Technisch-Organisatorische Maßnahmen

endica Allgemein (Stand 2024)

endica GmbH
Pfannkuchstraße 4
76185 Karlsruhe
Deutschland

Inhaltsverzeichnis

1. Einleitung und Rahmenbedingungen

1.1 Einleitung

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.2 Unternehmen / Behörde

Die folgenden Festlegungen repräsentieren das Datenschutzkonzept der

endica GmbH
Pfannkuchstraße 4
76185 Karlsruhe
Deutschland

1.3 Externer Datenschutzbeauftragter

Externer Datenschutzbeauftragter
Komm.ONE AöR
Jürgen Kratzer
Auwaldstraße 11
79110 Freiburg
Deutschland
Telefon: 0761/1300-31739
E-Mail: datenschutz@komm.one

2. Technisch-Organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen Folgendes ein:

2.1 Gewährleistung der Vertraulichkeit

2.1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

- Automatisches Zugangskontrollsystem
- Chipkarten / Transpondersysteme
- Videoüberwachung der Eingänge
- Sicherheitsschlösser
- Besucher nur in Begleitung durch Mitarbeiter
- Alarmanlage
- Schlüsselregelung mit einer Liste
- Serverräume sind abgegrenzt (Sperrbereich)
- Protokollierung der Besucher

  - Dienstleister,

  - Schulungsteilnehmer,

  - ...

2.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Maßnahmen:

- Login mit Benutzername und Passwort
- Einsatz von VPN bei Remote-Zugriff
- Automatische Desktopsperre
- Sperre externer Schnittstellen (USB)
- Verschlüsselung von Datenträgern
- Verschlüsselung von Notebooks / Tablet
- Verschlüsselung von Smartphones
- Verwalten von Benutzerberechtigungen
- Zuordnung von Benutzerrechten
- Zugangssperre bei mehr als 3 Anmeldeversuchen
- Firewall
- Anti-Viren-Software
- Zentrale Passwortvergabe
- Passworthistorie
- SAP GUI Zugang bzw. Zugang über Komm.ONE Cloud/SAP GUI
- Zugang über geschlossenes Netz (KVN bzw. VPN Zugang)
- SAP Berechtigungsverwaltung: Transaktionaler Zugang zu den einzelnen Produkten

2.1.3 Zugriffskontrolle

Maßnahmen, die 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:

- Differenzierte Berechtigungen (Anwendungen)
- Differenzierte Berechtigungen (Daten)
- Einsatz von Entsorgungsunternehmen für die Entsorgung von Datenträgern
- MultiChannelFoundation (MCF) Zugriff im Selfservice-Portal für:
  endica4ERP Finance
  endica4ERP Ordermanagement
  endica4Utilities

2.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Maßnahmen:

- Logische Mandantentrennung (softwareseitig)
- Festlegung von Datenbankrechten
- Physikalische Trennung von Systemen
- Steuerung über Berechtigungskonzepte und Rollenkonzepte
- Trennung von Produktiv-, Entwicklungs- und Testumgebung

2.2 Gewährleistung der Integrität

2.2.1 Weitergabekontrolle

Maßnahmen, die 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:

- Dokumentierte Weitergabe der Daten an den Auftragsverarbeiter
- Einsatz von VPN-Technologie
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Dokumentation der Datenempfänger
- elektronische Empfangsbestätigungen
- Nutzung von Signaturverfahren
- AS4 Kommunikation

2.2.2 Eingabekontrolle

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

Maßnahmen:

- Teilweise technische Protokollierung der Eingabe von Daten
- Teilweise technische Protokollierung der Änderung von Daten
- Teilweise technische Protokollierung der Löschung von Daten
- Nachvollziehbarkeit der Bearbeitung von Daten durch individuelle Benutzernamen
- Übersicht über die Nutzung der Programme zur Bearbeitung von Daten
- Vergabe von Rechten zur Bearbeitung von Daten

- Manuelle Kontrolle der Protokolle

2.3 Pseudonymisierung und Verschlüsselung

2.3.1 Pseudonymisierung

Maßnahmen, die eine Pseudonymisierung von Daten gewährleisten.

Maßnahmen:

- Authentisierung im Selfservice-Portal (MCF) durch Pseudonyme (bspw. Kundennummer, Zählernummer...)

2.3.2 Verschlüsselung

Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

Maßnahmen:

- Sicherung der Kennwörter mit Hash Werten
- Verschlüsselung des Transports von E-Mails
- Verschlüsselung von Daten in mobilen Geräten
- Transportverschlüsselung im Selfservice-Portal (MCF)

2.4 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

2.4.1 Verfügbarkeit (der Daten)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Maßnahmen:

- Datensicherungen

  Sicherungen auf SAN

  SAN an zwei RZ Standorten
- Unterbrechungsfreie Stromversorgung (USV)
- Backup & Recovery-Konzept (M11.S12)
- Wöchentliche Backups
- Datensicherungskonzept vorhanden
- Kontrolle des Sicherungsvorgangs
- SLA mit Hosting Dienstleister/Geschäftsbesorgungsvertrag

2.4.2 Belastbarkeit (der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Maßnahmen:

- Einsatz von Hardware Firewalls
- Einspielen von aktuellen Sicherheitsupdates auf allen Applikationsservern
- Einspielen von Sicherheitsupdates auf allen Entwicklersystemen

2.4.3 Wiederherstellbarkeit (der Daten / der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Maßnahmen:

- Feuer- und Rauchmeldeanlagen
- Backup & Recovery-Konzept (M11.S12)

2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

2.5.1 Auftragskontrolle

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

Maßnahmen:

- Abschluss der notwendigen Auftragsdatenvereinbarungen
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten

  - Kriterien für die Auswahl von Auftragsverarbeitern (Formular Garantien DSGVO 28.1)
- Überprüfung des Schutzniveaus des Auftragnehmers (kontinuierlich) im Rahmen IDW
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten (bei Bestellpflicht)
- Sicherheitszertifikat nach BSI IT-Grundschutz und ISO 27001 des Auftragsverarbeiters

2.5.2 Datenschutz-Management

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

Maßnahmen:

- Bestellung eines externen Datenschutzbeauftragten
- Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz
- Verpflichtung der Mitarbeiter auf die Vertraulichkeit und den Datenschutz

2.5.3 Incident-Response-Management

Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Maßnahmen:

- Dokumentation von Sicherheitsvorfällen
- Dokumentierter Prozess zur Erkennung von Sicherheitsvorfällen
- Dokumentierter Prozess zur Meldung von Sicherheitsvorfällen
- Einbindung von Datenschutzbeauftragten in Sicherheitsvorfälle
- Klarer Prozess zur Regelung von Verantwortlichkeiten bei Sicherheitsvorfällen

2.5.4 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) einer Software vorab ein gewisses Datenschutzniveau herrscht.

Maßnahmen:

- Personenbezogene Daten werden nur zweckerforderlich erhoben