jweiland.net

DOKUMENTATION DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN bei jweiland.net

gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g)
und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

V 1.2 vom 01.09.2020

jweiland.net - Jochen Weiland
Echterdinger Straße 57
70794 Filderstadt

jweiland.net

jweiland.net

Teil 1: Maßnahmen am Sitz des Unternehmens

1. Zutrittskontrolle zu den Arbeitsbereichen

Maßnahmen der Zutrittskontrolle, die es Unbefugten verwehren, sich den Büroräumen, Datenverarbeitungsanlagen sowie den vertraulichen Akten und Datenträgern physisch zu nähern.

Maßnahmen
Organisation der Zutrittskontrolle:
Schlüsselbuch
Wachdienst - 24/7
Videoüberwachung mit Aufzeichnung
Besucher-Regulierungen

Allgemeine Gebäudesicherheit:
Manuelles Schließsystem
Schließung aller Gebäudeeingänge, wie Fenster und Türen
Büroräume und Gebäude sind außerhalb der Arbeitszeit verschlossen
Technische Sicherheitsmaßnahmen:
Video-Überwachung
Wachdienst

2. Zugangskontrolle zu Datenverarbeitungssystemen

Maßnahmen der Zugangskontrolle, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen
Allgemeine Gebäudesicherheit:

Zusätzliche Zugangsbeschränkung des Serverschrank
Keine Standardkennwörter aller System- und Infrastrukturkomponenten
Hardware- und Netzwerk-Sicherheitsmaßnahmen:
Schutz der Infrastruktur durch Hardware-Firewalls
Zugangsbeschränkungen für bestimmte IP-Adressbereiche
VPN-Beschränkungen
Portregeln/Sperrung von nicht erforderlichen Ports
Externer Zugang nur über sichere Verbindungen (VPN) mit Zwei-Faktor Authentifizierung
W-LAN an allen Rechnern deaktiviert
LAN Anbindung an allen Rechnern
Sichere Verschlüsselung aller Speichermedien
Software-basierte Sicherheitsmaßnahmen:
Regelmäßige Software-Updates
Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich
Zweifaktor-Authentifizierung
Zwangs- oder Pflicht-Änderung der Kennwörter nach der ersten Anmeldung
Erforderliche Mindestkomplexität für Kennwörter
Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Falle eines verlorenen oder vergessenen Authentifizierungsdatensatzes
Konfigurationsänderungen
Verschlüsselte Speicherung von User-Passwörtern
User-Login-Verlauf
Organisatorische Sicherheitsmaßnahmen:
Vertraulichkeitserinnerungen
Regelmäßige Überprüfung der Systeme

3. Zugriffskontrolle auf bestimmte Bereiche der Datenverarbeitungssysteme

Maßnahmen der Zugriffskontrolle, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Maßnahmen
Organisatorische Sicherheitsmaßnahmen:
Schriftliche Verpflichtung auf Vertraulichkeit nach DS-GVO
administrative Aufgabentrennung
Geregeltes Löschen / Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks
Regelmäßige Sicherheitsprüfungen
Technische Sicherheitsmaßnahmen:
Trennung von Anwendungs- und Administrationszugängen
Regelmäßige Sicherheits-Updates
Nutzung von Aktenvernichter (Sicherheitsstufe 4, DIN 66399)
Überwachung und Protokollierung allgemeiner Benutzeraktivität (Datenzugriff, Datenexport, Datenlöschung)

4. Weitergabekontrolle

Maßnahmen der Weitergabekontrolle, die bei der Übermittlung oder beim Transport von personenbezogenen Daten eingesetzt werden, um unberechtigte Zugriffe, insbesondere zum Lesen, Kopieren, Verändern oder Entfernen dieser Daten zu vermeiden.

Maßnahmen
Technische Sicherheitsmaßnahmen:
Protokollierung von externen Support-Prozessen

Organisatorische Maßnahmen:
Datentransfer und -weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers
Verbot der Nutzung von privaten Datenträgern
Dokumentation der Weitergabe von physischen Speichermedien
Datenschutzkonforme Löschung aller Datenkopien und Datensicherungen nach Abschluss des Auftrags

5. Eingabekontrolle

Maßnahmen der Eingabekontrolle die feststellen, wer personenbezogene Daten in Systeme eingegeben, geändert oder entfernt hat und die die Überprüfbarkeit dessen gewährleisten.

Maßnahmen
Technische Maßnahmen:
Rollenabhängige Zugriffsbeschränkungen
Protokollierung der relevanten Prozesse (Speicherung, Verarbeitung, Modifizierung, Abrufen, Übertragung, Löschung, etc.)
Protokollierung von administrativen Änderungen
Organisatorische Maßnahmen:
Konzept zur Datenlöschung

6. Auftragskontrolle

Maßnahmen der Auftragskontrolle die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen
Organisatorische Maßnahmen:

Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers
Definition von Rollen für unterschiedliche Aufgaben
Aufteilung der Zuständigkeiten
Festgelegte Ansprechpartner für Änderungsanfragen
Regelmäßige Datenschutz-Unterweisung der Mitarbeiter
Regelmäßige Besprechungen mit den Datenschutzbeauftragten in Bezug auf Betriebsprozesse, welche die Verarbeitung von personenbezogenen Daten betreffen
Technische Maßnahmen:
Automatisierte Kontrollmechanismen oder technische Beschränkungen, mit denen die Datenverarbeitung entsprechend den Weisungen des Auftraggebers sichergestellt wird
Fern-Zugriff erfolgt per VPN nur mit starker Verschlüsselung, erfordert eine Benutzerauthentifizierung

7. Verfügbarkeitskontrolle

Schutzmaßnahmen der Verfügbarkeitskontrolle gegen einen zufälligen Verlust oder eine zufällige Zerstörung von elektronischen Daten, Akten und Datenträgern.

Maßnahmen
Technische Maßnahmen:
Feuerlöscher
Disaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
Tägliche inkrementelle Datensicherung
Wöchentliche vollständige Datensicherung
Wöchentliche Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systeme

Organisatorische Maßnahmen:
Notfallplan

Klar definierte Verwaltungsaufgaben für Auftraggeber und Auftragnehmer

8. Trennungskontrolle

Ist in Ihrem Unternehmen die Trennungskontrolle gewährleistet, indem personenbezogenen Daten so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist?

Maßnahmen
Physikalische Datentrennung: Getrennte Computersysteme oder Medien
Logische Datentrennung: Separate Datenbanken oder strukturierte Dateiablage
Separate Instanzen für Entwicklungs- und Produktivsystemen

Teil 2: Maßnahmen am Ort des Rechenzentrums CGN1 - Köln

1. Präambel

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, treffen der Auftraggeber und der Auftragnehmer die nachfolgenden technischen und organisatorischen Maßnahmen (TOM). Diese gelten für die im Hauptvertrag definierten IT-Leistungen, welche in den unter Ziffer 2 definierten Rechenzentren erbracht werden. Bei der Auswahl der Maßnahmen wurden die vier Schutzziele des Art. 32 Abs. 1 b) DSGVO, namentlich die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, berücksichtigt. Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet. Alle technischen und organisatorischen Maßnahmen werden regelmäßig gemäß Art. 32 Abs. 1 d) DSGVO auf ihre Wirksamkeit hin geprüft.

Die nachfolgenden Angaben beziehen sich auf das von jweiland.net für Hostingleistungen genutzte Rechenzentrum in CGN1 in Köln.

2. Fähigkeit der Vertraulichkeit

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

Maßnahmen
Festgelegte Sicherheitsbereiche
Individuelle Zutrittsberechtigungsvergabe
Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum Data Center nur für autorisierte Personen.
Dokumentation der Zutrittsberechtigungen
Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.)
Besucher-Regulierungen
Automatisches Zuziehen und Verschließen von Türen
Schließung aller Gebäudeeingänge, wie Fenster und Türen
Zusätzliche mechanische Schutzmaßnahmen für das Erdgeschoss oder die Kellerfenster
Büroräume außerhalb der Arbeitszeit sind verschlossen
Schutz und Beschränkung der Zutrittswege

Transponder- oder schlüsselkartenbasierte Schließanlage
Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes
Dem im Hauptgebäude 24/7 befindlichen Personal werden die Alarmmeldungen angezeigt
Eingezäuntes Gelände mit Videoüberwachung
Zusätzliche Zugangsbeschränkung der Serverräume
Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten
Protokollierung von Benutzer relevanten Aktivitäten (Anmeldung, Abmeldung, Zugangsverweigerungen, etc.)
Demilitarisierte Zonen
Schutz der Infrastruktur durch Einbruchmeldeanlagen
Zugangsbeschränkungen für bestimmte IP Adressbereiche
VPN-Beschränkungen
Sperrung von nicht erforderlichen Ports
Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar)
W-LAN Verschlüsselung
Regelmäßige Software Updates
Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich
Einschränkung der zeitlichen Gültigkeit der Benutzerkonten
Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins
Zwangs- oder Pflicht-Änderung der Kennwörter nach der ersten Anmeldung
Ablauf von Benutzerpasswörtern
Erforderliche Mindestkomplexität für Kennwörter
Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passwortes
Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Falle eines verlorenen oder vergessenen Authentifizierungsdatensatzes
Verschlüsselte Speicherung von User-Passwörtern
User-Login-Verlauf
Vernichtung von physikalischen Medien nach DIN 66399
Nutzung eines Aktenvernichters (mindestens Sicherheitsstufe 3 gem. DIN 66399)

3. Fähigkeit der Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.

Maßnahmen
Rollenbasiertes Berechtigungskonzept (Lesen/Schreiben/Ändern/Kopieren/Löschen)
Dokumentation der Vergabe von Zugriffsrechten
Strenge administrative Aufgabentrennung
Protokollierung von externen Support-Prozessen
Dokumentation der Weitergabe von physischen Speichermedien
Logische Datentrennung: Separate Datenbanken oder strukturierte Dateiablage
Separate Instanzen für Entwicklungs- und Produktivsysteme (Sandboxes)
Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff/Berechtigungskonzept

4. Fähigkeit der Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Maßnahmen
Schutz der Infrastruktur durch Hardware-Firewalls
Software-Firewall
Antivirus Software auf allen Systemen
Überwachung und Protokollierung von administrativen Systemzugang und von Konfigurationsänderungen
Kontrollierter Zugang zu E-Mails und Internet
Trennung von Anwendungs-und Administrationszugängen
Überwachung und Protokollierung allgemeiner Benutzeraktivität
Protokollierung von externen Support-Prozessen

Protokollierung von administrativen Änderungen
Zugriffsregelungen und Zugriffsverwaltung
Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
Unterbrechungsfreie Stromversorgung (USV)
Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr
Kühlsystem im Rechenzentrum/Serverraum
Sollte es wider Erwarten zu einer Rauchentwicklung oder gar einem Brand kommen, flutet die aufwendige Feuerbekömpfungsanlage mit 150fachem Luftdruck das Data Center innerhalb von nur 60 Sekunden vollständig mit dem Löschgas Argon
Disaster-Recovery-Maßnahmen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
Tägliche inkrementelle Datensicherung
Wöchentliche vollständige Datensicherung
Wöchentliche Backups auf separat gespeicherten physikalischen Medien oder auf physikalisch getrennten Systemen
Der Kraftstoffvorrat ist für mindestens 16 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich
Geräte zur Überwachung der Temperatur und Feuchtigkeit im Data Center
Notfallplan
Externe Audits und Sicherheitstests
Klar definierte Verwaltungsaufgaben für Auftraggeber und Auftragnehmer

5. Verfahren zur regelmäßigen Überprüfung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

Maßnahmen
Regelmäßige Überprüfung der Systemzugangsberechtigungen
Interne und externe Audits
Disziplinarmaßnahmen im Falle einer Datenschutzverletzung
Regelmäßige Sicherheitsprüfungen
Regelmäßige Kontrolle externer Dienstleister
Regelmäßige Besprechungen mit dem bestellten Datenschutzbeauftragten in Bezug auf die Betriebsprozesse, welche die Verarbeitung personenbezogener Daten betreffen

6. Schutz vor unrechtmäßigem Zugang zu personenbezogenen Daten

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

Maßnahmen
Kontrollierter Zugang zu E-Mails und Internet
Trennung von Anwendungs- und Administrationszugängen
Regelmäßige Sicherheitsupdates
Überwachung und Protokollierung allgemeiner Benutzeraktivität
Verbot der Benutzung von privaten Datenträgern
Rollenabhängige Zugriffsbeschränkungen
Applikationsbasierte Überprüfung der Eingabeberechtigung

7. Verarbeitung personenbezogener Daten nur nach Anweisung

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

Maßnahmen
Vertraulichkeitserinnerungen
Schriftliche Verpflichtung aller Mitarbeiter auf die Wahrung der Vertraulichkeit
Regelmäßige Datenschutz-Unterweisung der Mitarbeiter
Geregeltes Löschen/Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks
Datentransfer und -weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers
Schriftliche Richtlinien für die Datenübertragung und -weitergabe
Verbindliche Regeln für die Offenlegung von sensiblen Daten
Datenschutzkonforme Löschung aller Datenkopien und Datensicherung nach Abschluss des Auftrags
Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Anweisungen des Auftraggebers
Festgelegte Ansprechpartner für Änderungsfragen

Kontrollrechte des Auftraggebers bei der Auftragsverarbeitung
Subunternehmer werden auf die gleichen Regelungen und Bestimmungen verpflichtet wie der Betreiber des Data Centers selbst

8. Anonymisierung / Pseudonymisierung / Verschlüsselung

Anonymisierung, Pseutonymisisierung oder Verschlüsselung von Daten des Auftraggebers sind grundsätzlich nicht Gegenstand der vom Betreiber des Data Centers zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen werden.

9. Belastbarkeit der Systeme

Der Betreiber des Data Centers unternimmt die unter Ziffer 4 dargestellten Maßnahmen um eine Belastbarkeit der IT-Systeme sicherzustellen. Penetrationstests der IT-Systeme des Auftraggebers sind grundsätzlich nicht Gegenstand der vom Betreiber des Data Centers zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen werden.

Teil 3: Cloud Hosting Service unter Nutzung der Amazon Web Services (AWS)

1. Präambel

Zusätzlich zu dem Hosting Angeboten im Rechenzentrum CGN-1 (siehe Teil 2), bietet jweiland.net ab 1.September 2020 auch Cloud Hosting Tarife unter Nutzung der Infrastruktur des auf externes Server-Hosting spezialisierten Sub- Auftragsverarbeiters Amazon Web Services EMEA SARL (AWS) am Standort Frankfurt/Main an.

2. Technische und organisatorische Maßnahmen bei AWS

Die aktuellen Informationen zu den TOM für das externe Hosting bei AWS sind abrufbar unter:
https://aws.amazon.com/de/compliance/data-center/controls/

3. Datenspeicherung ausschließlich in Deutschland

Alle Kundendaten im Rahmen des Cloud Hosting werden -soweit vom Kunden nicht ausdrücklich anders festgelegt- in der AWS Verfügbarkeitszone „Frankfurt/Deutschland" gespeichert. AWS garantiert dabei, die Daten nicht außerhalb der Verfügbarkeitszone zu transferieren:
https://aws.amazon.com/de/compliance/germany-data-protection/

4. Zertifizierungen der AWS Rechenzentren

AWS verfügt über international anerkannte Zertifizierungen, die von unabhängigen renommierten Beratungsgesellschaften attestiert wurden und die Erfüllung höchster Sicherheitsanforderungen nachweisen.
AWS verfügt unter anderem über folgende internationale Zertifizierungen:

- ISO 9001, Weltweiter Qualitätsstandard
- ISO 27001, Sicherheitsmanagementkontrollen
- ISO 27017, Cloud-spezifische Kontrollen
- ISO 27018, Schutz personenbezogener Daten

AWS hat im November 2016 als erster Cloud-Service-Anbieter in Deutschland vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ein C5-Testat für Cloud- Anwendungen erlangt:
https://aws.amazon.com/de/compliance/bsi-c5/

jweiland.net

Bearbeitungshistorie

Version	Bemerkung	Wer	Datum
1.0.0	Neufassung gem. DSGVO	JG	13.04.2018
1.1.1	Ergänzungen Teil 2 Data Center	JW	07.05.2018
1.1.2	Änderung Seite 5: - Schriftliche Verpflichtung von BDSG nach DS-GVO Änderung Seite 10: - DIN 32757 nach DIN 66399	JG	04.07.2019
1.2	Erweiterung TOM bezüglich Cloud Hosting und AWS Rechenzentren	JW	01.09.2020