Stand: 26.07.2021

Dokumentation der technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 DSGVO

zur exone.Cloud der EXTRA Computer GmbH, Brühlstrasse 12, 89537 Giengen-Sachsenhausen

1. Gewährleistung der Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1. Zutrittskontrolle

Der Zutritt zum Rechenzentrum ist nur einem eingeschränkten Kreis von autorisierten Personen möglich.

1.1.1. Organisatorische Maßnahmen:

Das Rechenzentrumsgebäude ist von außen neutral und nicht als Rechenzentrum erkenntlich. Der genaue Standort des Rechenzentrums ist nicht öffentlich bekannt. Externe Personen ohne besondere Sicherheitsfreigabe erhalten nur Zutritt in ständiger Begleitung eines internen Mitarbeiters, der durch seine Zutrittskarte entsprechende Berechtigungen in die jeweiligen Bereiche erhält. Jeder Zutritt wird in dem RZ-Logbuch festgehalten. Sollten Personen das Rechenzentrum betreten, die in Begleitung einer zutrittsberechtigten Person Zugang zum Rechenzentrum erhalten, so sind diese gesondert im Logbuch festzuhalten und vorher anzumelden. Die Identifizierung der Personen ist vorab durch einen gültigen amtlichen Lichtbildausweis festzustellen. Durch das installierte Zutrittskontrollsystem können nur Personen n das Rechenzentrum, die im Vorfeld entsprechende Berechtigungen erhalten haben. Die Zutrittsberechtigungen werden in einem zentralen System eingerichtet und verwaltet. Hierfür existiert ein formaler Genehmigungsprozess. Der Zutritt zum Rechenzentrum erfolgt über einen neutralen Transponder in Form einer Zutrittskarte oder einem Schlüsselanhänger, der eine Zuordnung zur Funktion nicht verdeutlicht. Der Transponder ist mithilfe einer AES256 Verschlüsselung gegen Kopieren geschützt. Die Vergabe der Zutrittskarten/-anhänger wird dokumentiert. Bei Verlust des Zutrittsmediums wird dieses sofort über das Zentrale System gesperrt. Die Berechtigungen können unabhängig davon, wo sich der Transponder befindet, geändert, gelöscht oder gesperrt werden.

1.1.2. Technische Maßnahmen:

Das Rechenzentrum wird durch folgende technische Maßnahmen vor unberechtigtem Zutritt geschützt:

- Zutrittskontrollsystem
- Einbruchmeldeanlage
- Videokameras
- Sicherheitstüren

Der Standort des Rechenzentrums verfügt über Zugangsleser an allen Außen- und sicherheitsrelevanten Türen. Alle Zugänge sind videoüberwacht; die Videoüberwachung wird durch eine zentrale Anlage gesteuert. Die Aufzeichnungen werden über einen Zeitraum von 6 Monaten gespeichert. Zutritt erfolgt je nach Sicherheitsklassifizierung am Zugangsleser über eine zwei Faktor oder drei Faktor Authentifizierung (Transponder mit PIN oder Transponder mit wechselnder PIN alle 60 Sekunden). Beim Verlassen der letzten anwesenden Person wird die Einbruchmeldeanlage automatisch scharf geschaltet. Die Videoüberwachungsanlage setzt moderne Analysemethoden (wie z.B. Gesichtserkennung, verdächtiges Verhalten, … ein), um entsprechend proaktiv Alarme auslösen zu können.

1.2. Zugangskontrolle

Folgende technische und organisatorische Maßnahmen zur Benutzeridentifikation und Authentifizierung sind vorhanden:

Aufgrund des im Unternehmen geltenden Berechtigungskonzeptes wurde ein formaler Prozess eingerichtet. Ausschließlich auf der Grundlage dieses Prozesses werden Zugänge zum Datenverarbeitungssystem eingeräumt. Berechtigungen werden bei Verlassen des Unternehmens gesperrt. Gleiches gilt, sobald die Berechtigung nicht mehr benötigt wird bzw. bei missbräuchlicher und unberechtigter Verwendung. Die Zugangsberechtigungen sind so konfiguriert, dass Personen lediglich in den vorher definierten Bereichen Zugang zur Datenverarbeitung haben; Benutzerrechte werden eindeutig zugeordnet. Jeder Fernzugriff auf interne Systeme ist nur in authentifizierter Form möglich.

Im Einzelnen wurden folgende Maßnahmen getroffen:

- Einrichten einer formalen Benutzerverwaltung

- Nur bei uns registrierte Kunden erhalten einen Benutzerzugriff

- Einsatz eines Virtuellen privaten Netzwerkes (VPN)

- Verschlüsselungstechnik bei schutzbedürftigen Daten entsprechend dem aktuellen Stand der Technik

- Protokollierung der Besucher des Rechenzentrums

- Sorgfältige Auswahl des Reinigungspersonals

1.3. Zugriffskontrolle

Es wird gewährleistet, dass ein Zugriff ausschließlich auf die der Zugriffsberechtigung unterliegenden Daten erfolgt und dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten nach ihrer Speicherung stattfindet.

Die Zugriffsbefugnisse werden entsprechend dem Berechtigungskonzept erstellt und kontrolliert.

Der Zugreifende wird identifiziert. Zugriffe auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung der Daten) sowie Missbrauchsversuche werden protokolliert. Die Protokolle werden regelmäßig ausgewertet. Für die Protokollierung steht ein zentraler Server zur Verfügung, auf den lediglich autorisierte Administratoren lesenden Zugriff erhalten. Auffällige Zugriffsversuche lösen einen Alarm aus, der an die verantwortliche Stelle gesendet wird.

Passwörter werden nach aktuellem Stand der Technik und des Sicherheitsstandards generisch erzwungen.

Ist eine Änderung der Zugriffsberechtigung erforderlich, wird diese ausschließlich von hierfür bestimmten Administratoren vorgenommen. Dabei wird nach dem Mehraugenprinzip verfahren, so dass jeweils Rücksprache mit einer weiteren zuständigen Person (ggf. einem Vorgesetzten) erfolgt.

Lediglich ausgewählte Mitarbeiter erhalten administrative Rechte, die für einzelne Netzbereiche zugewiesen werden. Die entsprechende Beschränkung des Zugriffs wird durch die Konfiguration des Systems erzwungen. Benutzerberechtigungen, deren Grundlage entfallen ist, werden umgehend gelöscht; dies erfolgt auch automatisiert im Rahmen der Systemdiagnose.

Datenträger werden sicher aufbewahrt und vor ihrer Wiederverwendung physisch gelöscht. Eine ordnungsgemäße Vernichtung nicht mehr benötigter Datenträger ist gesichert, die verantwortlichen Personen werden jeweils eingewiesen. Die Vernichtung wird protokolliert.

1.4. Trennungskontrolle

Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Mandantentrennung wird softwareseitig durchgeführt; auch die Zugriffsregelung gewährleistet die erforderliche Trennung. Test- und Routineprogramme werden getrennt; Gleiches gilt für Test- und Produktivdaten; durch Netzwerksegmentierung werden Entwicklungssysteme technisch getrennt Dateiseparierung ist vorhanden; Kopien von Produktivdaten werden nicht zu Testzwecken verwendet.

2. Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Es wird gewährleistet, dass die Weitergabe personenbezogener Daten durch Einrichtungen der Datenübertragung überprüft- und nachvollziehbar ist und der Zugriff Unbefugter auf dem Transportweg verhindert wird. Hierzu wird eine Übersicht angelegt, die erkennen lässt, an welchen Stellen, während welcher Zeitspannen, welche personenbezogenen Daten durch Übertragungseinrichtungen übermittelt werden. Diese Übersicht wird ständig aktualisiert. Dokumentiert werden auch die Abruf- und Übermittlungsprogramme, die Übermittlungswege (soweit das Übermittlungsverfahren dies zulässt) und -stellen sowie die entsprechende Übermittlungs-Hardware. Es erfolgt eine Protokollierung der Abruf- und Übermittlungsaktivitäten.

Daten werden generell nur auf eigenen Systemen innerhalb Deutschlands gespeichert.

Grundsätzlich können auf die Systeme, die personenbezogene Daten verarbeiten, nur autorisierte Nutzer zugreifen. Alle personenbezogenen Daten werden in kennwortgeschützten Datenbanken gespeichert.

Verlassen die Daten beim Transport über Dateitransfer das separierte Netz des Rechenzentrums, werden zusätzlich SSL/TLS-, IPSec oder VPN-Verbindungen verwendet. Ausgenommen hiervon ist die Korrespondenz per E-Mail zur Auftragsbearbeitung, die unverschlüsselt stattfindet.

Der Zugriffsschutz auf Systeme mit sensiblen Informationen wird auf mehreren Ebenen realisiert: Auf Dateisystem-, auf Betriebssystem- und auf Netzwerkebene.

Der Zugriff und die Aktivitäten der Administratoren werden in speziellen Protokolldateien aufgezeichnet.

Die Protokollierung der Zugriffe erfolgt auf einem zentralen, dedizierten Protokollierungsserver, der von den zu protokollierenden Systemen getrennt installiert ist.

2.2. Eingabekontrolle

Der Auftragnehmer ist in der Lage, nachträglich festzustellen und zu überprüfen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Details zur Protokollierung wurden unter Ziff. 4.1 beschrieben. Es existieren Datenerfassungsanweisungen. Die Berechtigungen zur Eingabe, Änderung und Löschung von Daten sind dokumentiert. Protokollauswertungen werden regelmäßig von den Systemadministratoren vorgenommen, dabei wird ein festgelegtes Auswertungsverfahren für die automatisiert erstellten Protokolldaten angewandt.

2.3. Auftragskontrolle

Mitarbeiter der EXTRA Computer GmbH werden ausschließlich auf Anweisung der Vorgesetzten im Rahmen der Auftragsverarbeitung tätig. Ein Datenschutzbeauftragter ist bestellt. Die Weisungen des Auftraggebers (Resellers) sind ferner in der Auftragsvereinbarung mit der EXTRA Computer GmbH schriftlich niedergelegt; diese Vereinbarung enthält auch die Einzelheiten der Auftragskontrolle.

2.4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. Die getroffenen technischen Maßnahmen ermöglichen den Betroffenen eine einfache Ausübung des Widerrufsrechts.

3. Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO)

Zum Schutz gegen die zufällige Zerstörung oder den Verlust von Daten werden Firewalls sowie ein Virenschutz installiert, der Hackerangriffe abwehrt.

Alle sensiblen und kritischen Systeme sind mit einem fehlertoleranten Festplattenverbund (i.d.R. RAID5 oder höher) ausgestattet. Zusätzlich ist jedes Rack mit mindestens drei unabhängigen Phasen angebunden. Jedes kritische System besitzt redundante Netzteile zur Stromversorgung. Die Stromversorgung wird durch USV und Netzersatzanlagen (Dieselgenerator) gesichert. Die Daten werden täglich gesichert. Ein Backup- und Recoverykonzept wurde erstellt.

Die Verantwortlichkeit im Falle eines Notfalls wurde festgelegt und kommuniziert. Die schriftlichen Anleitungen für den Notfall bestimmen die erforderlichen Abläufe im Einzelnen (insbesondere die Informationswege und die Weiterleitung des Alarms an die zuständigen Stellen sowie die im Notfall zwingend vorgesehenen Handlungsschritte).

Um einen Brandfall im Vorfeld zu verhindern, werden kritische Bereiche mit einer Brandfrüherkennungsanlage überwacht; Feuerlöschgeräte sind vorhanden. Die Serverräume enthalten die zur Messung von Temperatur und Feuchtigkeit erforderlichen Geräte.

4. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die Verantwortlichkeit im Falle eines Notfalls wurde festgelegt und kommuniziert.

Als eingetragener Anbieter bei der Bundesnetzagentur werden alle Vorgaben von der Regulierungsbehörde erfüllt und eingehalten. Die schriftlichen Anleitungen für den Notfall bestimmen die erforderlichen Abläufe im Einzelnen (insbesondere die Informationswege und die Weiterleitung des Alarms an die zuständigen Stellen sowie die im Notfall zwingend vorgesehenen Handlungsschritte). Die Vorgehensweise zum Umgang mit Sicherheitsvorfällen ist dokumentiert. Es gibt einen formalen Prozess, der die Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen festlegt.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO

Ein Datenschutzmanagement wurde eingerichtet.

Durch interne Audits findet regelmäßig eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung statt.

6. Pseudonymisierung (Art. 32 Abs. 1 lit. a, Art. 25 Abs. 1 DSGVO)

6.1. Technische Maßnahmen:

Im Fall der Pseudonymisierung findet die Trennung der Zuordnungsdaten und die Aufbewahrung in einem getrennten, abgesicherten System (verschlüsselt) statt.

6.2. Organisatorische Maßnahmen

Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf einer gesetzlichen Löschfrist zu anonymisieren / pseudonymisieren

7. Verschlüsselung (Art. 32 Abs. 1 lit. b DSGVO)

7.1. Technische Maßnahmen:

- Sensible personenbezogene Daten werden verschlüsselt übertragen - Externer Zugang nur über sichere Verschlüsselte Verbindung möglich (VPN oder vergleichbar) - Verschlüsselte Speicherung von User-Passwörter - Verschlüsseltes Wlan nach aktuellem Standard - Verschlüsselung mobiler Datenträger (z.B. Notebooks, Smartphones, usw.) - Verschlüsselung sensibler Daten