DOKUMENTATION DER TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

gem. Anlage zu Art. 32 DSGVO

V 1.4

domainfactory GmbH

Oskar-Messter-Straße 33

85737 Ismaning

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.

Generell gilt es folgendes zu beachten:

Die DomainFactory GmbH vermietet die Datenverarbeitungsanlage an den Kunden. Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung. Der Kunde entscheidet allein und ausschließlich darüber, welche personenbezogene Daten in welcher Weise verarbeitet werden („Herr der Daten“). Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Kunden erstellt und eingesetzt. DomainFactory sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Kunden in welchem Umfang genutzt werden. Die Datenverarbeitung erfolgt durch den Kunden. DomainFactory hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

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 jeweiligen Data Center nur für autorisierte Personen
Dokumentationen von Zutrittsberechtigungen
Zutrittsdokumentation
Autorisiertes Wachpersonal[1] - Während der Geschäftszeiten - 24/7 - Sichtkontrollen
Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.)
Besucher-Regulierungen
Regelmäßige Kontrollgänge durch das Sicherheitspersonal außerhalb des RZ-Bereiches
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
Alarmmeldungen können von vor Ort befindlichem Personal eingesehen werden
Eingezäuntes Gelände inkl. Videoüberwachung
Zutrittskontrollsystem mit Zutrittskarten
Zusätzliche Zugangsbeschränkung der Serverräume

[1] Nicht RZ Köln (CGN1)

Maßnahmen
Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten
Protokollierung von Benutzer relevanten Aktivitäten (Anmeldung, Abmeldung, Zugangsverweigerungen, etc.)
Demilitarisierte Zonen
Schutz der Infrastruktur durch Alarmmeldungen an Fenstern und Türen
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 (gem. DIN 66399)

3. Fähigkeit der Integrität (Gilt für alle RZ-Standorte)

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)

Maßnahmen
Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr bzw. bei lokalem Sicherheitspersonal
Kühlsystem im Rechenzentrum / Serverraum
Automatische Brandlöschanlage[2]
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 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 in den Data Centern
Notfallplan
Externe Audits und Sicherheitstests
Klar definierte Verwaltungsaufgaben für Auftraggeber und Auftragnehmer

5. Verfahren zur regelmäßigen Überprüfung (Gilt für alle RZ-Standorte)

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 den bestellten Datenschutzbeauftragten in Bezug auf Betriebsprozesse, welche die Verarbeitung von personenbezogenen Daten betreffen

[2] RZ Straßburg (SXB): erwartet Ende 2020; zurzeit Brandfrüherkennungssystem. RZ Limburg (OVH): Brandfrüherkennungssystem

6. Schutz vor unrechtmäßigem Zugang zu personenbezogenen Daten (Gilt für alle RZ-Standorte)

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

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

7. Verarbeitung personenbezogener Daten nur nach Anweisung (Gilt für alle RZ-Standorte)

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 Datensicherungen nach Abschluss des Auftrags
Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers
Festgelegte Ansprechpartner für Änderungsanfragen
Kontrollrechte der Auftraggeber bei der Auftragsdatenverarbeitung

Maßnahmen
Subunternehmer werden auf die gleichen Regelungen und Bestimmungen verpflichtet wie Domainfactory selbst

8. Anonymisierung / Pseudonymisierung / Verschlüsselung

Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten des Auftraggebers sind grundsätzlich nicht Gegenstand der von Domainfactory zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

9. Belastbarkeit der Systeme

Domainfactory 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 von Domainfactory zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

10. Rechenzentren der OVH SAS

Für Produkte, die in Rechenzentren unseres Subunternehmens OVH SAS bereitgestellt werden, können die oben dargestellten Technischen und Organisatorischen Maßnahmen abweichen. Dies ist im Dokument entsprechend vermerkt.