



Anlage 1 – Technisch-organisatorische Maßnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten. Die Parteien haben das erforderliche Schutzniveau gemeinsam ermittelt und sind zu dem Ergebnis gekommen, dass ein sehr hohes Schutzniveau einzuhalten ist.

Das Schutzniveau wird durch diese Maßnahmen eingehalten:

a. Vertraulichkeit

- Türsicherung: Zutritt in die Räumlichkeiten mit Chipkarten der Mitarbeiter gesichert; der Zutritt ist jeweils beschränkt auf den notwendigen Personenkreis
- Gesicherter Eingang für An- und Ablieferung
- Authentifikation mit Benutzer ID und Passwort; Regeln zur Vergabe von Benutzer IDs und Passwörtern; es wird ein regelmäßiger Passwortwechsel erzwungen
- Einsatz von Anti-Viren-Software und Firewalls
- sorgfältig ausgewähltes Reinigungspersonal
- Verpflichtung auf das Datengeheimnis
- Regelungen für die Vergabe von Zugriffsberechtigungen
- Zugriff auf PCs durch Windows-Anmeldung gesichert, automatische Abmeldung bei Abwesenheit vom Arbeitsplatz

b. Integrität

- Sofern angelieferte personenbezogene Zahlungsdaten verändert oder entfernt werden müssen, geschieht dies nur in begründeten Fällen und anschließend gemäß schriftlichem oder telefonischem Auftrag
- Verpflichtung auf das Datengeheimnis

c. Verfügbarkeit und Belastbarkeit/Physischer oder technischer Zwischenfall

- Angelieferte Kundendaten werden redundant gespeichert, so dass beim Ausfall eines Datenspeichers die Daten noch vorhanden sind
- Tägliche Vollsicherung des Datenbestandes
- Notfallkonzeption und Durchführung von Notfalltests

d. Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen

- Es finden in regelmäßigen Abständen interne Auditierungen statt
- Datenschutzvorfälle werden stets dokumentiert und ausgewertet
- Es existiert ein angemessenes Informationssicherheitsmanagement / Informationsrisikomanagement
- Beteiligung des Datenschutzbeauftragten beim Abschluss neuer Vereinbarungen zur Auftragsverarbeitung
- Regelmäßige Kontrollen des Datenschutzbeauftragten und des Informationssicherheitsbeauftragten