DOM DATACENTER

Serverbetrieb und Datenschutz

Stand: April 2021

Das DOM-Datacenter im Gebäude des Interxion in Düsseldorf ist als „Raum-In-Raum“-Konzept realisiert. Es wird rund um die Uhr von qualifiziertem Personal überwacht. Alle Gebäude sind mit Doppelboden, automatischen Feuerlöschsystemen, unterbrechungsfreier Stromversorgung und Netzersatzanlagen ausgestattet, um einen ausfallsicheren Betrieb der Systeme zu gewährleisten.
Die Fakten auf einen Blick:

NETZWERK	• Redundante Internetanbindungen durch eigenes AS / RIPE • Redundante Konfiguration für alle Backbone-Komponenten
KLIMAKONTROLLE	• Durchschnittstemperatur: 22°C/72°F ; Grenzbereiche 18°C/64°F und 25°C/77°F • Luftfeuchtigkeit: 50% +/- 10% • Redundante Wärme-, Raumklima- und Belüftungssysteme • Klimakontrolle gemäss ETS 300019 class 3.1 „Telecommunications Centers“.
STROMVERSORGUNG	• Redundante, unterbrechungsfreie Stromversorgung, abgesichert durch USV und Generator • Potenzialausgleich und Überspannungsschutz • Diesel Notstromgeneratoren • Verfügbarkeit 99,99%
SICHERHEIT	• Nur autorisiertem und registriertem Personal wird Zutritt gestattet • Sicherheitsbereiche sind mit Alarmsystemen ausgestattet, Zutritt nur mit Keycard und Finger-Scan • Protokollierter Zutritt • Fernüberwachung aller Gebäude • Zugangskontrolle gern. EU-Norm Stufe3, EN 50133-1
FEUERSCHUTZ	• Gasfeuerlöschsystem (FM200, Inergen) • Lasergesteuertes Rauchfrühwarnsystem (VESDA) • Feuerschutzwände (F60)
VERKABELUNG	• Führung der Stromkabel unter Doppelboden • Kabelpritschen unter der Decke für UTP- und Glasfaserverkabelung
RÄUME	• 150 - 300kg Punktlast, 600 - 1200 kg/m2 • Türbreiten: 1,75m • Türhöhen: 2,00m • Dachhöhe: min. 2,25 bis 3,00m • Antistatische Bodenplatten • Doppelboden

DOM Digital Online Media GmbH
Bismarckstr. 60 • D-50672 Köln

Tel. +49 (0) 221 95168-0 • Fax +49 (0) 221 95168-8
Email : info@dom.de Web : www.dom.de

Bankverbindung: Kreissparkasse Köln • IBAN DE52 3705 0299 0000 3501 32
BIC COKS DE 33 • BLZ 370 502 99 • Kto.-Nr. 350 132

UST.-Ident. Nr. DE 814 416 951 • Amtsgericht Köln HRB 55347
Geschäftsführer: Markus Schulte

Die nachfolgend beschriebenen technisch-organisatorischen Maßnahmen nach DSGVO geben einen Überblick, wie der Betrieb der Server sowie der Datenschutz im Rahmen des DOM Managed Hosting umgesetzt werden. Die spezifische Maßnahmen für die Anwendung bzw. den Serverbetrieb des Kunden werden vorab ermittelt und ggf. angeboten. Die Details werden in einem Vertrag zur Auftragsverarbeitung (AVV) geregelt.

VERTRAULICHKEIT

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen im Rechenzentrum, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Zugangskontrolle gem. EU-Norm Stufe3, EN 50133-1
- Nur autorisiertem und registriertem Personal wird Zutritt gestattet („Prinzip der minimalen Berechtigung“)
- Begleitungen ins DOM-Datacenter müssen vorab angemeldet werden
- Sicherheitsbereiche im DOM-Datacenter sind mit Alarmsystemen ausgestattet
- Protokollierter Zutritt, nur mit Keycard und Finger-Scan
- Fernüberwachung aller Gebäude
- Eingangsbereich ist 24h überwacht, regelmäßige Kontrollbegehungen durch Wachpersonal im DOM-Datacenter
- Regelung für Reinigungspersonal

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Einsatz von Netzwerk- und Host-Firewallsystemen
- Einfache Authentisierung mittels Username/Passwort, in Verbindung mit Passwortrichtlinien
- Gesicherte Übertragungswege im Netzwerk via VPN sowie SSL/TLS >= 1.2 in Verbindung mit Zertifikaten bei Web-Anwendungen (HTTPS)
- Einsatz von Secure Shell (SSH) und ggf. Secure FTP (SFTP) im administrativen Bereich, in Verbindung mit SSH-Keys
- Passwörter werden verschlüsselt gespeichert
- Der Kreis der Personen, die administrativen Zugang haben, ist begrenzt und dokumentiert

Zugriffskontrolle

Maßnahmen, die gewährleisten, 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

- Der Kreis der Personen, die administrativen Zugang haben, ist begrenzt und dokumentiert
- Berechtigungen werden nach Möglichkeit auf das Notwendigste beschränkt
- Administrative Vorgänge auf dem Server werden protokolliert
- externe Datenträgern werden sicher aufbewahrt
- Datenträger werden vor der Wiederverwendung sicher gelöscht
- die Verschlüsselung von Datenträgern erfolgt mittels PGP oder TrueCrypt

Verwendungszweckkontrolle / Trennungsangebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Datengetrennt verarbeitet werden können.

- Logische Mandantentrennung, soweit zutreffend und anwendbar
- Festlegung von Datenbankrechten und Separierung unterschiedlicher Datenarten in getrennten Datenbanken, soweit zutreffend und anwendbar
- Der Kreis der Personen, die administrativen Zugang haben, ist begrenzt und innerhalb eines Berechtigungskonzepts dokumentiert, Mitarbeiter werden entsprechend sensibilisiert
- optional: Speicherung auf gesonderten Systemen oder Datenträgern, auch räumlich entfernt (> 25km)

INTEGRITÄT

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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Nur die erforderlichen Kommunikationsbeziehungen werden freigeschaltet
- Gesicherte Übertragungswege im Netzwerk via VPN sowie SSL/TLS >= 1.2 in Verbindung mit Zertifikaten bei Web-Anwendungen (HTTPS)
- Einsatz von Secure Shell (SSH) und Secure FTP (SFTP) im administrativen Bereich, in Verbindung mit SSH-Keys
- Einsatz von Firewallsystemen
- Verschlüsselung sensibler Daten mittels z.B. PGP oder Truecrypt
- Härtung der Serversysteme
- regelmäßige zeitnahe Software-Updates bei Bekanntwerden von Sicherheitsproblemen
- Verschlüsselung von mobilen Datenträgern und Aufbewahrung im Safe
- Datenschutzgerechte Vernichtung von Datenträgern (DIN 32757)

Eingabekontrolle

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

- Protokollierung der Eingabe, Änderung und Löschung von Daten in der Anwendung, soweit zutreffend und anwendbar
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen, d.h. Vermeidung von Benutzergruppen und generischen Rollen (z.B.„admin“)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts, soweit zutreffend und anwendbar

VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle

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

- Redundante, unterbrechungsfreie Stromversorgung, abgesichert durch USV und Generator, Verfügbarkeit 99,9%
- Redundante Klimaanlage in Serverräumen, Klimakontrolle gemäß ETS 300019 class 3.1 Telecommunications Centers
- Gasfeuerlöschsystem (FM200, Inergen, Lasergesteuertes Rauchfrühwarnsystem
- (VESDA) Feuerschutzwände (F60)
- Regelmäßige Prüfung der Notfalleinrichtungen im DOM-Datacenter
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backupkonzepts, regelmäßige Tests der Datenwiederherstellung
- Optional: Datenspiegelung zu geografisch getrenntem Standort (Köln) möglich

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG

Auftragskontrolle

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

- Weisungen des Auftraggebers werden schriftlich dokumentiert
- Aufträge werden über eine eigene Software verwaltet und dokumentiert

In Bezug auf Auftragnehmer der DOM:

- Weisungen des Auftraggebers werden schriftlich dokumentiert
- Aufträge werden über eine eigene Software verwaltet und dokumentiert

Schulungen

- Alle Mitarbeiter sind speziell auf den Datenschutz verpflichtet und nehmen regelmäßig an Datenschutz-Schulungen teil

Kontrolle der getroffenen Maßnahmen zum Datenschutz

- Halbjährliche Meetings des DOM-Datenschutz-Teams, die laufenden Verarbeitungen sowie die getroffenen Maßnahmen werden überprüft
- Bestellung eins externen Datenschutzbeauftragten