EISENMANN

Technische und organisatorische Maßnahmen zum Datenschutz

Der folgende Maßnahmenkatalog beschreibt die technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten in der Eisenmann SE gemäß Art. 32 DSGVO. Die Ausführungen zu den Rechenzentren beziehen sich auf die Standorte Tübinger Str. 81 in Böblingen, Daimlerstr. 5 in Holzgerlingen sowie Auf der Mauer 1 in Bovenden.

1. Maßnahmen zur Gewährleistung der Vertraulichkeit (Art 32 Abs. 1 lit. b DSGVO)

1.1 Zugangskontrolle (§ 64 Abs. 3 Nr. 1 BDSG)

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

- Alarmanlage
- Revierdienst
- Absicherung der Gebäudeschächte
- versperrte Eingangs- und Innentüren
- Abschließbare Serverräume / -schränke
- Sicherheitsschlösser
- Zutrittskontrollsysteme
- Kein Zutritt zu Serverräumen für Unbefugte (auch kein Reinigungspersonal)
- Sorgfalt bei Auswahl des Wachpersonals
- Besucher werden am Betriebsgelände nicht unbeaufsichtigt gelassen
- Protokollierung über Besuche (wer, wann, bei wem, warum)
- Mitarbeiter- / Besucherausweise
- Schlüsselregelung

1.2 Datenträgerkontrolle (§ 64 Abs. 3 Nr. 2 BDSG)

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

- Sichere Aufbewahrung von Datenträgern (Datenträger in Safe, Diebstahlsicherung für Notebooks)
- Einrichtungen von Standleitungen beziehungsweise VPN-Tunneln
- Verschlüsselung von Notebooks und externen Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern beziehungsweise Dienstleistern
- Protokollierung der Vernichtung
- Löschung von Datenträgern mit zertifizierter Software

Technische und organisatorische Maßnahmen zum Datenschutz

1.3 Speicherkontrolle (§ 64 Abs. 3 Nr. 3 BDSG)

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

- Festlegung von Berechtigungen in Active Directory, Fileservern und Applikationen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Zusätzlicher System-Login für bestimmte Anwendungen
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Fileserver
- Bildschirm- und Computersperre bei Verlassen des Arbeitsplatzes
- Sichtschutzfolien für Notebooks
- Verschlüsselte Speicherung auf Datenträgern

1.4 Benutzerkontrolle (§ 64 Abs. 3 Nr. 4 BDSG)

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

- Festlegung zugangsberechtigter Mitarbeiter zu Serverräumen
- Erstellen von Benutzerprofilen
- Authentifikation mit Benutzername/Passwort
- Regelmäßige Kontrolle von Berechtigungen
- Sperrung von Berechtigungen ausscheidender Mitarbeiter
- Einsatz von Verschlüsselungs-Technologie
- Einsatz von Anti-Viren-Software
- Festlegung der Personen, die Nutzungsberechtigungen haben (Zuständigkeiten)
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

1.5 Zugriffskontrolle (§ 64 Abs. 3 Nr. 5 BDSG)

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

- Festlegung von Berechtigungen in Active Directory, Fileservern und Applikationen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Fileservern

1.6 Trennbarkeit (§ 64 Abs. 3 Nr. 14 BDSG)

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

- unterschiedliche physische Systeme (inkl. eigenständigem Betriebssystem mit z. B. eigenständiger Datenbank je Datenbestand)
- unterschiedliche virtuelle Systeme (inkl. eigenständigem Betriebssystem mit z. B. eigenständiger Datenbank je Datenbestand)
- unterschiedliche Anwendung (z. B. zwei Datenbankensysteme) auf demselben Server
- unterschiedliche Datenbanken in einem Datenbanksystem (dabei darf ein Datenbankanwender nur Rechte auf je einer Datenbank erhalten)
- unterschiedliche Tabellen in einer Datenbank (dabei darf ein Datenbankanwender nur Rechte auf den Tabellensatz eines Datenbestandes haben)

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

2.1 Übertragungskontrolle (§ 64 Abs. 3 Nr. 6 BDSG)

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien
- Auswertungsmöglichkeiten (Feststellung der Sender und Empfänger)

2.2 Eingabekontrolle (§ 64 Abs. 3 Nr. 7 BDSG)

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

- Protokollierung der Änderungen an Daten, Anwendungen und Systemen (z.B. Fileserver, SAP, SharePoint)
- Protokollierung der Administrator-Aktivitäten in diversen Systemen
- Auswertung der Protokolldaten (bei Bedarf)
- Erfassung gescheiterter Zugriffsversuche

2.3 Transportkontrolle (§ 64 Abs. 3 Nr. 8 BDSG)

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien
- Verschlüsselte Übertragung und Speicherung auf Datenträgern

- Zugriff mittels verschlüsselten VPNs
- Schutz vor Schadsoftware (z.B. Viren)
- E-Mail-Verschlüsselung

2.4 Datenintegrität (§ 64 Abs. 3 Nr. 11 BDSG)

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

- Backup- & Recoverykonzept
- Datensicherungen erfolgen in periodischen Abständen (z.B. täglich bei Fileservern)
- Einsatz von Virenscannern, Firewalls, Spam-Filter)
- Sicherstellung der Stromversorgung bei Ausfall

3. Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit von Systemen und Diensten (Art 32 Abs. 1 lit. b DSGVO)

3.1 Zuverlässigkeit (§ 64 Abs. 3 Nr. 10 BDSG)

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- Unabhängig voneinander funktionierende Systeme
- Automatisierte Meldung von Fehlfunktionen
- Anti-Viren-Schutz

3.2 Verfügbarkeitskontrolle (§ 64 Abs. 3 Nr. 13 BDSG)

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

- Überwachung und Meldung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschanlage in Serverräumen
- Schutzsteckdosenleisten im Serverraum
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort (z.B. Datenschutztresor für CDs)
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Notfallplan (Dienstanweisung Wachschutz)

4. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall (Art 32 Abs. 1 lit. c DSGVO)

4.1 Wiederherstellbarkeit (§ 64 Abs. 3 Nr. 9 BDSG)

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

- Backup- & Recoverykonzept
- Festplattenspiegelung
- Testen von Datenwiederherstellung
- IT Notfallhandbuch

5. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art 32 Abs. 1 lit. d DSGVO)

5.1 Datenschutz-Management

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter
- Dokumentierter Prozess zum Umgang mit Auskunfts-, Berichtigungs- und Löschersuchen gemäß DSGVO
- Interner Datenschutzbeauftragter
- Information und Sensibilisierung der Mitarbeiter durch Verfahrensanweisung zum Umgang mit personenbezogenen Daten
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

5.2 Incident-Response-Management

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Intrusion Prevention System (IPS)
- Dokumentierter Prozess zur Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Einbindung des DSB in Sicherheitsvorfälle und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen

5.3 Datenschutzfreundliche Voreinstellungen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen (bei Mailingaktionen der Abteilung *Marketing*)

5.4 Auftragskontrolle (§ 64 Abs. 3 Nr. 12 BDSG)

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

- sorgfältige Auswahl des Auftragnehmers
- eindeutige Vertragsgestaltung, insbesondere Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer und Festlegung der durchzuführenden Kontrollmaßnahmen
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer soweit erforderlich
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Sub-unternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers
- klare und eindeutige Erteilung von Weisungen (im besten Fall in schriftlicher Form)
- Festlegung der zur Erteilung und zum Empfang von Weisungen berechtigten Personen
- Kontrolle der bei dem Auftragnehmer getroffenen technischen und organisatorischen Sicherheitsmaßnahmen
- Regelung des Einsatzes von Unterauftragnehmern
- Vereinbarung von Vertragsstrafen für Verstöße gegen erteilte Weisungen