



Verarbeitungstätigkeit

Arbeitsmedizinische Vorsorge

zu den Auftragsverarbeitern: Betriebsarzt (Ext_DE_BA), Betriebsarzt (Ext_AT_BA)

Das gegenständliche Dokument gilt als vertraulich und ist ausschließlich für den internen Gebrauch bestimmt.
Es ist nicht gestattet, dieses Dokument oder Teile daraus in irgendeiner Form zum Gebrauch durch Dritte zu vervielfältigen und/oder ganz bzw. auszugsweise zu veröffentlichen.
Das Dokument im Original, Kopien oder Auszüge daraus müssen auf Verlangen zurückgegeben werden.



Gesamtregister der ToEx AG

Organisationseinheit:	TogetherExample AG
OrgEh Verantwortlich:	Berthold Corporation
E-Mail:	Berthold.Corporation@example.com
Telefon:	+43 123 456 7890
Verantwortlicher:	Berthold Corporation
E-Mail:	Berthold.Corporation@example.com
Telefon:	+43 123 456 7890
Datenschutzbeauftragter:	D. Schutz
E-Mail:	datenschutz@example.com
Telefon:	+43 123 456 7890

Personalverwaltung

Organisationseinheit:	HR Services
Verantwortlich:	Christian Personnel
E-Mail:	Christian.Personnel@example.com
Telefon:	+43 123 456 7890

Verarbeitungstätigkeiten

1. Arbeitsmedizinische Vorsorge

VT-Verantwortlichkeit:	TogetherExample AG (ToEx AG), Betriebsarzt (Ext_DE_BA), Betriebsarzt (Ext_AT_BA)		
Einführungsdatum:	14.01.2025	Version:	1 (Bearbeitung abgeschlossen)
Zweck:	Verarbeitung von gesundheitsbezogenen Daten der Mitarbeiter im Rahmen der arbeitsmedizinischen Vorsorge und Arbeitszeitgesetz		
Datenschutz-Folgenabschätzung:	<input checked="" type="checkbox"/> DSFA Arbeitsmedizinische Vorsorge Eine Erforderlichkeit der DSFA aufgrund der Schwellwertanalyse wurde nicht ermittelt: Durchführung arbeitsmedizinischer Untersuchungen aller Mitarbeiter, inkl. Auszubildender, die das 18. LJ noch nicht erreicht haben. Es werden keine Ergebnisse oder Befunde an den Arbeitgeber übermittelt, daher wird die Erforderlichkeit einer DSFA als nicht gegeben angesehen. Eine DSFA erscheint aufgrund einer Erforderlichkeitsprüfung als nicht notwendig. Ergebnis der Datenschutz-Folgenabschätzung: Die Verarbeitungstätigkeit steht im Einklang mit den datenschutzrechtlichen Vorgaben.		



Betroffene

1. Mitarbeiter

Rechtsgrundlage:	Rechtliche Verpflichtung
Anmerkungen:	ASchG bzw. ArbmedVV

Datenkategorien

1.1. Mitarbeiterdaten V1

Beschreibung:	Diese Datenkategorie enthält die Subkategorien zu Mitarbeiterdaten.
---------------	---

Gesundheitsdaten MA

Beschreibung:	Daten aus der Betreuung durch den Betriebsarzt oder das Medical Team				
Löschfrist:	10 Jahr(e)				
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV:	<input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge			
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV:	<input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge			
Empfänger:	TogetherExample AG	Extern:	<input type="checkbox"/>	AV:	<input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Ergebnissen aus der arbeitsmedizinischen Vorsorge			

Kontaktdaten MA

Beschreibung:	E-Mail-Adresse dienstlich und privat, Telefonnummer dienstlich und privat, Wohnadresse, Notfallkontakte, Angehörigendaten				
Löschfrist:	30 Jahr(e)				
Begründung:	§ 1163 in Verbindung mit § 1478 des aBGB maximal 30 Jahre nach Beendigung des Dienstverhältnisses				
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV:	<input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge			
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV:	<input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge			
Empfänger:	TogetherExample AG	Extern:	<input type="checkbox"/>	AV:	<input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Ergebnissen aus der arbeitsmedizinischen Vorsorge			



Organisatorische Zugehörigkeit

Beschreibung:	Positionscode, Kostenstelle, Dienstvertrag, Einstufung, Eintrittsdatum, Kündigungsfrist			
Löschfrist:	30 Jahr(e)			
Begründung:	§ 1163 in Verbindung mit § 1478 des aBGB maximal 30 Jahre nach Beendigung des Dienstverhältnisses			
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge		
	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge		
	TogetherExample AG	Extern:	<input type="checkbox"/>	AV: <input type="checkbox"/>
Empfänger:	TogetherExample AG	Extern:	<input type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Ergebnissen aus der arbeitsmedizinischen Vorsorge		

Personendaten MA

Beschreibung:	Staatsangehörigkeit, Geschlecht			
Löschfrist:	10 Jahr(e)			
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge		
	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge		
	TogetherExample AG	Extern:	<input type="checkbox"/>	AV: <input type="checkbox"/>
Empfänger:	TogetherExample AG	Extern:	<input type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Ergebnissen aus der arbeitsmedizinischen Vorsorge		

Stammdaten MA

Beschreibung:	Name, Titel, Anrede, Geburtsdatum und -ort, Personalnummer			
Löschfrist:	30 Jahr(e)			
Begründung:	§ 1163 in Verbindung mit § 1478 des aBGB maximal 30 Jahre nach Beendigung des Dienstverhältnisses			
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge		
	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
Empfänger:	Betriebsarzt	Extern:	<input checked="" type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Daten zur Durchführung der arbeitsmedizinischen Vorsorge		
	TogetherExample AG	Extern:	<input type="checkbox"/>	AV: <input type="checkbox"/>
Empfänger:	TogetherExample AG	Extern:	<input type="checkbox"/>	AV: <input type="checkbox"/>
	Zweck und Rechtsgrundlage:	Übermittlung von Ergebnissen aus der arbeitsmedizinischen Vorsorge		



Allgemeine technische und organisatorische Maßnahmen

Auftragskontrolle

Beschreibung:	<p>Eine Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich nach Weisung durch den Verantwortlichen/Auftraggeber. Hierfür ist für jeden Vorgang eine schriftliche Auftragsverarbeitungsvereinbarung erforderlich.</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none">• potenzieller Auftragnehmer unter sorgfältiger Berücksichtigung der Wahrung von Datenschutz und Datensicherheit der notwendigen Auftragsverarbeitungsvereinbarung vor Aufnahme der Tätigkeit Weisung zum Ablauf
---------------	--

Datenschutz-Management

Beschreibung:	<p>Maßnahmen zum zuverlässigen Schutz personenbezogener Daten sowie zur Überprüfung des Datenschutzkonzeptes</p> <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none">• 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
---------------	---

Datenschutzfreundliche Voreinstellungen

Beschreibung:	<p>Mittels getroffener Voreinstellungen werden nur solche personenbezogenen Daten erhoben und verarbeitet, welche für den jeweiligen bestimmungsgemäßen Zweck tatsächlich erforderlich sind.</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none">• Einsatz von Systemen, die die Grundsätze zur Verarbeitung standardmäßig unterstützen• Einsatz von Verschlüsselung bei der Speicherung und Übermittlung von personenbezogenen Daten <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none">• Spezielle Schulung der Beschäftigten hinsichtlich des Grundsatzes der Datenminimierung
---------------	---



Eingabekontrolle

Beschreibung:	<p>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.</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none"> • Einsatz von Protokollierungssystemen • Benutzerrechteverwaltung und Rechtemanagement zur Verhinderung von Datenlöschungen <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none"> • Fremd- bzw. Fernwartung ist durch einen AV-Vertrag gesichert und wird zusätzlich durch einen firmeninternen Mitarbeiter überwacht
---------------	--

Incident-Response-Management

Beschreibung:	<p>Maßnahmen zur Vorbeugung oder als Reaktion auf erkannte/vermutete Sicherheitsvorfälle oder Störungen</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none"> • Einsatz von Firewall Systemen • Einsatz von Spamfilter Systemen • Einsatz von Virenscannern • regelmäßige Aktualisierung der Systeme <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none"> • 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
---------------	--

Trennungskontrolle

Beschreibung:	<p>Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden.</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none"> • Physische Trennung zwischen Verarbeitungstätigkeiten mit Unternehmensdaten und Gesundheitsdaten • Kundendatenbanktrennung bei Auftragsverarbeiter • Trennung von Benutzer- und Administrationsrechten • Trennung von Test- und Produktivdaten <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none"> • Verwendung separater Datenbanksysteme für unterschiedliche Anwendungen inkl. abweichender Zugangsdaten für System-Administratoren
---------------	---



Verfügbarkeitskontrolle

Beschreibung:	<p>Verhinderung der zufälligen Zerstörung, des Verlusts oder Untergangs personenbezogener Daten.</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none">• 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 <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none">• Datensicherungskonzept• Mehrmals tägliche Datensicherung• Regelmäßige Prüfung der Sicherungsbestände• Tätigkeiten des Rechenzentrums auf Basis eines Service-Level-Agreements
---------------	---

Verfügbarkeitskontrolle

Beschreibung:	<p>Verhinderung der zufälligen Zerstörung, des Verlusts oder Untergangs personenbezogener Daten.</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none">• 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 <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none">• Datensicherungskonzept• Mehrmals tägliche Datensicherung• Regelmäßige Prüfung der Sicherungsbestände• Tätigkeiten des Rechenzentrums auf Basis eines Service-Level-Agreements
---------------	---



Weitergabekontrolle

Beschreibung:	<p>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.</p> <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none">• 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
---------------	---

Zugriffskontrolle

Beschreibung:	<p>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.</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none">• Modifikation von Zugriffsberechtigungen nur durch einen Administrator-Account möglich• Protokollierung von relevanten Systemaktivitäten zur Rekonstruktion unerwünschter Ablauffolgen• Verschlüsselung von Festplatten <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none">• 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)
---------------	---



Zutrittskontrolle Betriebsräume

Beschreibung:	<p>Der Schutz vor unbefugtem Zutritt zu den Betriebsräumen erfolgt mehrstufig mittels folgender Maßnahmen:</p> <p>Technische Maßnahmen</p> <ul style="list-style-type: none">• 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 <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none">• Besucher bewegen sich ausschließlich gemeinsam in Begleitung autorisierte Firmenmitglieder in sensiblen Bereichen• Empfangsbereich ist durch eigenes Personal besetzt• Dokumentierte Schlüsselübergabe
---------------	--

Zutrittskontrolle zu Server und Netzwerk-Management

Beschreibung:	<p>Technische Maßnahmen</p> <ul style="list-style-type: none">• abgeschlossener Raum mit separatem Schließkreis und Sicherheitsschloss• Server-Schrank separat mit Zylinderschloss gesichert <p>Organisatorische Maßnahmen</p> <ul style="list-style-type: none">• Zutritt durch Reinigungspersonal innerhalb der Arbeitszeit und unter Aufsicht
---------------	---