Auftragsverarbeitungsbestimmungen

Technische und organisatorische Maßnahmen nach Artikel 32 EU-DSG

Autor: Dirk Pessarra

Version: 1.3

Datum: 12.05.2023

Einleitung

Die neomatt GmbH, im Folgenden “neomatt” verarbeitet personenbezogene Daten im Auftrag und trifft die folgenden technischen und organisatorische Maßnahmen im Sinne des Artikel 32 EU-DSGVO.

neomatt bietet Software-as-a-Service (SaaS) Leistungen und Dienstleistungen an. Durch die Nutzung der Leistungen werden Daten der Auftraggeber und Nutzer der Services gespeichert, um die beste Bereitstellung der Services zu ermöglichen. Der Auftraggeber selbst sorgt dafür, seine vor der Verarbeitung eingegebenen Daten zu speichern. Die neomatt erstellt täglich Datensicherungen der verarbeiteten Daten. Dies garantiert eine Wiederherstellung der verarbeiteten Daten. Eine Herstellung in jedem Fall und in vollem Umfang kann aus technischen Gründen leider nicht zu 100% garantiert werden.

Die neomatt nutzt Server die bei Folgendem Anbieter in einem Rechenzentrum stehen:

myLoc - WIIT AG

Joachim-Erwin-Platz 3

40212 Düsseldorf

Die Angaben beziehen sich dabei auf die Verarbeitung unter Verwendung der Server bei diesem Hosting-Anbieter.

1 Vertraulichkeit

1.1 Zutrittskontrolle

Ziel: Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

- Videoüberwachung der Ein- und Ausgänge zu den Büroflächen und umfassende Überwachung der Rechenzentren
- Elektronisches Zutrittskontrollsystem mit digitaler Protokollierung
- Personalisierte individuelle Vergabe der zur auszuführenden Tätigkeit notwendigen Zutrittsberechtigungen für Mitarbeiter, Dienstleistern, Kunden und Besucher durch leitende Angestellte
- Zentrale Einbruchmeldeanlage je Standort

- Sicherheitstüren F90 oder höher in den Rechenzentren
- Mehrere Sicherheitszonen und mehrstufiges Zutrittssystem (Gelände, Gebäude, Raum, Cage/Modul/Rack)

Ergänzende Maßnahmen am Standort Am Gatherhof 44, 40472 Düsseldorf:

- 24/7 Besetzung durch eigenes technisches Personal

Ergänzende Maßnahmen am Standort In der Steele 2, 40599 Düsseldorf:

- 24/7 Überwachung durch eigenes technisches Personal am Hauptstandort
- Besetzung mit eigenem technischen Personal während der Geschäftszeiten

1.2 Zugangskontrolle

Ziel: Zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen:

- Bei durch die neomatt konfigurierten Passwörtern gilt die Passwortrichtlinie der neomatt (>= 6 Zeichen, Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen). Grundsätzlich wird nach Übertragung eines Passwortes an den Auftraggeber wird dieser aufgefordert ein neues Passwort zu vergeben.
- Alleinige Entscheidung über Zuteilung von Zugangsberechtigungen durch den Auftraggeber.
- Zugang besteht nur durch ausgewählte und autorisierte technische Mitarbeiter der neomatt

1.3 Zugriffskontrolle

Ziel: Zu 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.

Maßnahmen:

- Nach Beendigung des Vertrags ermöglicht neomatt eine Löschung oder Anonymisierung der Daten nach aktuellem Stand der Technik sicher.
- Neomatt ermöglicht nur Mitarbeitern den Zugriff auf die Daten, wenn der Mitarbeiter diesen Zugriff zur Erfüllung der Leistungen für den Auftraggeber benötigt.

1.4 Trennungskontrolle

Ziel: Zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen:

- Es erfolgt eine logische oder physikalische Trennung der verschiedenen Mandantenumgebungen durch neomatt.

2 Integrität

2.1 Weitergabekontrolle

Ziel: Zu 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.

Maßnahmen:

- Datenschutzkonforme Löschung , Anonymisierung oder Zugangssperrung von Daten
- Der Auftraggeber verantwortet die verschlüsselte Übertragung jeglicher Daten und stellt durch geeignete Maßnahmen deren Integrität sicher.
- Wenn ein Zugriff auf die Daten des Auftraggebers durch die neomatt notwendig ist, erfolgt dieser nach Abstimmung über das Firmennetzwerk der neomatt.
- Externen Zugriff auf das Firmennetzwerk der neomatt ist nur über verschlüsselte VPN-Verbindungen möglich.

2.2 Eingabekontrolle

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

Maßnahmen:

- Der Auftraggeber erfasst in der Regel personenbezogene Daten selbst.
- Erfasst oder ändert neomatt personenbezogene Daten geschieht dies ausschließlich auf explizite Anweisung durch den Auftraggeber und diese Änderungen werden geeignet protokolliert.

3 Verfügbarkeit und Belastbarkeit

Ziel: Zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

- Monitoring aller relevanten Infrastrukturkomponenten (Strom, Klimatisierung, Netzwerk, Sicherheit, Backup)
- Backup- und Recovery-Konzept für alle kritischen Infrastrukturkomponenten
- Eigene Trafostationen mit mehrseitigem Anschluss an den örtlichen 10 KV Ring
- Einsatz von Systemen zur unterbrechungsfreien Stromversorgung (USV)
- Einsatz von Netzersatzanlagen zur längerfristigen Überbrückung von Netzausfällen (NEA)
- Notbetankungskonzept zur Sicherstellung eines kontinuierlichen NEA Betriebs
- Sofern vereinbart Bereitstellung mehrerer unabhängiger Stromversorgungen in Abstufungen (verschiedene Stromkreise, verschiedene USV und NEA).
- Einsatz von aktuellen Virenscannern, Firewalls, Verschlüsselungs- und Signierungssoftware sowie Spam-Filter im Firmennetzwerk der neomatt Maßnahmen Colocation, Managed Hosting und Cloud Services:
- Klimatisierung der Serverräume, sofern vereinbart redundant
- Brandmeldeanlage mit Früherkennungssystem sowie Argon oder Inerten
- Löschanlage mit Aufschaltung bei der örtlichen Feuerwehr
- Infrastruktur Überwachung durch mehrere unabhängige Überwachungsdienstleister
- Belüftungs- und Klimatisierungskonzept der Rechenzentren

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Kontrolle

4.1 Datenschutz Management

Maßnahmen:

- Es erfolgt eine regelmäßige Unterweisung der Mitarbeiter in Bezug auf Datenschutz gemäß aktuellen gesetzlichen Vorgaben.
- Ein Vertrag zur Auftragsdatenverarbeitung zwischen der neomatt und dem Server-Hosting Unternehmen ist geschlossen