Technische und organisatorische Maßnahmen

Datensicherheitskonzept der Omikron Data Quality GmbH (V5.3)

1. Einleitung

Diese Dokumentation dient der Übersicht der vorgehaltenen organisatorischen und technischen Maßnahmen bei der Omikron Data Quality GmbH am Standort Pforzheim (im Folgenden „Omikron“ genannt) in der Auftragsverarbeitung.

Bei der Niederlassung Berlin handelt es sich um einen Entwicklerstandort. Die Sicherheitsmaßnahmen sind bis auf die folgenden Unterschiede dieselben:

- In Berlin sind die Türen ebenfalls verschlossen und mit einem starren Türknauf versehen, jedoch nicht durch ein elektronisches Zugangssystem, sondern durch mechanische Schlösser gesichert.
- Die Räumlichkeiten sind nicht durch eine Alarmanlage gesichert

2. Zutrittskontrolle

Die Zutrittskontrolle verwehrt Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Daten erhoben, verarbeitet und genutzt werden.

Die Türen zu den Geschäftsräumen von Omikron sind mit Sicherheitsschlössern, starrem Türknauf und einem automatischen Zuzieher versehen. Der Zugang zu den Geschäftsräumen wird über ein elektronisches Zugangssystem abgewickelt.

Die Türen sind auch tagsüber geschlossen und können nur über einen Schlüssel oder das elektronische Zugangssystem geöffnet werden. Des Weiteren sind im Hauptgebäude die Türen außerhalb der Arbeitszeiten (22:00 bis 06:00 Uhr) abgeschlossen und die Räumlichkeiten sind mit einer Alarmanlage gesichert.

Die Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden sind durch eine ständig verschlossene Türe sowie einer Zugangsprüfung über RFID-Chips gesichert.

Schlüssel werden nur an Berechtigte und fest angestellte Mitarbeiter ausgegeben und eingezogen, sobald die Berechtigung erlischt. Dieselbe Regelung gilt für die Registrierung für den Fingerscan.

Fenster im UG, sind mit Gittern gegen unbefugten Eintritt gesichert. Die Fenster im EG, 1. und 2. OG, sind außerhalb der Arbeitszeiten fest verschlossen.

Der Zugang zum Serverraum ist stets verschlossen und ist nur durch die Administration möglich.

Die Gebäudesicherung erfolgt mittels Alarmanlagen.

3. Zugangskontrolle

Die Zugangskontrolle verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Jeder Berechtigte erhält eine individuelle Benutzerkennung und ein persönliches, geheim zu haltendes Passwort, das nicht an Dritte weitergegeben werden darf.

Das Passwort wird sofort gesperrt, falls die Berechtigung erlischt. Das Passwort besteht aus mindestens 8 Zeichen, wobei die Zeichen zufällig ausgewählte Großbuchstaben, Kleinbuchstaben und Zahlen sein müssen.

Die dargestellten Passwortkonventionen werden durch Systemeinstellungen (technisch) erzwungen. Des Weiteren bestehen entsprechende Passwortrichtlinien (organisatorisch).

Die Arbeitsstationen werden bei Inaktivität automatisch nach 5 Minuten gesperrt. Eine Arbeitsanweisung an die Mitarbeiter gibt verbindlich vor, dass bei Verlassen der Arbeitsstation diese sofort gesperrt wird.

Eine Sperre der Benutzerkennung erfolgt nach 10 Fehlversuchen.

Interne Netze werden nach dem Stand der Technik gegen Zugriffe durch vollständige physische Trennung interner und externer Netze von außen abgeschottet. Des Weiteren werden entsprechende Firewalls eingesetzt.

Einrichtung und Sperrung der Zugangsberechtigungen im System werden dokumentiert.

4. Zugriffskontrolle

Die Zugriffskontrolle beschränkt die Benutzung eines Datenverarbeitungssystems durch die Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten.

Innerhalb des Zugangsberechtigungskonzeptes sind abgestufte Zugriffsberechtigungen vorhanden, die das Eingeben, Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Verarbeitung, Nutzung und nach der Speicherung nur in dem für die jeweilige Aufgabe erforderlichen Umfang erlauben und ansonsten verhindern.

Die Berechtigungen auf Dateisystemebene sind durch entsprechende Nutzergruppen kategorisiert. Auftragsdaten werden in speziell geschützten Pfaden auf dem Server abgelegt und dort verarbeitet.

Die Verwaltung der Zugriffsrechte erfolgt ausschließlich durch die Systemadministratoren. Die mit der Erhebung, Verarbeitung und Nutzung von Daten befassten Mitarbeiter verfügen nicht über Administratorenrechte auf dem Server.

Datenträger werden nach dem Einlesen und Verifizieren der Daten in einem abgeschlossenen Bereich verwahrt oder sofern möglich physikalisch vernichtet (z.B. CDs).

Die administrativen Tätigkeiten sind auf einen kleinen Kreis von Administratoren eingeschränkt.

5. Weitergabekontrolle

Die Weitergabekontrolle verhindert das unbefugte Lesen, Kopieren, Verändern oder Entfernen der Daten bei der elektronischen Übertragung oder während des Transports oder bei ihrer Speicherung auf Datenträgern und protokolliert, an welchen Stellen eine Übermittlung von Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Daten werden in Absprache mit dem Auftraggeber verschlüsselt übertragen. Omikron bietet dazu mit PGP verschlüsselte Filecontainer sowie die verschlüsselte Übertragung der Daten z.B. über HTTPS an.

Es erfolgt eine Dokumentation von Datenempfänger/n, sowie Transport-/ Übermittlungsweg.

Weiterhin gibt es spezielle Verpackungs- und Versandvorschriften zur Beauftragung zuverlässiger Transportunternehmen mit entsprechend dokumentiertem Versandweg (idR. UPS).

6. Eingabekontrolle

Die Eingabekontrolle protokolliert, ob und von wem Daten in Datenverarbeitungssysteme eingegeben und verändert oder entfernt werden.

Die Eingabekontrolle (unbefugte Änderung, Löschung sowie Protokollierung der Änderungen) wird durch Omikron auf Grund der Verarbeitungsart (teilautomatisierte Batch-Verarbeitung) wie folgt umgesetzt:

Alle personenbezogenen Daten werden vor Beginn der Arbeiten mit einem eindeutigen Schlüssel versehen, welcher über alle Verarbeitungsschritte bis hin zu Endergebnis jeden Datensatz eindeutig identifiziert.

Vor jedem Bearbeitungsschritt werden die Daten zur Dokumentation als Kopie abgelegt, so dass alle Änderungen in einem Arbeitsschritt dediziert nachvollzogen werden können. Die Kopien werden im gleichen kundenindividuellen Arbeitsverzeichnisbaum vorgehalten wie die Originale. Sie werden mit den Originalen zu Ende der Beauftragung gelöscht.

7. Auftragskontrolle

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

Grundlage der Verarbeitung der Daten ist die schriftliche Beauftragung durch den Auftraggeber. Omikron wird sich an die jeweils letzte gültige Version der Spezifikation für die Auftragsverarbeitung halten.

Durch den Auftraggeber erwünschte Änderungen im Auftragsablauf werden dokumentiert und dem Auftraggeber schriftlich zur Verfügung gestellt.

Eventuelle Änderungen im Auftragsvolumen und Preis werden gesondert angeboten.

8. Verfügbarkeitskontrolle

Eine Verfügbarkeitskontrolle sichert die Daten gegen zufällige Zerstörung oder Verlust.

Ein Softwareschutz ist gewährleistet durch speicherresidente Scanner gegen die Verletzung der Systemintegrität mit Viren, Trojanern, Würmern und sonstiger Malware. Der Scanner wird täglich (bei Bedarf auch mehrmals) aktualisiert und mit neuen Updates versehen.

Das Betriebssystem sowie die vorhandenen Betriebs- und Sicherheitssoftware werden mit zentral verteilten Updates und Patches aktuell gehalten. Ein Spamfilter sorgt zusätzlich für die Entfernung schädlicher Nachrichten.

Durch eine unterbrechungsfreie Stromversorgung ist hinreichender Hardwareschutz der Serversysteme gewährleistet, auf denen die Daten gespeichert werden.

Das Datensicherungskonzept sieht vor, dass Sicherungskopien des Datenbestands täglich angefertigt werden, dabei sind mehrere Sicherungsversionen verfügbar. Zusätzlich werden regelmäßig Rücksicherungsversuche zur Sicherstellung der Restore-Möglichkeit durchgeführt.

Eine Löschung erfolgt je nach Sicherungsmaßnahme rollierend, d.h. durch Überschreiben der alten Backupkopie der Daten im jeweiligen Rhythmus der Sicherungskopie (d.h. tägliche Backups werden nach aktuellem Stand nach 7 Tagen überschrieben, monatlich rollierende Backups nach 3 Monaten).

Die Aufbewahrung der Sicherungskopien erfolgt außerhalb der Immobilie in einem Schließfach.

Ein Notfall-Handbuch / Notfallkonzept liegt vor.

9. Trennungskontrolle

Die Trennungskontrolle stellt sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Daten werden für jeden Auftragnehmer und jedes Projekt getrennt verarbeitet. Alle Daten werden in separaten Datenbanken und Projektordnern abgelegt.

Die begleitende Auftragsdokumentation dient der Dokumentation der Zwecke, für die die jeweiligen Daten verarbeitet und genutzt werden sollen.

Auftragsdaten sind für die Omikron-eigene Administration zum Zwecke der Datensicherung und für die Mitarbeiter der Abteilung Professional Services zum Zwecke der Verarbeitung zugänglich.

10. Pseudonymisierung

Durch Omikron erstellte Auswertungen werden pseudonymisiert, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist.

11. Datengeheimnis

Alle Mitarbeiter, die personenbezogene oder sonstige Auftragsdaten verarbeiten oder Zugriff darauf haben, wurden schriftlich auf das Datengeheimnis verpflichtet.

Die Übermittlung oder der Zugriff auf personenbezogene Daten an Unterauftragnehmer wird erst dann erfolgen, wenn diese eine Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO unterzeichnet haben.