkommen schlagen die internen Systeme Alarm und eskalieren den Vorgang an die Geschäftsleitung und die Leitung der IT-Technik.

5. Eingabekontrolle

Durch die umfangreiche Rechtestruktur und Protokollierung ist gewährleistet, dass es nachvollziehbar ist, wer, wann, wo, woran gearbeitet hat.
Automatische Eskalation von Sicherheitsmeldungen wenn gravierende Veränderungen am System vorgenommen wurden, bspw. die Erstellung von weiteren Adminaccounts bzw. Veränderung von Passwörtern von Adminaccounts oder dem Abfluss von größeren Datenmengen.
Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.

6. Verfügbarkeitskontrolle

- Einsatz von Firewallsystemen mit Filterung des ein-und ausgehenden Traffics
- Datensicherungskonzept und Anzahl von 14 Datensicherungsgenerationen
- Backup- und Restorekonzept welche wöchentlich vollautomatisch erstellt und getestet werden.
- Einsatz von USVs
- Sicherung der Daten an vier verschiedenen Standorten (Frankfurt, Nürnberg, Falkenstein und Helsinki).
- Notfallhandbuch mit entsprechenden Plänen und Dokumenten.

Die Systeme sind mehrfach redundant ausgelegt. Das Live-System I synchronisiert den Datenbestand in Echtzeit mit den Slave-Systemen II und III. Im Falle eines Ausfalls des Live-Systems, wird der Kunde nahtlos auf das Slave-System II geleitet. Das Slave-System III ist nicht für die Bereitstellung der Applikationen vorgesehen, sondern dient ausschließlich als Backupsystem. Zudem werden die Daten täglich in einem Rechenzentrum eines anderen Dienstleisters gespeichert. Die Backups werden somit bei zwei verschiedenen Dienstleistern gespeichert.

Die Backuphistorie beträgt 14 Tage. Längere Speicherpläne können gegen Aufpreis eingerichtet werden.

7. Trennungskontrolle

Jeder Kunde erhält sein eigens Server-System. Die Daten unterschiedlicher Auftraggeber sind je nach gebuchtem Paket entweder logisch oder physisch voneinander getrennt. Des Weiteren sind die Systeme durch verschiedene Netzsegmente getrennt.

Die Systeme sind aufgeteilt in Entwicklungs-, Test- und Produktivsystem.