TOM-Bericht

Inhaltsverzeichnis

Allgemeine technische und organisatorische Maßnahmen **1**

Allgemeine technische und organisatorische Maßnahmen

DP_M_ToEx AG_001 : Zutrittskontrolle Betriebsräume

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Der Schutz vor unbefugtem Zutritt zu den Betriebsräumen erfolgt mehrstufig mittels folgender Maßnahmen: **Technische Maßnahmen** • Sicherheitsschloss mit Sicherheitsschlüssel, die nicht vervielfältigt werden können • Betriebsräume besitzen eigenen, vom restlichen Gebäude separierten Schließkreis • Einsatz persönlich zugewiesener Schlüssel • Zentrale Freischaltung der Eingangstür nach Meldung an Gegensprechanlage • Schutz der Datenverarbeitungsanlagen und Netzwerk-Infrastruktursysteme durch Zylinderschlösser an Gehäusen bzw. Schränken **Organisatorische Maßnahmen** • Besucher bewegen sich ausschließlich gemeinsam in Begleitung autorisierte Firmenmitglieder in sensiblen Bereichen • Empfangsbereich ist durch eigenes Personal besetzt • Dokumentierte Schlüsselübergabe

DP_M_ToEx AG_002 : Zutrittskontrolle zu Server und Netzwerk-Management

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	**Technische Maßnahmen** • abgeschlossener Raum mit separatem Schließkreis und Sicherheitsschloss • Server-Schrank separat mit Zylinderschloss gesichert **Organisatorische Maßnahmen** • Zutritt durch Reinigungspersonal innerhalb der Arbeitszeit und unter Aufsicht

DP_M_ToEx AG_003 : Zugriffskontrolle

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Tiefgreifende und weiterführende Maßnahmen zur Gewährleistung der ausschließlichen Nutzung von Datenverarbeitungssystemen durch Berechtigte mit deren differenzierten Zugriffsberechtigungen. Entsprechende Berechtigungen können ausschließlich durch die Geschäftsleitung erteilt werden. **Technische Maßnahmen** • Modifikation von Zugriffsberechtigungen nur durch einen Administrator-Account möglich • Protokollierung von relevanten Systemaktivitäten zur Rekonstruktion unerwünschter Ablauffolgen • Verschlüsselung von Festplatten **Organisatorische Maßnahmen** • vorrangige Vergabe untergeordneter Rollen an zu autorisierende Mitarbeiter anstelle vollständiger Administratoren-Berechtigung • Entfernen von Benutzerrechten erfolgt unverzüglich bei Ausscheiden bzw. bei Entfall des Erfordernisses • Gewährung von Benutzerrechten erfordert die Freigabe des jeweiligen Vorgesetzten bzw. der Geschäftsleitung • Vernichtung von Dokumenten und Datenträgern mit schützenswerten Inhalten durch zertifizierte Entsorgungsunternehmen gegen Nachweis (DIN 32757)

DP_M_ToEx AG_004 : Weitergabekontrolle

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Sicherstellung, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Ebenso muss feststellbar sein, an welche Stellen eine Übermittlung vorgesehen ist. Regelungen für eine datenschutzgerechte Vernichtung von Dokumenten und Datenträgern ergänzt die Weitergabekontrolle. **Organisatorische Maßnahmen** • Kein elektronischer Versand von Dokumenten mit personenbezogenen Inhalten • Verpflichtung der Mitarbeiter auf ausschließlichen Versand von E-Mails ohne Inhalte über personenbezogene Daten • Schulung der Mitarbeiter zum Umgang mit IT-Geräten, insbesondere bei mobiler Arbeit

DP_M_ToEx AG_005 : Trennungskontrolle

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden. **Technische Maßnahmen** • Physische Trennung zwischen Verarbeitungstätigkeiten mit Unternehmensdaten und Gesundheitsdaten • Kundendatenbanktrennung bei Auftragsverarbeiter • Trennung von Benutzer- und Administrationsrechten • Trennung von Test- und Produktivdaten **Organisatorische Maßnahmen** • Verwendung separater Datenbanksysteme für unterschiedliche Anwendungen inkl. abweichender Zugangsdaten für System-Administratoren

DP_M_ToEx AG_006 : Verfügbarkeitskontrolle

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Verhinderung der zufälligen Zerstörung, des Verlusts oder Untergangs personenbezogener Daten. **Technische Maßnahmen** • Interne Datenverarbeitungsanlagen • Redundante Datenspeicherung • Rechenzentrum mit geeigneten Redundanzen • Klimatisierung • Versorgungssysteme und unterbrechungsfreie Stromversorgung • ausgelegte IT-Systeme • Rauch- und Brandmeldesystem • Einsatz von Antivirus-Software und Firewalls mit Netzwerküberwachung **Organisatorische Maßnahmen** • Datensicherungskonzept • Mehrmals tägliche Datensicherung • Regelmäßige Prüfung der Sicherungsbestände • Tätigkeiten des Rechenzentrums auf Basis eines Service-Level-Agreements

DP_M_ToEx AG_007 : Eingabekontrolle

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden. Eine Eingabekontrolle wird durch Protokollierung erreicht, die auf verschiedenen Ebenen stattfinden kann. **Technische Maßnahmen** • Einsatz von Protokollierungssystemen • Benutzerrechteverwaltung und Rechtemanagement zur Verhinderung von Datenlöschungen **Organisatorische Maßnahmen** • Fremd- bzw. Fernwartung ist durch einen AV-Vertrag gesichert und wird zusätzlich durch einen firmeninternen Mitarbeiter überwacht

DP_M_ToEx AG_008 : Verfügbarkeitskontrolle

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Verhinderung der zufälligen Zerstörung, des Verlusts oder Untergangs personenbezogener Daten. **Technische Maßnahmen** • Interne Datenverarbeitungsanlagen • Redundante Datenspeicherung • Rechenzentrum mit geeigneten Redundanzen • Klimatisierung • Versorgungssysteme und unterbrechungsfreie Stromversorgung • ausgelegte IT-Systeme • Rauch- und Brandmeldesystem • Einsatz von Antivirus-Software und Firewalls mit Netzwerküberwachung **Organisatorische Maßnahmen** • Datensicherungskonzept • Mehrmals tägliche Datensicherung • Regelmäßige Prüfung der Sicherungsbestände • Tätigkeiten des Rechenzentrums auf Basis eines Service-Level-Agreements

DP_M_ToEx AG_009 : Datenschutz-Management

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Maßnahmen zum zuverlässigen Schutz personenbezogener Daten sowie zur Überprüfung des Datenschutzkonzeptes **Organisatorische Maßnahmen** • Zugänglichmachen von Datenschutzdokumenten für Beschäftigte • Datenschutzrichtlinie • IT-Sicherheitskonzept • TOMs • Verzeichnis der Verarbeitungstätigkeiten • Verpflichtung auf das Datengeheimnis aller Mitarbeiter, firmenintern und Mitarbeiter von Auftragsverarbeiter • Schulung von Mitarbeitern, firmenintern und Mitarbeiter von Auftragsverarbeiter • Regelmäßige Überprüfung auf Wirksamkeit der TOMs

DP_M_ToEx AG_010 : Incident-Response-Management

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Maßnahmen zur Vorbeugung oder als Reaktion auf erkannte/vermutete Sicherheitsvorfälle oder Störungen **Technische Maßnahmen** • Einsatz von Firewall Systemen • Einsatz von Spamfilter Systemen • Einsatz von Virenscannern • regelmäßige Aktualisierung der Systeme **Organisatorische Maßnahmen** • Sichtung und Auswertung von Log-Files und Protokollen durch autorisierte Personen • Maßnahmen zur Behandlung erkannter Sicherheitsvorfälle durch geeignete Personen • Dokumentation erkannter Sicherheitsvorfälle • Informationen an Beschäftigte bei akuten Gefährdungslagen

DP_M_ToEx AG_011 : Datenschutzfreundliche Voreinstellungen

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Mittels getroffener Voreinstellungen werden nur solche personenbezogenen Daten erhoben und verarbeitet, welche für den jeweiligen bestimmungsgemäßen Zweck tatsächlich erforderlich sind. **Technische Maßnahmen** • Einsatz von Systemen, die die Grundsätze zur Verarbeitung standardmäßig unterstützen • Einsatz von Verschlüsselung bei der Speicherung und Übermittlung von personenbezogenen Daten **Organisatorische Maßnahmen** • Spezielle Schulung der Beschäftigten hinsichtlich des Grundsatzes der Datenminimierung

DP_M_ToEx AG_012 : Auftragskontrolle

OrgEh:	TogetherExample AG (ToEx AG)
Beschreibung:	Eine Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich nach Weisung durch den Verantwortlichen/Auftraggeber. Hierfür ist für jeden Vorgang eine schriftliche Auftragsverarbeitungsvereinbarung erforderlich. **Technische Maßnahmen** • potenzieller Auftragnehmer unter sorgfältiger Berücksichtigung der Wahrung von Datenschutz und Datensicherheit der notwendigen Auftragsverarbeitungsvereinbarung vor Aufnahme der Tätigkeit Weisung zum Ablauf