Anlage: Technische und organisatorische Maßnahmen

Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz gemäß Art. 32 DSGVO der 4A-SIDE GmbH

1. **Vertraulichkeit:**

Zutrittskontrolle:

☒ Zutrittskontrolle durch Transponder-Schließsystem, Schlüsselregelung
☒ Aufenthalt von Besuchern nur in Anwesenheit von Mitarbeitern
☒ Videoüberwachung am Serverraum
☒ Fenster einbruchsicher (4. Stock)
☒ Serverraum verschlossen, Zutritt nur für EDV-Mitarbeiter, Geschäftsführung
☒ Sorgfältige Auswahl Reinigungspersonal

Zugangskontrolle:

☒ Identifizierung und Authentifizierung durch Benutzername/Passwort
☒ Passwortrichtlinie
- Minimale Kennwortlänge: 8 Zeichen
- Komplexität: „4 aus 4“ (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen)
- Keine Weitergabe von Passwörtern

☒ Begrenzung der Fehlversuche
☒ Systemverwalterbefugnisse/ -protokollierung
☒ Arbeitsanweisung Sperren des Bildschirms bzw. Abmelden vom System
☒ Protokollierung der Anmeldung
☒ Firewalls (2x) und Antivirensoftware

Zugriffskontrolle:

☒ Berechtigungskonzept mit Rollen und unterschiedlichen Berechtigungsstufen
☒ Definierte VPN-Benutzerprofile gem. Benutzertätigkeiten für den Zugriff von extern auf die IT-Systeme
☒ Administratoren-Rechte auf das „Notwendigste“ reduziert
☒ Datenträgervernichtung intern mit Protokollierung
☒ Vernichtung Papier intern mit Aktenvernichter, Sicherheitsstufe 4 (geheimzuhaltendes Schriftgut)
☒ Verschlüsselung von Datenbanken und Datenträgern

Trennungsgebot:

☒ Projektbezogen jeweils getrennte virtuelle Entwicklungs-, Demo- und Livesysteme zum Verarbeiten von Daten
☒ Logische Kundentrennung (softwareseitig)
☒ Unterschiedliche Datenbanken
☒ Festlegung von Datenbankrechten
☒ Physikalische Trennung Personaldaten (Papierakten), logische Trennung digitaler Personaldaten über Berechtigungskonzept

2. Integrität:

Weitergabekontrolle:

☒ Bestandsverzeichnis und Bestandskontrolle der Datenträger durch mit Leitung der Datenverarbeitung beauftragte Person und den Datenschutzbeauftragten
☒ Es erfolgt keine Weitergabe von Datenträgern an Dritte
☒ Einsatz VPN-Technologie
☒ Sichere Aufbewahrung von Datenträgern

Eingabekontrolle:

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten auf relevanten Datenbank-Feldern
☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
☒ Rechtevergabe Lesen, Eingeben, Änderung und Löschung im Rahmen des Berechtigungskonzeptes

3. Verfügbarkeit und Belastbarkeit:

Verfügbarkeitskontrolle:

☒ Serverraum nicht unter sanitärer Anlage
☒ Klimaanlage im Serverraum
☒ Schutzsteckdosenleisten im Serverraum
☒ Unterbrechungsfreie Stromversorgung (USV)
☒ Angriff von außen: Firewall (2x)
☒ Risiko- und Schwachstellenanalyse im Rahmen des jährlichen Audits durch den Datenschutzbeauftragten
☒ alle 24h ein Backup in einen sicheren, ausgelagerten Ort (Datentresor)
☒ Testen von Datenwiederherstellung
☒ Schulung der Mitarbeiter bezüglich Sicherheitsanforderungen durch den Datenschutzbeauftragten

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

Datenschutzmanagement:

☒ Dokumentation Verfahren / Verfahrensregister sind vorhanden, vollständig und aktuell
☒ Fachkundenachweise des Datenschutzbeauftragten liegen vor
☒ Einhaltung Datengeheimnis, sämtliche Mitarbeiter sind auf das Datengeheimnis verpflichtet
☒ Regelmäßige Datenschutzmerkblätter für die Mitarbeiter, Datenschutzschulung durch den Datenschutzbeauftragten
☒ Dienstanweisung über die Internet- und E-Mail-Nutzung
☒ jährliche Audits durch den Datenschutzbeauftragten

Incident-Response-Management:

☒ Etwaige Vorfälle werden unverzüglich dem Datenschutzbeauftragten gemeldet
☒ Bearbeitung etwaiger Fälle durch den Datenschutzbeauftragten

Auftragskontrolle:

☒ Schriftliche Verträge zur Auftragsverarbeitung liegen vor und werden jährlich auditiert durch den Datenschutzbeauftragten
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
☒ Kontrolle der Einhaltung beim Auftragnehmer und/oder Überprüfung Zertifikat(e) durch den Datenschutzbeauftragten, Protokollierung

Technische und organisatorische Maßnahmen in dem Rechenzentrum
(Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen)

Die Darstellung der technischen und organisatorischen Maßnahmen beschränkt sich für die Dienstleistungen in dem Rechenzentrum auf die Beschreibung der Zutrittskontrollen und der Verfügbarkeitskontrollen. Dies erfolgt im Einklang mit den Empfehlungen der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) gem. GDD-Ratgeber Datenschutz-Prüfung von Rechenzentren:

Zutrittskontrolle:

- Datacenterparks in Nürnberg und Falkenstein
  - elektronisches Zutrittskontrollsystem mit Protokollierung
  - Hochsicherheitszaun um den gesamten Datacenterpark
  - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
  - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
  - 24/7 personelle Besetzung der Rechenzentren
  - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
  - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
- Verwaltung
  - elektronisches Zutrittskontrollsystem mit Protokollierung
  - Videoüberwachung an den Ein- und Ausgängen

Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
- Einsatz von Festplattenspiegelung.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Einsatz von Softwarefirewall und Portreglementierungen.
- Dauerhaft aktiver DDoS-Schutz.

Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.