Anlage Vertrag zur Auftragsverarbeitung: Technische und organisatorische Maßnahmen als Auftragsverarbeiter Art. 30 Abs. 2 lit. und § 64 BDSG

Version 2.3 vom 18.9.2023

Die TOM sind technische sowie organisatorische Maßnahmen, um eine strikte und rechtskonforme Einhaltung der Datenschutzbestimmungen zu gewährleisten. Jeder Verantwortliche, der personenbezogene Daten verarbeitet, muss Sicherheit dieser Verarbeitung gewährleisten und nachweisen können.

Mit dem Ziel eines angemessenen Schutzniveaus sind die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind. Dies können sein: Vernichtung, Verlust oder Veränderung, unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung / unbefugten Zugang zu personenbezogenen Daten, die verarbeitet werden.

Die DSGVO fordert in Artikel 32 unter anderem

1. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
2. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
4. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Zugangskontrolle

Es soll bei IT-Systemen sichergestellt sein, dass nur berechtigte Personen oder Computer Zugang und Zutritt zur IT erhalten. Die unbefugte Nutzung wird verhindert. Die Identifikation und die Authentifikation sind zentrale Elemente der Zugangskontrolle.

☒ Absicherung durch Alarmanlage selektiv	☒ Sorgfältige Auswahl von Wachpersonal bei Alarmauslösung
☐ Sicherheitsverglasung	☐ Absicherung von Kellerschächten
☒ Sicherung von Gebäudeschächten, Fenstern und Türen	☒ Chipkarten-/Transponder-Schließsystem
☐ Automatisches Zugangskontrollsystem	☒ Manuelles Schließsystem nur 7 Generalschlüssel
☐ Schließsystem mit Codesperre	☐ Videoüberwachung der Zugänge
☐ Biometrische Zugangssperren	☒ Sicherheitsschlösser, nur berechtigte haben einen Schlüssel, Ausgabe- und Rückgabeprotokoll Büroräume mit besonders schützenswerten Daten
☒ Lichtschranken / Bewegungsmelder	☒ Authentifikation mit Benutzername / Passwort
☒ Schlüsselregelung (Schlüsselausgabe, etc.)	☐ Gehäuseverriegelungen
☒ Protokollierung / Kontrolle der Besucher	☐ Sperren von externen Schnittstellen(z.B. USB, etc.)
☐ Besucherausweise	☒ Sorgfältige Auswahl von Reinigungspersonal
☐ Tragepflicht von Berechtigungsausweisen	

- Einsatz von Angriffserkennungssystemen
- Einsatz von Anti-Viren-Software
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
OpenVPN, WireGuard
- Verschlüsselung von Smartphone-Inhalten
Android / iOS integrierte Verfahren
- Einsatz von zentraler MDM-Software
- Einsatz einer Hardware-Firewall
Bei Hetzner
- Einsatz einer Software-Firewall
Eigenentwicklung auf Basis von Debian Linux
- Bildschirmsperren sind eingerichtet, Anweisungen
hierzu veröffentlicht

- Verschlüsselung von mobilen Datenträgern
BitLocker / FileVault / LUKS

Datenträgerkontrolle

meint Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern

Verschlüsselung von Datenträgern

- Sichere Aufbewahrung von Datenträgern,
z.B. durch verschlossene Räumlichkeiten oder Behälter
- Es besteht ein Berechtigungskonzept für die Daten
- Richtlinien wurden erstellt zum Umgang mit Datenträgern
- Protokollierung der Eingabe, Änderung und Löschung von Daten
auf Servern

Eingabekontrolle

Durch die Etablierung von Maßnahmen in diesem Bereich kann genau überprüft werden, wer welche personenbezogenen Daten innerhalb der Datenverarbeitungssysteme eingegeben, verändert oder gelöscht hat.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle
Benutzernamen (nicht Benutzergruppen)
selektiv
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben,
geändert und gelöscht werden können.
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen
worden sind
- Sonstiges:

Speicherkontrolle

Im Gegensatz zur Eingabekontrolle geht es hier nicht um die Überprüfbarkeit der Datenverarbeitungen, sondern um die Verhinderung von unbefugten Datenverarbeitungen. Die technisch-organisatorischen Maßnahmen orientieren sich dabei an den Beispielen zur Eingabekontrolle.

- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

- Authentifikation durch die Eingabe eines Benutzernamens und Passwortes
- Festlegung zugangsberechtigter Mitarbeiter
- Regelmäßige Kontrollen bezüglich der Berechtigungen
selektiv
- Passende Zuteilung von Benutzerprofilen zu IT-Systemen

Zugriffskontrolle

steuert den Zugriff auf Computerressourcen und Daten für Berechtigte.

- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Physische Löschung von Datenträgern vor Wiederverwendung
- Verwaltung der Rechte durch Systemadministrator
- Datenschutzkonforme Passwortregeln
- Sichere Aufbewahrung von alten Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Datenschutzkonforme Vernichtung von Datenträgern (Akten, Laufwerke etc.)
- Sonstiges:

Weitergabekontrolle

Mit der Weitergabekontrolle sind Maßnahmen gemeint, die die Sicherheit von personenbezogenen Daten während einer Datenweitergabe sicherstellen. Vor allem dürfen während der Datenübermittlung oder des Transportes die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Es findet keine Weitergabe an Dritte statt.
- Kontrolle der Datenempfänger und entsprechende Dokumentation dieser Empfänger selektiv
- E-Mail-Verschlüsselung Es wurde eine Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen erstellt
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen Das Anschließen privater Datenträger ist untersagt.
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form Sonstiges:

Transportkontrolle

Bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern muss die Vertraulichkeit und Integrität der Daten gegeben bleiben.

- Es findet kein Transport der Daten durch uns statt.
- Nachweis über Versand, Kennzeichnung und Inventarisierung von Datenträgern
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -Fahrzeugen

Übertragungskontrolle

Die Übertragungskontrolle soll die Vertraulichkeit der elektronischen Datenübertragung sichern.

- Passwortschutz einzelner Dokumente
- E-Mail-Verschlüsselung für sensible Daten
- Einrichtungen von Standleitungen bzw. VPN-Tunneln

Rasche Wiederherstellbarkeit

Eingesetzte Systeme müssen im Störfall wiederhergestellt werden können.

- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Testen von Datenwiederherstellung
- Dokumentation der notwendigen Wiederherstellungsmaßnahmen
- Berechtigungskonzept für Zugriff auf Backups
- Sonstiges:

Zuverlässigkeit

Es muss gegeben sein, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen schnell gemeldet werden.

- Sicherheits-Updates werden zeitnah eingespielt (Konzept)
- Absicherung gegen Hardwaredefekte durch beispielsweise gespiegelte Festplatten oder zusätzliche Netzteile (Redundanz),
- Aufteilung der Dienste auf unterschiedliche Server; fällt ein System oder Dienst aus, ist der andere noch verfügbar selektiv

Datenintegrität

Hierzu gehört beispielsweise die Erstellung und Einrichtung eines Backup- und Recovery-Konzepts. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

- Es besteht ein Backup- & Recoverykonzept
- Fehlerprotokolle werden regelmäßig ausgelesen und ausgewertet.

Auftragskontrolle

meint, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) Teil des AV-Vertrages
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Überprüfung der Datenvernichtung nach Auftragsende
- Vertragsstrafen
- Auftragnehmer hat Datenschutzbeauftragten bestellt HM-Consult.de
- Sonstiges:

Verfügbarkeitskontrolle

Personenbezogene Daten müssen gegen Zerstörung oder Verlust geschützt sein.

- Unterbrechungsfreie Stromversorgung (USV)
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Serverräume nicht in der Nähe von Wasserrohren
- Feuer- und Rauchmeldeanlagen
- Klimaanlage in Serverräumen

- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- regelmäßige Tests für Datenwiederherstellungen
- In Hochwassergebieten: Serverräume über der Wassergrenze

Trennbarkeit

personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, sollten auch getrennt verarbeitet werden können. Dies betrifft die Mandantentrennung als auch die Kennzeichnung des Zwecks in Datensätzen.

- getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Klare Trennung der für verschiedene Zwecke gespeicherten Daten
- Es besteht ein Berechtigungskonzept
- Sandboxing
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Festlegung von Datenbankrechten
- Produktiv- und Testsystem werden getrennt
- Logische Mandantentrennung (softwareseitig)
- Sonstiges:

Pseudonymisierung / Verschlüsselung

sind Maßnahmen, die gewährleisten, dass Datenschutzgrundsätze, wie etwa Datenminimierung, wirksam umgesetzt und die notwendigen Garantien in die Verarbeitung aufgenommen werden, um den Anforderungen dieser Verordnung zu genügen.

- Wir pseudonymisieren die Daten selbst nicht
- Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Es werden geeignete technisch-organisatorische Maßnahmen zur Aufbewahrung der Zuordnungsdatei ergriffen.
- Die Pseudonymisierung ist im Verarbeitungsprozess so früh wie möglich durchzuführen.
- Pseudonymisierung wird zum Schutz der Vertraulichkeit wann immer möglich praktiziert.
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Sonstiges:

Datenschutz-Management

Die innerbetriebliche Organisation muss so gestaltet werden, dass sie den besonderen Anforderungen des Datenschützers gerecht wird.

- Regelmäßige Schulung der Mitarbeiter/innen zum Datenschutz.
- Es bestehen Standards für die IT-Sicherheit (IT Grundschutz BSI, ISO 27001, etc.) IServ arbeitet angelehnt an den Grundschutz, Zertifizierung ist in Planung
- Quartalsweise Schulung neuer Mitarbeiter
- Ein Verzeichnis der Verarbeitungstätigkeiten ist vorhanden.

- Es besteht ein Notfallplan
Zudem ein Kommunikationskonzept für den Notfall (sofern erforderlich) werden durchgeführt und protokolliert.
- Aufbewahrung der elektronischen Protokolle ist geregelt. Protokoll- und Log-Dateien werden regelmäßig ausgewertet.
- Schriftliche Bestellung eines Datenschutzbeauftragten: datenschutz@hm-consult.de Datenschutz- und Datensicherungsmaßnahmen werden gelegentlich unvermutet kontrolliert.
- Nachweise über die Verpflichtung auf das Datengeheimnis sind vorhanden. Sonstiges:
- Ein Datenschutzkonzept ist vorhanden. Es erfolgen Aktualisierungen /Evaluierungen in regelmäßigen Abständen
- Datenschutz-Folgenabschätzungen Es liegen folgende Zertifikate/ Prüfberichte vor:

Incident-Response-Management

Im Falle einer Datenpanne muss eine unmittelbare Information an den Auftraggeber erfolgen können.

- Schulung der Mitarbeiter bzgl. Erkennen einer Datenpanne Teil der Basisschulung Es gibt ein Konzept zur Meldung von Datenpannen an den Auftraggeber.
- Es existiert ein internes Incident-Response-Management-Konzept Sonstiges:

Homeoffice

Das Homeoffice erfordert besondere technisch-organisatorische Maßnahmen

Wenn Mitarbeiter im Homeoffice auf Kundendaten zugreifen, muss der Arbeitgeber für Datenschutz und Datensicherheit sorgen. Das BSI hat deutlich gemacht, dass das Homeoffice ein besonderes Risiko für die Sicherheit von Daten darstellt.

- Lokales Speichern ist nur temporär auf verschlüsselten Datenträgern erlaubt, die Daten sind so bald wie möglich auf einen Server zu übertragen
- Es wird im Homeoffice nur firmeneigene Hardware eingesetzt
- Verbindung zu Firmenservern nur über sichere VPN-Tunnel OpenVPN
- Es bestehen Anweisungen zum datenschutzkonformen Arbeiten
- Das Verwenden oder Anschließen von privater Hardware ist untersagt.
- Sonstiges: