Anhang „Technisch-organisatorische Maßnahmen nach § 9 BDSG

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

Im Einzelnen werden folgende Maßnahmen bestimmt:

Nr	Maßnahme	Umsetzung der Maßnahme
1	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	• Festlegung befugter Personen • (Betriebsangehörige und Betriebsfremde) • Access-Chip Regelung • Regelung für Firmenfremde • Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage • Türsicherung (elektrischer Türschließer, Ausweisleser) • Entsprechende Ausgestaltung der • Maßnahmen zur Objektsicherung (z.B. Einbruchmeldesystem, Geländebewachung)
2	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	• Teilweise Verschlüsselung • Vergabe und Sicherung von Identifizierungsschlüsseln (User ID) • Regelung der Benutzerberechtigung • Verpflichtung auf das Datengeheimnis nach § 5 BDSG • Differenzierte Zugriffsregelung (z. B. durch Segmentzugriffsperren) • Protokollierung und Auswertung der Dateibenutzung

3	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung un- und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können	• Verschlüsselung • Regelung der Zugriffsberechtigung • Auswertung von Protokollen • Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen
4	**Weitergabekontrolle** Es ist zu gewährleisten, dass perso-nenbezogene Daten bei der elektro-i-schen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung perso-nenbezogener Daten durch Einrich-tungen zur Datenübertragung vorgesehen ist.	• Verschlüsselung • Feststellung befugter Personen • Gesicherter RZ Eingang für An und Ablieferung • Ausgabe von Datenträgern nur an autorisierte Personen (z. B. Auftragsquittung, Begleitpapier) • Datenträger Verwaltung Bestandskontrolle • Gesonderter Verschluss vertraulicher Datenträger • Sicherheitsschränke • Kontrollierte Vernichtung von Datenträgern (z. B. Fehldrucke) • Regelung der Anfertigung von Kopien • Dokumentation der Abruf und Übermittlungsprogramme • Bestimmte autorisierte Benutzer • Verpackungs-und Versandvorschriften (Versandart z. B. in verschlossenen Behältnissen) • Direktabholung, Kurierdienst, Transportbegleitung • Löschung von Datenresten vor Datenträgeraustausch
5	**Eingabekontrolle** Es ist zu gewährleisten, dass nach-träglich überprüft und festgestellt werden kann, ob und von wem perso-nenbezogene Daten in Datenverarbei-tungssysteme eingegeben, verändert oder entfernt worden sind	• Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe • Protokollierung von Eingaben • Protokollierung der Dateibenutzung • Verfahrens-, Programm- und Arbeitsablauforganisation • Verpflichtung auf das Datengeheimnis

6	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	• Erfüllung von Datenverarbeitungsverträgen • Sicherer Daten-und Datenträgertransport (idR. DHL) • Sichere Datenverarbeitung • Sichere Datenlöschung nach erfülltem Auftrag • Interne Prozesse zur Auftragserfüllung und Überwachung der Prozesse • Standard Change Management Prozess (nach ITIL)
7	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind	• Maßnahmen zur Datensicherung (physikalisch / logisch). • Backups • Sicherungsverfahren und Archivierung • Wiederherstellung der Infrastruktur (Desaster Recovery) • Schutz gegen „malicious code"
8	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können	• Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken. • Mandantentrennung • Funktionstrennungen • Trennung von Test-und Produktivsystemen