Anlage /1 – Technisch-organisatorische Maßnahmen

Vertraulichkeit

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, durch elektronisches Schließsystem mit Chipschlüssel (für die Büroräume und zusätzlich für die Serverräume der Verantwortlichen), Schlüssel, Alarmanlage (nach Bereichen getrennt), Zugang Externer in die Büroräumlichkeiten nach Absprache, Zugang zu den Serverräumen nur mit entsprechender Berechtigung (alarmgesichert);
- **Zugangskontrolle:** Schutz vor unbefugter Systembenutzung und Dateneinsicht durch Authentifikation mit Benutzername und Kennwort (einschließlich entsprechender Policy) und Zertifikate, Zuordnung von Benutzerrechten, Einsatz von VPN-Technologie, Einsatz von Schutzprogrammen (Firewall, Antivirensoftware etc.) und automatische Sperrmechanismen, Verschlüsselung von Datenträgern wo angemessen;
- **Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Anzahl der Administratoren auf das Notwendigste reduziert, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, tägliche Datensicherung, Einsatz von Aktenvernichtern;
- **Anonymisierung:** Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung bei nicht aufrechter Kundenbeziehung und sofern nicht mehr erforderlich überschrieben;
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

- **Weitergabekontrolle:** Alle Mitarbeiter:innen und Sub-Auftragnehmer sind dem Datengeheimnis verpflichtet (gem. Art. 2 § 6 DSG). Es erfolgt kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport bzw. Zugriff auf Ressourcen. Getroffene Maßnahmen sind z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle:** Es besteht die Möglichkeit der Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B. durch Protokollierung und Nachvollziehbarkeit bis auf Userebene (personenbezogene Benutzer), Rechte auf Basis eines Berechtigungskonzepts, Dokumentenmanagement;

Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle & Datenintegrität:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch entsprechende Backup-Strategie (on-site/off-site, Backupserver physisch getrennt), unterbrechungsfreie Stromversorgung (USV), Einsatz von Festplattenspiegelung bei allen relevanten Servern, Security Checks auf Infrastruktur- und Applikationsebene, mit Experten sachkundig geplanter Einsatz von Schutzmaßnahmen (Virenschutz, Firewall, Verschlüsselung, Spamfilter), Systemmonitoring, Sicherungskonzept, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche **Wiederherstellbarkeit**;

- **Löschungsfristen:** Für Kundendaten (nach gesetzlichen Vorgaben, Kundenvorgaben und unter Berücksichtigung von berechtigtem Interesse);

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management, Mitarbeiter:innen-Schulungen, Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers/Verantwortlichen, Auswahl von (Sub-) Auftragnehmern unter Sorgfaltsgesichtspunkten (v.a. im Hinblick der Datensicherheit), regelmäßige Überprüfung der (Sub-) Auftragnehmer, sowie eine möglichst eindeutige Vertragsgestaltung mit ggf. Vertragsstrafen bei Verstößen und Nachkontrollen;

Stand: Oktober 2025