

AV-Vertrag: Anlage 1

Technische und organisatorische Maßnahmen
des Auftragnehmers zur Gewährleistung der
Datensicherheit

Soziales | Gesundheit | Bildung | Kultur | Heimat | Umwelt

1. Maßnahmen zur Pseudonymisierung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

(Gewährleisten, dass die Verarbeitung personenbezogener Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

Übermittlung von Daten in anonymisierter oder pseudonymisierter Form auf Basis der Notwendigkeit und Erforderlichkeit der Datenverarbeitung
Einhaltung der Grundsätze der Erforderlichkeit, Speicherbegrenzung und Datenminimierung
Verwendung von Pseudonymen und Anonymen / Aggregierte Daten
getrennte Aufbewahrung von Pseudonymen und Zuordnungstabellen

Weitere: _____

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

(Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

Elektronisches Schließsystem
Sicherheitsschlösser
Mechanisches Schloss
Chipkartensystem
PIN-Eingabe
Pfortner / Videoüberwachung / Bewegungsmeldeanlage
Einlasskontrolle / Anmeldung
Sicherheitsdienst / Wachdienst
Einbruchmeldeanlage (EMA)
Umzäuntes / Ummauertes Gebäude
Räumlichkeiten mind. Im 2. Obergeschoss
Absicherung von Gebäudeschächten
Einbruchsicherung (Sichere Verglasung, Einbruchssichere Fenster)

Weitere: _____

Zugangskontrolle

(Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

Authentifizierung mit benutzerbezogenen Kennungen und Passwörter
Passwortvergabe nach allgemein gültigen BSI-Standards
Zentrales Passwortmanagement / z.B. Passwortmanager
Dokumentierte Passwortrichtlinie
Plausibilitätsprüfung der Passwörter
Sperrung nach mehrmaliger Falscheingabe
Automatische Desktopsperre
Anweisung zur manuellen Bildschirmsperre
Verschlüsselter Zugang von extern (z.B. VPN-Tunnel, Netzwerkeinbindung, Token)
Firewall nach aktuellem Stand der Technik

Weitere: _____

Zugriffskontrolle

(Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten nach der Speicherung und bei der Verarbeitung, Nutzung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

Eingeschränkte Benutzerrechte
Trennung von Anwender- und Administratorenrechten
Festlegung von Datenbankrechten
Protokollierter und nachvollziehbarer Zugriff
regelmäßige Stichprobenkontrollen
Dokumentiertes Rollen- und Rechtekonzept
Genehmigung der Erteilung durch Vorgesetzte / auf Antrag nach vorgegebenem Prozesse
Protokollierte Änderung der Berechtigungen
Entzug der Berechtigungen nach Ausscheiden des Mitarbeiters
Sichere Entsorgung von nicht mehr benötigten Datenträgern/ Daten, sodass eine Rekonstruktion nicht möglich ist
Verschlüsselung der Datenträger
Kopien/ Backups werden in einem separaten verschlossenen Brandabschnitt aufbewahrt

Weitere: _____

Trennungskontrolle

(Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

- Physische Trennung von Datenbeständen
- Logische Trennung von Datenbeständen
- Testumgebung für neue Applikationen
- Mandantenfähigkeit in relevanten Anwendungen
- Speicherkonzept erstellen
- Kontrolle Datenbestände
- Steuerung über Berechtigungskonzept

Weitere: _____

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

- VPN-Verbindungen
- E-Mail-Verschlüsselung
- Verschlüsselung von E-Mail-Anhängen
- Deaktivierung von Schnittstellen an PCs (z.B. USB)
- Sichere Transportbehälter
- Verschlüsselte Verbindungen wie sftp oder https
- Sensibilisierung und Schulung Mitarbeiter
- Konkrete und verbindliche Anweisungen
- Dokumentation Datenempfänger
- Persönliche Übergabe mit Protokoll

Weitere: _____

Eingabekontrolle

(Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt werden.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

Protokollierte Anmeldung im System
Festhalten aller zur Rückverfolgung benötigten Daten
Protokollierte Änderungen in den Bewegungsdaten
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten individueller Benutzer
Vergabe von Berechtigungen zur Eingabe, Änderung und Löschung auf Basis eines Rechte- und Rollenkonzepts
Plausibilitätsprüfungen bei Eingabe

Weitere: _____

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

Spiegelung der Festplatten, Datenreplikation
Regelmäßige Backups / revisionssichere Archivierung
Dokumentiertes Datensicherungskonzept
Schutz vor Spyware
Spamfilter
Externe Datenträger werden vor Gebrauch auf Viren überprüft
Sperrung von Zugängen
Virenschutz
Regelmäßige Aktualisierung der Antiviren-Software
Schriftliche Erklärung der Mitarbeiter, dass Belehrung stattgefunden hat

Weitere: _____

5. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

(Gewährleisten, dass eine rasche Wiederherstellung der Daten bei einem Datenverlust realisiert werden kann.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

Disaster-Recovery-Konzept / Notfallplan / Dokumentiertes Notfallkonzept

Datensicherungs- / Datenwiederherstellungskonzept

Regelmäßige Tests der Wiederherstellung von Datensicherungen

Weitere: _____

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

Auftragskontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.)

(Auftragnehmer: **Bitte zutreffendes ankreuzen**)

vertragliche Regelung in Bezug auf den Einsatz von Subunternehmen, insbesondere Sicherstellung einer sicheren Datenübermittlung aufgrund geeigneter Garantien sowie die vertragliche Verpflichtung, etwaige Pflichten aus der Vereinbarung im Auftrag auch auf Subunternehmen zu übertragen

Sicherstellung der Vernichtung, Löschung und Herausgabe der Daten nach Auftragsbeendigung

Verpflichtung zur Vertraulichkeit eingesetzter Mitarbeiter

Sicherstellung der Verpflichtung zur Geheimhaltung von Berufsgeheimnissen eingesetzten Personals

Überprüfung der technischen und organisatorischen Maßnahmen und Kontrolle

Weitere: _____