

## Anlage 2: Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen zum Datenschutz durch den Auftragnehmer werden verbindlich vereinbart:

### I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

#### 1) Zutrittskontrolle

Ein unbefugter Zutritt zu den Datenverarbeitungsanlagen und Datenträgern ist durch geeignete Maßnahmen zu verhindern, zum Beispiel durch ein Zutrittskontrollsystem (Ausweisleser, Magnetkarte, Chipkarte), Schließsystem mit dokumentierter Schlüsselvergabe, Türsicherung, Werkschutz, Pförtner, Überwachungseinrichtung.

#### 2) Zugangskontrolle

Das Eindringen in die IT-Systeme des Auftragnehmers und deren Nutzung durch Unbefugte ist zu verhindern, zum Beispiel durch Kennwort- / Passwortschutz, Benutzerrechtssystem, Benutzeridentifikation, Authentifizierung und Verschlüsselung von Datenträgern.

#### 3) Zugriffskontrolle

Unerlaubte Tätigkeiten in den IT-Systemen des Auftragnehmers außerhalb eingeräumter Berechtigungen sind zu verhindern, zum Beispiel durch bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.

#### 4) Mobiler Datenzugriff

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

#### 5) Trennungskontrolle

Eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden ist sicherzustellen. Dies gilt für die Datentrennung verschiedener Kunden des Auftraggebers. Datenträger, die vom Auftraggeber stammen oder für diesen genutzt werden, sind gesondert zu kennzeichnen. Eingang und Ausgang sind zu dokumentieren.

### II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

#### 1) Weitergabekontrolle

Der Auftragnehmer hat in seinem Unternehmen das Ob und das Wie einer Weitergabe der personenbezogenen Daten zu regeln, insbesondere für die elektronische Übertragung, den Datentransport und die Übermittlungskontrolle. Geeignete Schutzmaßnahmen sind zu ergreifen, zum Beispiel Verschlüsselung / Tunnelverbindung (VPN), elektronische Signatur, Protokollierung und Transportsicherung. Auch physische Datenträger sind zu verschlüsseln. Die kontrollierte Vernichtung von Datenträgern und Papierdokumenten nach DIN-Norm 66399 mit Sicherheitsstufe 4 ist ebenfalls sicherzustellen.

## **2) Eingabekontrolle**

Der Auftragnehmer ist zur Protokollierung und Dokumentation der vertragsgegenständlichen Datenverarbeitung verpflichtet. Hierzu gehört auch die regelmäßige Kontrolle der System- und Nutzungsprotokolle.

## **3) Verschlüsselung**

Der Auftragnehmer hat die vertragsgegenständlichen Daten sowohl auf seinem vertragsgegenständlichen IT-System als auch beim Transport im Rahmen eines Datenabrufs durch den Auftraggeber bzw. dessen Kunden nach dem aktuellen Stand der Technik zu verschlüsseln.

# **III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

## **1) Verfügbarkeitskontrolle**

Die Daten sind gegen Zerstörung oder Verlust zu schützen, insbesondere durch effektive Maßnahmen zur Datensicherung (Redundanz; Backupkonzepte), unterbrechungsfreie Stromversorgung (USV), getrennte Aufbewahrung der Datensicherungen, Virenschutz / Firewall. Der Auftragnehmer ist verpflichtet, ein Notfallkonzept zur Notfallvorsorge zu unterhalten und umzusetzen, das dem aktuellen Stand der Technik entspricht und dies auf Anforderung nachzuweisen.

## **2) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)**

Die Wiederherstellbarkeit gesicherter Daten hat der Auftragnehmer zu gewährleisten.

# **IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**

## **1) Aktualität**

Der Auftragnehmer hat seine technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen, zu bewerten und zu evaluieren, insbesondere durch ein Datenschutz-Management-System und die Anwendung datenschutzfreundlicher Voreinstellungen (Art. 25 Abs. 2 DSGVO).

## **2) Auftragskontrolle**

Der Auftragnehmer muss die weisungsgemäße Auftragsdatenverarbeitung gewährleisten, zum Beispiel durch vertragliche Verpflichtungen seiner Mitarbeiter, Erteilung eindeutiger Weisungen an diese, Auswahl qualifizierter Mitarbeiter und Kontrolle der Arbeitsergebnisse der Mitarbeiter.

## **3) Datenschutzbeauftragter**

Der Auftragnehmer hat einen fachkundigen Datenschutzbeauftragten zu bestellen, sofern die gesetzliche Pflicht einer Bestellung vorliegt und dem Auftraggeber dessen Kontaktdaten unaufgefordert zu nennen. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Sofern der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, teilt er dem Auftraggeber einen Ansprechpartner für alle Datenschutzfragen mit.