FLAVE TECHNISCH-ORGANISATORISCHE MASSNAHMEN

VERTRAULICHKEIT

- **Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen; Gesichertes Housing innerhalb der EU (Frankfurt); Rechenzentrumsbetreiber & -standort ISO27001:2013 und ISO9001 zertifiziert.**
- **Zugangskontrolle: Kennwörter (einschließlich entsprechender Policy); automatische Sperrmechanismen; kein physikalischer Zugriff auf die Hardware;**
- **Zugriffskontrolle: Standard-Berechtigungsprofile auf „need to know-Basis"; Standardprozess für Berechtigungsvergabe; Protokollierung von Zugriffen; periodische Überprüfung der vergebenen Berechtigungen;**
- **Trennungskontrolle: Dedizierter virtueller Server pro Kunde / Projekt; dedizierte Benutzerkonten & Passwörter, umfangreiches Berechtigungssystem; getrennte, Datenbanken;**
- **Pseudonymisierung: Gäste-/Kundendatensätze werden über UUIDs identifiziert; IP-Adressen werden temporär (bis Ende des Projekts) gesondert & verschlüsselt gespeichert um Sicherheitsvorfälle zu analysieren**

INTEGRITÄT

- **Weitergabekontrolle: sämtliche ein- und ausgehenden Verbindungen werden verschlüsselt; Protokollierung von Zugriffen; sensiblere Daten werden zusätzlich verschlüsselt gespeichert;**
- **Eingabekontrolle: Protokollierung; Versionierung; stündliche Backups;**

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle: Stündliche off-site Backups; unterbrechungsfreie Stromversorgung (USV); Rechenzentrumsbetreiber & -Standort ISO27001:2013 und ISO9001 zertifiziert; Hardware RAID; Intrusion Prevention System (IPS), Permission-System um die Ausführung nicht autorisierter Anwendungen zu unterbinden; Virenschutzprogramme auf Server & Clients (Mitarbeiter des AN)**
- **Rasche Wiederherstellbarkeit durch stündliche Backups & Versionierung**
- **Kurze Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl., spätestens mit Ende der Vereinbarung.**

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- **Grundsätze: Datenschutz ist Aufgabe des gesamten Unternehmens; es werden datenschutzfreundliche Technologien eingesetzt; IT-Sicherheit muss auf dem aktuellen Stand der Technik sein**
- **Datenschutz-Management: Durchgeführte Verarbeitungstätigkeiten werden einheitlich und nachweisbar dokumentiert; Weisungen von & ausgeführte Tätigkeiten für Kunden im Rahmen einer Auftragsverarbeitung werden kundenbezogen dokumentiert.**
- **Incident-Response-Management: Es bestehen interne Richtlinien und Prozesse zum Datenschutz, die bei Bedarf oder sich ändernden Voraussetzungen erweitert bzw. ergänzt werden.**
- **Datenschutzfreundliche Voreinstellungen: Es werden für den jeweiligen Verarbeitungszweck geeignete technische und organisatorische Maßnahmen getroffen, die jedem Auftraggeber im Rahmen der Vereinbarung einer Auftragsverarbeitung zugesichert werden. Beispiele: Neue Objekte in der Berechtigungs- und Zugriffsverwaltung haben keinerlei Rechte im System und dürfen zunächst keine Daten-Inhalte sehen. Auswertungsergebnisse und Listen können nur von berechtigten Personen eingesehen werden.**
- **Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers; Verpflichtung der Beschäftigten des Auftragnehmers auf das Datengeheimnis; Bestellung eines Datenschutzbeauftragten; Bestellung eines Datenschutzkoordinators;**
- **Gerade im Prozess der ISO/IEC 27001:2017 & ISO/IEC 27018:2014-Zertifizierung; regelmäßiger Mitarbeiter-Schulungen;**