gridscale

Auskunft über technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

Inhaltsverzeichnis

I. Vertraulichkeit (Art. 32 Abs. 1lit. b DSGVO)

Zutrittskontrolle

Die nachfolgende Themen wurden aus Gründen der Sicherheit (von außen nach innen) betrachtet

Der Zugang zum Rechenzentrum ist nur durch einen ständig bewachten Eingangsbereich möglich und nur für Personen die auf einer Zutrittsberechtigungsliste stehen oder angemeldet wurden. Der Serverraum selbst befindet sich in einem Innenbereich und ist durch ein Zugangskontrollsystem vor unbefugtem Zutritt geschützt. Die berechtigten Mitarbeiter können die Tür mit einem PIN-Code in Verbindung mit einer Zutrittskarte öffnen.

Die Berechtigungen werden vom Head of Security" verwaltet/berechtigt und sind im Portal des Rechenzentrums dokumentiert.

Ausreichende Absicherung der Zugänge

Die Zugänge zum Rechenzentrum sind ständig verschlossen und ein Portier sitzt am Haupteingang. Alle Türen zum Gebäude, den Etagen sowie den Räumen auf der Etage und dem Zugang zu unserer Rechenzentrumsfläche sind immer verschlossen, mit einem elektronischen Türschloss gesichert.

Es sind keine Lichtschächte vorhanden, keine Lüftungsöffnungen, keine Fenster, und es gibt keine Feuerleiter.

An beiden Gebäudeenden gibt es ein Feuertreppenhaus.

Alle Türen verfügen über elektrische Türöffner mit Zugangssteuerung.

Bewachung

Das Gelände des Rechenzentrums wird rund um die Uhr bewacht und auch die Pforte des Rechenzentrums ist rund um die Uhr besetzt.

Das Gelände des Rechenzentrums sowie der Innenbereich werden mit Kameras überwacht.

Schriftliche Dokumentation und Anweisungen

Badges die als Schlüssel und müssen am Empfang im Rechenzentrum, nach vorheriger Anmeldung, abgeholt werden und mit denen dann der Zutritt erfolgen kann. Diese Zutrittsberechtigungen werden im Portal des Rechenzentrumsbetreibers dokumentiert und geregelt.

Überwachungseinrichtungen zur Sicherstellung der Zutrittskontrolle für kritische Sicherheitsbereiche, wie z.B. für Serverräume.

Der Zugang wird manuell durch den Pförtner am Eingang kontrolliert und durch Videoüberwachung. Der Serverraum ist mit einem Zahlencode gesichert, in Verbindung mit dem "Badge". Nach drei fehlerhaften Eingaben wird der Zugang für 15 Min. gesperrt.

Es gibt eine Videoüberwachung aller Gängen, in jedem Gebäude und im gesamten Rechenzentrum.

Kriterien für die Zugangsberechtigung

Es gibt ein Besucherbuch am Haupteingang zur Aufnahme der Besucherdaten und Ausstellung eines Besucherausweises von autorisierten Personen.

Es besteht eine Trennung von Bearbeitungs- und Publikumszonen. Besucher melden sich am Haupteingang an, um einen Besucherausweis zu erhalten, bevor sie das Rechenzentrum betreten dürfen.

Besucher müssen über das Portal des RZ-Betreibers vorher angemeldet werden. Diese melden sich dann am Haupteingang, um einen Besucherausweis zu erhalten, gegen Vorlage eines Ausweisdokuments, bevor sie das Rechenzentrum betreten dürfen. Besucherberechtigungen müssen vorher von autorisierten Personen vergeben werden.

Sicherheitsbetrachung der Arbeitsplätze

Es besteht eine schriftliche Anweisung (Policy) für mobiles Arbeiten. Wir haben keine BYOD Geräte.

Dokumentation der Zutritte

Der Zugang für Reinigungspersonal muss auf dem Portal des RZ-Betreibers beantragt/berechtigt werden.

Ebenso muss der Zugang für Wartungspersonal auf dem Portal des RZ-Betreibers beantragt/berechtigt werden.

Der Zugang für Security-Begleitung muss ebenfalls auf dem Portal des RZ-Betreibers beantragt/berechtigt werden.

Zugangskontrolle

Benutzeridentifikation und Passwortverfahren sind festgelegt

Keine Eigennamen und Wörter aus dem Wörterbuch, Sonderzeichen müssen verwenden werden, die minimale Passwortlänge ist vierzehn Stellen oder mehr.

Die Passwort Richtline ist in der gridscale Informationssicherheitsrichtline dokumentiert.

Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

Das Auto-Logout (ähnlich wie Bildschirmsperre) ist automatisiert auf allen Servern ausgerollt.

Eine Sperrung des Zugangs bei mehr als drei Anmeldefehlversuchen, ist entweder Standard oder sonst technisch nicht möglich. Es gibt im gesamten Unternehmen eine “Clean Desk Policy”.

Einrichtung eines Benutzerstammsatzes pro User

Die Weitergabe von Passwörtern ist verboten

Verschlüsselung von Datenträgern

Zugriffskontrolle

Schutz gegen unberechtigte interne und externe Zugriffe

Alle Server sind technisch hinter mehreren, redundanten Firewalls, positioniert.

Das Standard-Sicherheitskonzept von Linux ist so gebaut dass kein Virenscanner notwendig ist. Regelmäßige Pachtes sorgen außerdem dafür, dass Viren keine Möglichkeit haben, weil die Software stets aktuell ist.

Bei Windows Systemen wird die Microsoft Lösung verwendet. Alle Dokumente liegen entweder in Cloudbasierten Lösungen oder werden entsprechend gesichert, um ggf. eine Wiederherstellung zu ermöglichen.

Verschlüsselung zum Schutz gegen unberechtigte interne und externe Zugriffe

Berechtigungskonzept für Zugriffsrechte

Für Anwender und für Administratoren, gibt es eine zentrale Instanz für die Berechtigungsvergabe basierend auf einem Rollenmodell.

Regelungen zur Überwachung und Protokollierung

Zugriffe bzw. Zugriffsversuche werden protokolliert.

Die Auswertung der Protokolle erfolgt durch automatisierte Auswertung und Benachrichtigung.

Die Aufbewahrungsdauer der Protokolle beträgt zwischen 3 - 12 Monate, abhängig vom jeweiligen System.

Schriftliche Dokumentation von Datenträgern

Die Art und Anzahl von Datenträgern sind dokumentiert.

Datenträger werden in einem Stahlschrank vor Ort im Rechenzentrum in einem verschlossenen Raum gelagert.

Datenträgerverwaltung

Es gibt einen Nachweis über den ein- und Ausgang von Datenträgern und ein Bestandsverzeichnis sowie eine regelmäßige Datenträgerinventur.

Regelung zum Umgang mit Datenträgern

Der Bereich, in dem sich Datenträger befinden dürfen, ist definiert.

Die Personen, die Datenträger befugt entnehmen dürfen ist festgelegt.

Regelung zur Datenträgernutzung

Der Einsatz externer Speichermedien ist untersagt.

Der Umgang mit Datenträgern ist geregelt

Die Lagerung von veralteten bzw. zu vernichtenden Datenträgern sowie deren Zerstörung ist in einem Prozess definiert.

Die Zerstörung erfolgt durch einen zertifizierten Anbieter.

Das Entsorgungsunternehmen ist zertifiziert.

Pseudonymisierung

Pseudonymisierung personenbezogener Daten „Pseudonymisierung“ wird in Art. 4 Nr. 5 DS-GVO definiert als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“

Diese Daten werden getrennt zu den Pseudonymen aufbewahrt.

Durch technische und organisatorische Maßnahmen wird eine Nichtzuordnung gewährleistet. Nach einer Kündigung wird das Benutzerkonto sofort unwiderruflich gelöscht und direkt aus der Datenbank entfernt, sofern keine gesetzliche Aufbewahrungsfristen bestehen.

Der Löschungsnachweis wird für 90 Tage aufbewahrt und nach 90 Tagen wird auch der Löschungsnachweis dauerhaft gelöscht.

Für die De-Pseudonymisierung ist ein eigenständiges Rechte- und Rollenkonzept vorhanden.

Trennungsgebot

Umsetzung des Trennungsgebots

Test- und Entwicklungsumgebungen, wie auch die Betriebsumgebung, sind voneinander getrennt. Ein direkter Datenaustausch zwischen den einzelnen Umgebungen findet nicht statt. Die Arten der Testumgebungen sind von Testlauf und Testart abhängig und reichen von Unittests in automatisiert bereitgestellten Testcontainern bis zu einem Hardware-Staging in welchem Integrationstests einzelner Komponenten vorgenommen werden. Die Prozesse wurden entsprechend dokumentiert.

Regelung der Trennung

Die Trennung erfolgt durch eine physische Lösung durch, getrennte Server Hardware und durch eine virtualisierte Lösung mit VLAN/Switchen.

Mandatentrennung auf den Systemen

Zur Sicherstellung der datenschutzkonformen Mandantenfähigkeit, wird eine Virtualisierung der einzelnen Kunden Maschinen genutzt (Kernel Based Virtual Machine) und es wird eine Virtualisierung Software eingesetzt. Dadurch wird eine Separierung der einzelnen virtuellen Maschinen erreicht, die auch eine ungewollte Interaktion der VM’s untereinander verhindert und damit isoliert.

Zur Gewährleistung der datenschutzkonformen Zweckbindung, werden Daten gem. Verarbeitungsverzeichnis verarbeitet und dokumentiert.

Sicherstellung der Datenschutzkonformität

Die Verarbeitung ist durch eine Software-, eine Hardware- und eine Virtualisierungsschicht vollständig voneinander getrennt.

II. Integrität (Art. 32 Abs. 1lit. b DSGVO)

Weitergabekontrolle

Übermittlung

Erfolgt per Datenleitung durch VPN und HTTPS.

Datenschutzkonformität

Durch eine sichere Versendungsform mit VPN (Virtual Private Network).

Eingabekontrolle

Datenschutzkonforme Eingabekontrolle

Wird in Protokollierungs- und Protokollauswertungssysteme erfasst: im jeweiligen Log-File erfasst, aber nicht ausgewertet.

Die Aufbewahrungsdauer der Protokolle werden gemäß der Rechtsgrundlage und dem legitimen Zweck für die Verarbeitung aufbewahrt und entsprechend gelöscht.

III. Verfügbarkeit und Belastbarkeit - von Systemen und Diensten (Art. 32 Abs. 1lit. b DSGVO)

Verfügbarkeit und Belastbarkeit

Überwachung aller ausfallkritischen Infrastruktursysteme des Rechenzentrums

Brandschutzeinrichtungen und Überwachung mit automatischer, digitaler Brandmeldeanlage. F-90-Brandbekämpfungsabschnitte und Brandschutzwände der Feuerwiderstandsklasse F 90.

Feuerlöscher sind in jedem Raum vorhanden.

Rauchmelder, Brandfrühesterkennungssysteme (Rauchansaugsystem – RAS), die in eine Brandmeldeanlage eingebunden sind, gewährleisten die frühestmögliche Detektion.

Brandmelder mit automatischer Überwachung und digitaler Brandmeldeanlage.

Die Brandbekämpfung erfolgt durch eine automatisch angesteuerte Feuerlöschanlage.

Hochwasserschutzeinrichtungen sind für den Serverraum nicht erforderlich, der Serverraum befindet sich im 1. OG.

Im gesamten Rechenzentrum gibt es ein Rauchverbot.

Redundante Stromversorungseinrichtungen sind mit separaten USV-Systemen (A- und B-Versorgung) vorhanden.

Notstromgenerator sind durch redundant ausgelegte Netzersatzanlagen, mit Dieselgeneratoren gelöst.

Unterbrechungsfreie Stromversorgung (USV) durch separate USV-Systeme (A- und B-Versorgung).

Die Festplatten sind durch ein RAID-System abgesichert.

Konzept zum regelmäßigen Backup

Sicherungsdatenträger werden getrennt aufbewahrt beziehungsweise die Aufbewahrung der Datensicherung erfolgt in einem anderen geografischen Standort.

Datensicherungen werden, wo notwendig, als Tagessicherungen, Monatssicherungen oder Jahressicherungen, nach einem dokumentierten Backup Verfahren, automatisiert durchgeführt.

Die Belastbarkeit der Systeme und Dienste wird regelmäßig überprüft bzw. getestet.

Als belastbar werden IT-Systeme bezeichnet, sofern diese ausreichend widerstandsfähig sind, um auch trotz Störungen und Fehlern bei hoher Belastung (z.B. bei DDoS–Attacken) funktionsfähig zu bleiben und, mit Blick auf die Verarbeitung personenbezogener Daten, die Sicherheit garantiert werden kann. In diesem Sinne meint, Belastbarkeit Robustheit.

Konzept für regelmäßigen Sicherheits-Updates

Updates werden, abhängig vom System, wöchentlich, monatlich oder wenn erforderlich umgehend, installiert.

IV. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Rasche Wiederherstellbarkeit

Checkliste zur Prüfung des Notfallkonzepts

Auf der Basis einer Risikoanalyse wurde ein Sicherheitskonzept für möglicherweise auftretenden Störungen wie z.B. technische Defekte, Brand, Sabotage, Naturgewalten, etc., entwickelt.

Diese Konzept wird laufend (mindestens jährlich) an die veränderten Gegebenheiten angepasst. Es wurde ein entsprechender Audit-Plan erstellt, der mind. ein Mal im Jahr eine Überprüfung des Dokuments vorsieht.

Erkannte Schwachstellen werden beseitigt. Es ist eine Notstromversorgung vorhanden und es wurde ein Überspannungsschutz installiert.

Es ist dokumentiert, welcher Bedarf an Hardware für den Notfall besteht. Jede Hardware ist redundant ausgelegt und wurde genau zu diesem Zweck angeschafft und implementiert.

Es erfolgt eine Spiegelung der wichtigsten Dateien auf ein anderes Speichermedium.

Die Verfügbarkeit der zu alarmierenden eigenen Mitarbeiter (z.B. Systemverantwortliche, Operating, RZ-Leiter, Datenbankadministrator etc.) ist gewährleistet.

Die erforderlichen Systempasswörter wurden an einer sicheren Stelle hinterlegt.

Die Verfügbarkeit von Wartungstechnikern und Hardwareersatzteilen wurde durch den Abschluss eines Wartungsvertrags mit dem Hersteller geregelt. Der Ausfall von einer Komponente hat keinen Ausfall der Dienstleistung für die Kunden zur Folge. Der Dienst ist Herstellerunabhängig.

Es besteht eine mehrfache Redundanz für die Datenleitungen.

Der Bedarf der nötigsten Peripheriegeräte (Bildschirme etc.) wurde geregelt.

Es wurde ein Archiv für die Auslagerung von Sicherungsdatenträgern eingerichtet.

Die Verfügbarkeit dieser Datenträger ist im Notfall gewährleistet.

Es kann mit der Aufnahme eines Notbetriebs der wichtigsten Dienste (gemäß der vorher festgelegten Prioritätenliste) bzw. der vollen Datenverarbeitung innerhalb eines vertretbaren Zeitraums wieder begonnen werden.

Es existiert eine dokumentierte Beschreibung der Wiederanlaufmaßnahmen und Prozesse.

Die erforderlichen Maßnahmen sind den betroffenen Personen bekannt.

Entsprechende Maßnahmen werden regelmäßig (mindestens halbjährlich) überprüft und getestet.

Die oben genannte Prüfpunkte sind schriftlich dokumentiert.

V. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Überprüfung der technischen und organisatorischen Maßnahmen

Rechenschaftspflicht (Art. 5 Abs. 2 EU-DSGVO)

Aufbauorganisation

Es ist eine Datenschutzleitline im Unternehmen vorhanden und den Mitarbeitern bekannt gemacht.

Ein Datenschutzbeauftragter ist bestellt und der Aufsichtsbehörde gemeldet.

Meldebestätigung des DSB war der 01.11.2021.

Die Aufgaben des Datenschutzbeauftragten sind definiert.

Der Datenschutzbeauftragte unterstützt beratend die Geschäftsführung und die Abteilungen.

Ausserdem ist er für die Schulung und Kontrolle der Mitarbeiter zum Datenschutz verantwortlich. Es wird beim On-Boarding eine DSGVO / GDPR Schulung durchgeführt und es gibt jährlich mehrere Schulungen zur Auffrischung und Weiterbildung.

Audits und Kontrollen werden im Rahmen des Auditplans durchgeführt und dokumentiert. Das jährliche ISO Audits wird durch eine externe Zertifizierungsstelle durchgeführt, dokumentiert und bewertet.

Die Beantwortung / Klärung von Datenschutzbeschwerden werden organisatorisch an das Management eskaliert bzw. zum Datenschutzbeauftragten.

Die Anfrage von Betroffenen werden entweder an compliance@gridscale.io gestellt oder organisatorisch an das Management eskaliert bzw. zum Datenschutzbeauftragten weitergeleitet. Zur Beantwortung solcher Anfragen wurden entsprechende Templates erstellt.

Die Meldung von Datenschutzverletzungen (Art. 33/34 DS-GVO), wird durch eine "Data Breach Procedure" (SOP-60) gesteuert und durchgeführt.

Ein einheitliches Datenschutzkonzept ist für alle Standorte vorhanden.

Es wurde ein Konzept für die Aufgaben und die Schulungen zum Datenschutz erstellt. Alle Mitarbeiter erhalten mehrmals jährlich ein Auffrischungstraining zum Datenschutz und der Datensicherheit.

Eine Regelung für Interne Kontrollen wurde definiert und wird im Rahmen der ISO 27001 / 27018 regelmäßig auditiert und überprüft gem. Auditplan.

Der Umgang mit Datenschutzberichten wurde geregelt und umgesetzt. Der Datenschutzbericht wird einmal jährlich veröffentlicht und dem Management zur Verfügung gestellt.

Eine Regelung für die Zusammenarbeit zwischen den Abteilungen und dem DSB wurde implementiert. Das Management ist sich der Notwendigkeit, der Implementierung der DSGVO Anforderungen, z.B. in Programmen, der Datensparsamkeit, security by design etc. bewusst und zieht ggf. den DSB hinzu. Ausserdem sorgt die Sales Abteilung für die Erfüllung entsprechender, vertraglicher Anforderungen wie z.B. AVV, TOMs etc. mit dem Kunden. Dies wird z.B. in regelmäßigen Trainings und Informationsschulungen vertieft.

Basis-Anforderungen:

Ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) ist erstellt und gepflegt.

Ein einheitliches Risikomodell wurde umgesetzt.

Eine datenschutzkonforme Verarbeitung wurde umgesetzt.

Der Umgang mit Betroffenenrechten ist geregelt.

Der Umgang mit Datenschutzverletzungen ist definiert.

Der Einsatz von Unterauftragnehmern und fremden Fachleistungen sind dokumentiert.

Ist ein Auftragnehmer als Auftragsverarbeiter nach Art. 28 DS-GVO tätig, verarbeitet der Auftragnehmer personenbezogene Daten nur entsprechend den vertraglichen Vorgaben des Auftraggebers.

Bei zusätzlichen Aufträgen z.B. „Remote Hands“, die die Verarbeitung oder den physischen Zugriff auf Datenträger von personenbezogenen Daten beinhalten oder nicht ausschließen können, werden ggf. gesonderte Verträge gemäß DS-GVO Art. 28 abgeschlossen oder bestehende Verträge ergänzt.

Mit Subunternehmern werden, sofern erforderlich, datenschutzkonforme Verträge nach DS-GVO Art. 28 geschlossen. Die Auswahl von Dienstleistern erfolgt sorgfältig.

gridscale GmbH