DEMANDO

Technische und organisatorische Maßnahmen gem. Art. 32 Datenschutz-Grundverordnung

Stand Juni 2017

1. Technische und organisatorische Sicherheitsmaßnahmen

Gemäß Art. 32 DS-GVO sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

a) Innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

b) Konkretisierung der Einzelmaßnahmen

Zur Erfüllung der gesetzlichen Anforderungen sind in Art. 32 DS-GVO verschiedene Anforderungen / Kontrollen definiert. Der Auftragnehmer setzt die Anforderungen in seinem Einflussbereich in Bezug auf diese Vereinbarung um:

2. Zutrittskontrolle

Mit dem Begriff „Zutritt“ ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT-Systeme betrieben und genutzt werden. Dies können z.B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und Netzverkabelungen befinden und verlegt sind, gehören hierzu. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden (können), zu verwehren. Der Auftragnehmer muss deshalb dafür Sorge tragen, dass Unbefugte Räume, in denen Daten des Auftraggebers verarbeitet oder gespeichert werden, nicht betreten können und keinen Einblick oder Zugriff auf Datenverarbeitungsgeräte (Monitore, Drucker, etc.) erlangen können, auf denen Daten des Auftraggebers verarbeitet oder ausgegeben werden.

<u>Umsetzung der Zutrittskontrolle</u>

(1) Rechenzentrum (DEMANDO Datacenter):

- Überwachtes Betriebsgelände und Leitstelle.
- Mehrere Sicherheitsbereiche im Hochsicherheitsrechenzentrum.
- Sicherheitsschleusen mit unterschiedlichen Berechtigungsstufen.
- Fest definierter Prozess für Autorisierung der Zutritte zum RZ, einschließlich jährlicher Überprüfung, dass dieser Prozess eingehalten wird. Kontrollierte Schlüsselvergabe (im Notfall) an einen eng begrenzten Personenkreis.
- Zugang mit Code-Karte (Ausweisleser), PIN und Biometrie. Protokollierung des Zugangs.
- Videoüberwachung des kompletten Eingangsbereiches zum RZ und im RZ.

- Einbruchmeldeanlage
- Nur autorisierte Mitarbeiter haben Zutritt zu den Räumen in denen personenbezogene Daten verarbeitet werden.
- Besucher dürfen sich nur nach vorheriger Anmeldung und in Begleitung eines Mitarbeiters des RZ's im RZ-Sicherheitsbereich aufhalten.
- Nur wenige Mitarbeiter des Auftragnehmers dürfen Begleitpersonen mit in das RZ nehmen.
- Mit Zugangscode gesicherter Zutritt zu Serverräumen und Serverschränken. Der Code ist nur den zutrittsberechtigten Personen bekannt.

(2) Bürostandort

- Besucher müssen sich auch während der Geschäftszeiten per Klingel anmelden
- alle Außentüren sind stets verschlossen.
- Mitarbeiter nehmen die Besucher in Empfang.
- Besuchermanagement
- Alle Mitarbeiter sind angehalten fremde Personen ohne Begleitung in den Demando Räumen umgehend anzusprechen.
- Einsatz eines Sicherheitsdienstes
- Alarm gesicherte Räume
- Videoüberwachung im Eingangsbereich
- Zugang mit Code-Karte (Ausweisleser) Protokollierung des Zugangs.

3. Zugangskontrolle

Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV- Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden. Unbefugte dürfen keinen Zugang zu den Datenverarbeitungssystemen des Auftragnehmers erlangen können. Daher muss der Auftraggeber die mit der Erfüllung der Leistungen des Auftrags beauftragten Personen mit einer sicheren Benutzeridentifikation versehen.

<u>Umsetzung der Zugangskontrolle</u>

- Der Zugang zu den Systemen ist reglementiert und begrenzt auf Administratoren.
- Berechtigungen werden beschränkt auf die Tätigkeit im Rahmen des Administratorenauftrages vergeben. Die Identifikation erfolgt über persönliche Kennwortzugänge und verschlüsselte Kommunikation. Die Kennwortverfahren sind reglementiert. Bei Fehlversuchen erfolgt eine automatische Sperrung, der Anmeldevorgang wird protokolliert. Die Verschlüsselungsverfahren entsprechen dem Stand der Technik.

- Revisionssicheres Verfahren zur Vergabe der Berechtigungen und zum Rücksetzen der Passwörter.
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner).

4. Zugriffskontrolle

Die Anforderungen der Zugriffskontrolle sind darauf ausgerichtet, dass nur durch Berechtigte auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass die Daten nicht durch Unbefugte manipuliert oder gelesen werden können. Es ist zu verhindern, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Umsetzung der Zugriffskontrolle

- Der Zugriff zu Informationen wird ausschließlich nach dem “Bedarfs-Prinzip” gewährt.
- Bei Anmeldung an Datenverarbeitungssystemen wird dem Benutzer ein definiertes Profil oder eine entsprechende Rolle zugeordnet.
- Die Benutzerverwaltung, Identifikation und Authentifizierung erfolgt grundsätzlich nach den gleichen Prinzipien mit der notwendigen Eingrenzung der Zugriffsberechtigung (bedarfsgerechte Rechtevergabe).

5. Weitergabekontrolle

Der Auftragnehmer muss verhindern, dass personenbezogene Daten des Auftraggebers 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.

Umsetzung der Weitergabekontrolle

- Die Datenübertragung von und zum DV-System wird bei kritischen Aktivitäten (z.B. Systempflege, Software-Updates, Backup) durch folgende Maßnahmen gegen Nutzung durch Unbefugte gesichert:
- Verschlüsselte Datenübertragung (SSL).
- Protokollierung der Systemnutzung und Protokollauswertung.

6. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Es müssen daher für derartige Maßnahmen entsprechende Protokollierungssysteme vorhanden sein.

Umsetzung der Eingabekontrolle

- Jeder Login und jeder Zugriff wird temporär im Rahmen der Aufbewahrungsfristen protokolliert.

7. Auftragskontrolle

Der Auftragnehmer muss gewährleisten, dass personenbezogene Daten des Auftragnehmers nur gemäß dessen Weisungen verarbeitet werden. Beschäftigt der Auftragnehmer einen Unterauftragnehmer, so muss er diesen in gleicher Weise zur Erfüllung der Weisungen und zur Einhaltung des Datenschutzes verpflichten.

Umsetzung der Auftragskontrolle

- Unterauftragnehmer werden nur eingesetzt sofern dies vereinbart wurde.
- Beim Einsatz von Unterauftragnehmern achtet DEMANDO auf die ordnungsgemäße Vertragsgestaltung und auf die Erfüllung der Kontrollpflichten.

8. Verfügbarkeitskontrolle

Der Auftragnehmer muss dafür sorgen, dass personenbezogene Daten des Auftraggebers gegen zufällige Zerstörung oder Verlust im Rahmen des beauftragten Leistungsumfangs geschützt sind.

Umsetzung der Verfügbarkeitskontrolle

Brandschutz:

- Branddetektion für das gesamte Gebäude
- Mehrbereichslöschanlage nach VdS Richtinie 2095 für beide Serverräume und Technikräume
- Optische Brandmelder in 2 – Meldelinien-Abhängigkeit in Räumen, Doppelboden und Kaltgängen
- 2 Rauchansaugsysteme für die Bereiche außerhalb der IT-Sicherheitsräume
- Aufschaltung der Brandmeldezentrale auf die örtliche Leitstelle der Feuerwehr
- Gaslöschanlage mit Novec ™ 1230 für hohe Löscheffektivität, Umweltverträglichkeit und Personensicherheit

Energieversorgung:

- Die gesamte Stromversorgung, bestehend aus 2 redundanten Niederspannungshauptverteilern (NSHV), unterbrechungsfreier Stromversorgung (USV) und Unterverteilung-USV (UV-USV)
- Netzersatzanlage (NEA) für die Versorgung bei Spannungsausfall mit Treibstoffbevorratung bis zu 48 h und gesicherte Nachlieferung durch eigene Dieseltankstelle auf dem Gelände
- Redundante unterbrechungsfreie Stromversorgung (USV)
- Blitz- und Überspannungsschutz
- Trafostation mit mehreren Trafozellen
- Rittal Ri4Power, Systemverteiler für je 22 Serverracks
- Jedes Rack wird energieseitig von 2 Stromversorgungen eingespeist
- Integriertes Überwachungs- und Meldesystem

Klimatisierung:

- Direkte freie Kühlung über Luftkanäle mit regelbarem Temperatur und Luftmengenmassenstrom
- Luftführung über Luftkanäle im Doppelboden und intelligenter Steuerung (DDC)
- Kaltgangschottung
- Im Bedarfsfall zusätzlich wasserbasierte direkte Kühlung (skalierbar)
- Lüftungsgeräte in n+1 Redundanz

Netzwerk / Carrier:

- Mehrere Carrier sorgen für ausfallsichere Leitungen. Eine unterschiedliche Trassenführung und die Einspeisung in zwei getrennte Carrier-Räume gewährleistet höchste Ausfallsicherheit auf Leitungsebene. Wir unterhalten die Anbindungen an mehrere Carrier, um die bestmögliche Erreichbarkeit und ein optimales Routing unserer IP-Netze zu gewährleisten.

Überwachung & Support:

- Unser Rechenzentrum wird durch ein lokales Network Operations Center (NOC) überwacht. Das NOC verwendet modernste Systeme für die Überwachung und Wartung des Netzwerks und der Systeme.
- 24x7 Network Operation Center
- 24x7 Sicherheit, technischer Support
- 24x7 Netzwerkmonitoring

Datensicherung:

- Die Datensicherung erfolgt soweit Bestandteil des Leistungsgegenstandes entweder auf Band und/oder auf Disk (je nach Anwendung).
- Die Sicherungsdaten werden räumlich getrennt von den Produktivdaten aufbewahrt. Für Kunden kann dies auf Wunsch umgesetzt werden.

9. Trennungsgebot

Es ist dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten muss so gestaltet sein, dass eine „Vermischung" mit Daten anderer Vertragspartner / Auftraggeber des Auftragnehmers und auch unbefugte Zugriffe Dritter (auch versehentlich) unmöglich sind.

Umsetzung des Trennungsgebotes

- Es wird technisch und organisatorisch sichergestellt, dass kein Kunde auf die Daten eines anderen Kunden zugreifen kann.
- Demando sorgt dafür, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet und gespeichert werden.

10. Rechenzentrum

Das Rechenzentrum ist vom der TÜV Saarland mit der Nummer Z2015/1357 zertifiziert, gemäß der hochverfügbar Stufe 3tekPlus mit folgendem Prüfkatalog:

- Konzeption
- bauliche Sicherheit
- technische Sicherheit
- Dokumentation und Betriebsführung
- Organisatorische Anforderungen

DEMANDO

Zertifikat

TÜV SAARLAND
Geprüftes Rechenzentrum
Freiwilliges Prüfzeichen
www.tuev-saar.de

Geprüftes Rechenzentrum hochverfügbar Stufe 3tekPlus

Die Zertifizierende Stelle der tekit Consult Bonn GmbH, TÜV Saarland Gruppe, bestätigt hiermit, dass die Firma

Demando GmbH

Europaallee 10, D- 67657 Kaiserslautern

berechtigt ist, das Prüfzeichen „Geprüftes Rechenzentrum" für das

Rechenzentrum Stiftswaldstraße 4 in Kaiserslautern

als Ergebnis einer erfolgreichen Sicherheitsüberprüfung in Anlehnung an BSI-Grundschutz, ISO 27002 und TIA-942 zu führen. Der Nachweis wurde durch eine Auditierung vor Ort erbracht und beinhaltete folgende Punkte:

- Konzeption
- bauliche Sicherheit
- technische Sicherheit
- Dokumentation und Betriebsführung
- Organisatorische Anforderungen

Grundlagen dieser Zertifizierung sind

- die „Anforderungen an ein hochverfügbares Rechenzentrum Stufe 3tekPlus" V2.2,
- der Prüfbericht TR02116.

Das Zertifikat gilt ausschließlich für das auditierte Rechenzentrum zum Zeitpunkt der Prüfung und berechtigt den Inhaber unübertragbar, das abgebildete Prüfzeichen werblich im Gültigkeitszeitraum zu nutzen, sofern keine wesentlichen Änderungen des Rechenzentrums innerhalb der Laufzeit des Zertifikats vorgenommen werden.

Dieses Zertifikat ist bis zum 31. März 2019 gültig.

Zertifikat-Nr. Z2017/1738

Bonn, den 1. März 2017

GEPRÜFT tekit Member of TÜV Saarland Group TÜV SAARLAND APPROVED

tekit TÜV SAARLAND GRUPPE
Zertifizierende Stelle der tekit Consult Bonn GmbH
TÜV Saarland Gruppe
Alexanderstraße 10
53111 Bonn
Telefon +49 (0) 228 60 889-0, Fax -20
www.tekit.de, info@tekit.de