Merkblatt 2
zum Vertrag zur Auftragsverarbeitung
gemäß Art. 28 DS-GVO
–
Technische und organisatorische Maßnahmen (TOM)

Bezugnehmend auf Abschnitt 3 des Vertrags zur Auftragsverarbeitung nennt der Auftragnehmer (OS Datensysteme GmbH) folgende technische und organisatorische Maßnahmen:

a) Zutrittskontrolle

Zutrittssicherung an allen Zutrittsmöglichkeiten zum Sicherheitsbereich
Verzeichnis zur Verwaltung und Vergabe der individuellen Zutrittsberechtigungen zum Sicherheitsbereich
Einbruchmeldeanlage gegen unbefugten Zutritt zum Sicherheitsbereich
Einbruchmeldeanlage mit Aufschaltung zum Sicherheitsdienst
Zutritt von Mitarbeitern in den Sicherheitsbereich nur mit zutrittsberechtigtem ID-Chip/Schlüssel
Zutritt betriebsfremder Personen nur nach vorheriger Identifikation
Zutritt außerhalb der Geschäftszeiten nur mit elektrischer Türöffnung
Dokumentation der Vergabe von Schlüsseln

b) Zugangskontrolle

Keine unbefugte Systembenutzung möglich
Verwendung von sicheren Kennwörtern
Automatische Sperrmechanismen
Zwei-Faktor-Authentifizierung
Zugangsberechtigung zu personenbezogenen Daten nur für Mitarbeiter mit der jeweiligen Zugangsberechtigung
Verschlüsselung von Datenträgern
Verwaltung und Dokumentation der Vergabe von Schlüsseln, und Schließberechtigungen an Betriebsangehörige

c) Zugriffskontrolle

Kein unbefugtes Lesen von Daten von nicht berechtigten Personen möglich
Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
Protokollierung von Zugriffen
Verpflichtung aller Mitarbeiter auf alle einschlägigen und relevanten Gesetze
Sorgfältige Auswahl und fortlaufende Kontrolle der Mitarbeiter
Durchführung interner Audits

d) Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

e) Pseudonymisierung (Art. 32 Abs. 1 a DS-GVO; Art 25 Abs. 1 DS-GVO)

Die Verarbeitung der personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technische und organisatorische Maßnahmen unterliegen

Merkblatt 2
zum Vertrag zur Auftragsverarbeitung
gemäß Art. 28 DS-GVO
–
Technische und organisatorische Maßnahmen (TOM)

f) Maßnahmen zur Sicherstellung von Integrität

Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind: Protokollierung, Dokumentenmanagement.
Arbeitsanweisungen und Qualitätsmanagementsystem zur Sicherstellung der Integrität
Regelmäßige Schulung aller Mitarbeiter auf die in ihrem Arbeitsbereich wichtigen, datenschutzrelevanten Aspekte bei der Auftragsdurchführung

g) Maßnahmen zur Sicherstellung von Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: Backup-Strategie, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.
Einbruchmeldeanlage im Sicherheitsbereich
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 c DS-GVO).
Notfallplanung zur Prävention und Bewältigung von Notfällen

h) Maßnahmen zur Gewährleistung der Wirksamkeitskontrolle

Verfahren für regelmäßige Kontrollen/Audits
Definition von Prozessen und Arbeitsanweisungen zur Sicherstellung der vertraglich vereinbarten Leistungen

i) Weisungskontrolle bzw. Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen
Verpflichtung aller Mitarbeiter auf alle einschlägigen und relevanten Gesetze
Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern