MENNEKES

Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO

IS
Z-I-IS-001
Version: 2.1
öffentlich

I Geltungsbereich

MEK, MEN, MDS, Midena

II Zweck

Mithilfe dieses Dokuments erfüllen die betroffenen Unternehmen von MENNEKES ihre Pflicht des Art. 32 DS-GVO gegenüber Verantwortlichen.

III Umsetzung & Einhaltung

Z-I

IV Folgen bei Nichteinhaltung oder Nichtbeachtung

- Unklare Rechten und Pflichten
- Auftraggeber kann nicht entscheiden, ob ihm die Standards von MENNEKES ausreichen
- Kein Zustandekommen von Verträgen
- Falsche Auffassungen bzgl. Verantwortlichkeiten

MENNEKES hat die innerbetriebliche Organisation so gestaltet, dass diese den besonderen Anforderungen des Datenschutzes gerecht wird. Die dazu getroffenen Maßnahmen werden im Folgenden detailliert beschrieben.

1 Vertraulichkeit

1.1 Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:
Berechtigungen zu den Räumlichkeiten der IT werden nur an Berechtigte mithilfe von Chipkarten heraus gegeben, der Zutritt zum Rechenzentrum ist protokolliert. Weiterhin ist der Zutritt zum Rechenzentrum nur mithilfe einer freigeschalteten Chipkarte in Verbindung mit einem individuellen PIN-Code möglich. Zutritte zu einzelnen Bereichen werden individuell vergeben. Im Falle eins Alarms greift ein Eskalationsplan über Wachdienst, Polizei und Mitarbeitern von MENNEKES. Während normaler Bürozeiten ist im Eingangsbereich der Empfang ständig besetzt, betriebsfremde Personen werden nicht ohne Begleitung auf das Gelände gelassen. Der Serverraum ist generell verschlossen, sofern keine Wartungsarbeiten durchgeführt werden. Die Türen zu den fensterlosen Serverräumen bestehen aus Stahl / Metall. Weiterhin werden Zaunanlagen genutzt, um unbefugten Zutritt zum Gelände zu verhindern.

1.2 Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Zugang zu den Verarbeitungssystemen ist nur mit Benutzername und Passwort möglich. Für die Arbeitssysteme ist eine automatische Sperrung per Gruppenrichtlinie eingerichtet, die den Bildschirm nach spätestens 15 Minuten automatisch sperrt.

Zudem gibt es Passwortrichtlinien, die von den Benutzern abhängig ihrer Risikoklassifizierung eine bestimmte Passwortlänge erfordert. Eine Firewall ist eingerichtet, wird stets aktualisiert, beobachtet und ausgewertet. Für den Datenaustausch existieren Systeme mit Transportverschlüsselung.

1.3 Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Es gibt unterschiedliche Berechtigungsprofile je Mitarbeitergruppe. Diese werden in Absprachen zwischen der IT-Abteilung und dem Fachbereich individuell vergeben. Über die Beobachtung von Logfile-Protokollen kann im Bedarfsfall der Datenzugriff dem jeweiligen Benutzer zugeordnet werden. Für die ERP-Software, das CRM-System, sowie die Domänen-Anmeldung (Active Directory) werden die Berechtigungen separat geregelt. Berechtigungen werden je nach Aufgabenfeld der Beschäftigten angepasst oder entzogen, etwa bei Personalwechsel. Der Zugriff extern arbeitender Mitarbeiter erfolgt über einen VPN-Zugang (IP-sec-Tunnel) mit 2-Faktor-Authentifizierung.

Außerdem werden Verträge zu Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen abgeschlossen, sofern bei der Fernwartung die Verarbeitung von personenbezogenen Daten Gegenstand der Dienstleistung ist. Bei ausgewählten Mitarbeitern werden ebenfalls Sichtschutzfolien für mobile Datenverarbeitungssysteme eingesetzt.

1.4 Trennungsgebot

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Sämtliche Daten werden auf mehreren Servern virtuell voneinander getrennt. Das Datenablage- und Archivsystem von MENNEKES ist strukturiert in allgemeine Unternehmens-/Verwaltungsdaten und Daten zu projekt-/prozessbezogener Tätigkeit.

Jeder Kunde erhält eine eigene Kundennummer, zu der sämtliche Daten strukturiert abgelegt und archiviert werden. Die Daten werden entweder nach Auftragsabwicklung gelöscht oder, wenn erforderlich, entsprechend der gesetzlichen Vorgaben aufbewahrt und archiviert. Die Trennung von Daten wird durch logische Trennung der Systeme und entsprechenden Zugriffsrechten sichergestellt.

1.5 Pseudonymisierung

Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr zugeordnet werden können.

Anwendung der Prinzipien der Datenminimierung und Speicherbegrenzung bei der Verarbeitung von personenbezogenen Daten:

Die Bearbeitung personenbezogener Daten erfolgt nur auf der Grundlage von vertraglichen Vereinbarungen, Kundenaufträgen oder sonstiger legitimer Rechtsgrundlagen.

Es kommen die Prinzipien der Datenminimierung und Speicherbegrenzung bei der Verarbeitung von personenbezogenen Daten zur Anwendung. So werden zu Zwecken von globalen Auswertungen und Statistiken Daten anonymisiert. Die Auswertung von Trackingdaten beim Zugriff auf Webspace erfolgt ausschließlich anonym und ohne Reporting von IP-Adressen oder Nutzerdaten.

2 Integrität

2.1 Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle...

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Sensible personenbezogene Daten werden grundsätzlich nicht auf unverschlüsselten elektronischen Datenträgern außerhalb des Unternehmens transportiert. Generell erfolgt der Datenaustausch mit Kunden per E-Mail oder über spezielle Tools zur verschlüsselten Übermittlung von Daten.

E-Mails werden auf dem Server protokolliert und archiviert. Zum Einsatz kommende mobile Endgeräte werden verschlüsselt und mit Zugriffsschutz betrieben. Es werden getunnelte Datenfernverbindungen genutzt (VPN).

2.2 Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Bei der Datenverarbeitung der ERP- und CRM-Software kommt eine Protokollierung zum Einsatz. So ist bei der Arbeit im System nachvollziehbar, welcher Benutzer zuletzt Daten eingegeben, verändert oder gelöscht hat.

Darüber hinaus bestehen in anderen Systemen ebenfalls grundsätzliche Protokollierungsmechanismen, um dort die Nachvollziehbarkeit der Datenverarbeitung zu gewährleisten.

Mit Subunternehmen bestehen vertragliche Bedingungen, die auch den sicheren Umgang mit Auftragsdaten regelt. Für den Netzwerkzugriff ist eine Firewall eingerichtet die den Netzwerkverkehr in protokolliert. Bei Bedarf können Protokolle nach dem Vier-Augen-Prinzip genauer ausgewertet werden.

3 Verfügbarkeit

3.1 Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

Firewall und Virenschutz befinden sich jederzeit auf dem aktuellsten Stand. Um maximale Verfügbarkeit gewährleisten zu können, erfolgt ein Monitoring aller wichtigen Anwendungen. Zudem werden die zentralen Hardwaresysteme redundant in einem zweiten Rechenzentrum gehalten. Ein Datensicherungskonzept für die Systeme ist vorhanden. So wird regelmäßig eine Datensicherung durchgeführt, um im Notfall die Systeme wieder herstellen zu können. Eine Dokumentation des Netzwerkaufbaus ist vorhanden. Die Netzwerkanbindungen zu den verschiedenen MENNEKES-Standorten sowie zum Internet sind ebenfalls redundant gehalten. Eine unterbrechungsfreie Stromversorgung und ein Dieselgenerator sorgen dafür, dass die Serversysteme auch bei einem Stromausfall nicht ausfallen. Das Einspielen von Sicherheitsupdates wird mittels zentralem Patch-Management sichergestellt. Die eingesetzte IT-Software wird vor dem Rollout geprüft.

3.2 Wiederherstellbarkeit

Zerstörte oder verlorengegangene Daten sind in einem angemessenen Zeitrahmen wiederherstellbar.

Relevante Daten werden mehrfach täglich gesichert, je nach Datenkategorien und Änderungsfrequenzen. Nach festgelegten Zeitabschnitten werden die zwischenzeitlich auf einen Diskpool gesicherten Daten auf Magnetband geschrieben, die in einem klassischen Generationen-Prinzip strukturiert werden. Die Bänder werden räumlich getrennt von den Platten aufbewahrt.

Im Notfall kann der gesamte Datenbestand über die Bänder entsprechend eingespielt und in angemessener Zeit wiederhergestellt werden. Im Falle eines Stromausfalls, werden alle Server über eine alternative Stromversorgung (USV und Diesel-Aggregat) in Betrieb gehalten. Speziell für den Serverraum ist eine Klimatisierung installiert. Virenschutz/Endpoint-Protection, Firewall sowie ein E-Mail Schutz sichern unser System von außen. Ein Notfallplan wurde erarbeitet. Die Notfalldokumentationen liegen als praktische Anweisung für entsprechende Situationen vor.

4 Prüfbarkeit

4.1 Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich auf der Grundlage von Verträgen, konkreten Aufträgen, explizitem Einverständnis oder berechtigtem Interesse. Lieferanten und Subunternehmer werden sorgfältig ausgewählt und zum Datengeheimnis verpflichtet. Zudem werden Vereinbarungen zur Auftragsverarbeitung nach Art. 28 DSGVO geschlossen.

4.2 Organisationskontrolle

Innerbetriebliche Organisation stellt sicher, dass die Anforderungen des Datenschutzes erfüllt werden können.

Alle Mitarbeiterinnen und Mitarbeiter sind auf das Datengeheimnis verpflichtet und gemäß der allgemeinen Datenschutzrichtlinien von MENNEKES belehrt. Ein entsprechender Nachweis liegt vor. Zum Thema Informations- und IT-Sicherheit sind ebenfalls alle Mitarbeiterinnen und Mitarbeiter informiert. Im Falle eines Datenschutzvorfalls liegt ein Notfallkonzept vor. MENNEKES hat einen internen Datenschutzbeauftragten bestellt. Der Datenschutzbeauftragte hat die stattfindenden Prozesse aus daten-schutzrelevanter Sicht analysiert und diese dokumentiert.