

Information Security Document

ADOLF WÜRTH GMBH & CO.KG

Technische und Organisatorische Maßnahmen
(TOMS) AWKG -DE-

Inhaltsverzeichnis

1. ZWECK, ANWENDUNGSBEREICH UND ANWENDER	3
2. REFERENZDOKUMENTE	3
3. VERTRAULICHKEIT	3
3.1. Zutrittskontrolle	4
3.2. Zugangskontrolle	4
3.3. Zugriffskontrolle	5
3.4. Trennungskontrolle.....	5
3.5. Pseudonymisierung.....	6
4. INTEGRITÄT	6
4.1. Weitergabekontrolle	6
4.2. Eingabekontrolle	6
5. VERFÜGBARKEIT UND BELASTBARKEIT	7
5.1. Verfügbarkeitskontrolle	7
6. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG.....	8
6.1. Datenschutzmaßnahmen	8
6.2. Incident-Response-Management.....	8
6.3. Datenschutzfreundliche Voreinstellungen	9
6.4. Auftragskontrolle.....	9
7. GÜLTIGKEIT UND DOKUMENTEN-MANAGEMENT.....	10

1. Zweck, Anwendungsbereich und Anwender

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

Technische und organisatorische Maßnahmen werden in den Anforderungen des Datenschutzes methodisch geordnet. Diese Kategorien sind wie folgt unterteilt:

- **Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**
 - Zutrittskontrolle
 - Zugangskontrolle
 - Zugriffskontrolle
 - Trennungskontrolle
 - Pseudonymisierung
- **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**
 - Weitergabekontrolle
 - Eingabekontrolle
- **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**
 - Verfügbarkeitskontrolle
- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)**
 - Datenschutz-Maßnahmen
 - Incident-Response-Management
 - Datenschutzfreundliche Voreinstellungen
 - Auftragskontrolle

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

2. Referenzdokumente

- ISO/IEC 27001 Standard
- 5.2 Richtlinie Informationssicherheit

3. Vertraulichkeit

3.1. Zutrittskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Alarmanlage	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input checked="" type="checkbox"/> Automatisches Zugangskontrollsystem	<input checked="" type="checkbox"/> Empfang / Rezeption / Pförtner
<input checked="" type="checkbox"/> Biometrische Zugangssperren	<input checked="" type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input checked="" type="checkbox"/> Chipkarten/Transpondersysteme	<input checked="" type="checkbox"/> Mitarbeiter- / Besucherausweise
<input checked="" type="checkbox"/> Manuelles Schließsystem	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals
<input checked="" type="checkbox"/> Absicherung der Gebäudeschächte	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input checked="" type="checkbox"/> Türen mit Knauf Außenseite	
<input checked="" type="checkbox"/> Klingelanlage mit Kamera	
<input checked="" type="checkbox"/> Videoüberwachung der Eingänge	
<input checked="" type="checkbox"/> Sicherheitsverglasung	

3.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die Verhinderung der unbefugten Nutzung von Anlagen gemeint.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Login mit Benutzer + Passwort	<input checked="" type="checkbox"/> Verwalten von Benutzerberechtigungen
<input checked="" type="checkbox"/> Zertifikatbasierte Zugriffsberechtigung	<input checked="" type="checkbox"/> Erstellen von Benutzerprofilen
<input checked="" type="checkbox"/> Anti-Viren-Software Server	<input checked="" type="checkbox"/> Zentrale Policy für Passwortvergabe (Wechseldauer, Komplexität)
<input checked="" type="checkbox"/> Anti-Virus-Software-Clients (Desktops, Laptops, Windows-Tablets)	<input checked="" type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Mitarbeiter- / Besucherausweise
<input checked="" type="checkbox"/> Intrusion Detection Systeme	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Einsatz von VPN bei Remote-Zugriffen	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals

<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input checked="" type="checkbox"/> Verschlüsselung von Notebooks/Tablet (Windows)	<input checked="" type="checkbox"/> IT-Verfahren sicheres Passwort
<input checked="" type="checkbox"/> BIOS Schutz (separates Passwort)	<input checked="" type="checkbox"/> IT-Verfahren Löschen/Vernichten
<input checked="" type="checkbox"/> Überwachung externer Schnittstellen (USB)	<input checked="" type="checkbox"/> IT-Verfahren „Clean Desk“
<input checked="" type="checkbox"/> Automatische Desktopsperre	<input checked="" type="checkbox"/> Allg. Richtlinie Datenschutz und/oder Sicherheit
	<input checked="" type="checkbox"/> IT-Verfahren Mobile Device
	<input checked="" type="checkbox"/> Anleitung „Manuelle Desktopsperre“

3.3. 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 Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Aktenschredder	<input checked="" type="checkbox"/> Einsatz Berechtigungskonzept
<input checked="" type="checkbox"/> Externer Aktenvernichter (DIN 66399)	<input checked="" type="checkbox"/> Minimale Anzahl an Administratoren
<input checked="" type="checkbox"/> Physische Zerstörung von Datenträgern (DIN 66399)	<input checked="" type="checkbox"/> Datenschutztresor
<input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren
<input checked="" type="checkbox"/> Sicherung von Schnittstellen	

3.4. 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.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Trennung von Produktiv- und Testumgebung	<input checked="" type="checkbox"/> Steuerung über Berechtigungskonzept
<input checked="" type="checkbox"/> Mandantenfähigkeit relevanter	<input checked="" type="checkbox"/> Festlegung von Datenbankrechten

Anwendungen	
-------------	--

3.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technische und organisatorische Maßnahmen unterliegen (Art.4 Nr. 5 DSGVO)

Aktuell keine entsprechenden Verarbeitungen.

4. Integrität

4.1. 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..

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Einsatz von VPN	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
<input checked="" type="checkbox"/> Protokollierung der Zugriffe und Abrufe	
<input checked="" type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
<input checked="" type="checkbox"/> Nutzung von Signaturverfahren	

4.2. 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.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
<input checked="" type="checkbox"/> Manuelle Kontrolle der Protokolle	<input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung, Löschung von Daten auf Basis eines Berechtigungskonzepts

	<input checked="" type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	<input checked="" type="checkbox"/> Klare Zuständigkeiten für Löschungen

5. Verfügbarkeit und Belastbarkeit

5.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen	<input checked="" type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input checked="" type="checkbox"/> Feuerlöscher Serverraum	<input checked="" type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input checked="" type="checkbox"/> Serverraumüberwachung (Temperatur, Feuchtigkeit)	<input checked="" type="checkbox"/> Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse.
<input checked="" type="checkbox"/> Serverraum klimatisiert	<input checked="" type="checkbox"/> Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
<input checked="" type="checkbox"/> USV (unterbrechungsfreie Stromversorgung)	<input checked="" type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
<input checked="" type="checkbox"/> Schutzsteckdosen Serverraum	<input checked="" type="checkbox"/> Getrennte Partitionen für Betriebssystem und Daten
<input checked="" type="checkbox"/> Datenschutztresor (S60DIS, S120DIS andere geeignete Normen mit Quelldichtung etc.)	
<input checked="" type="checkbox"/> RAID System / Festplattenspiegelung	
<input checked="" type="checkbox"/> Videoüberwachung Serverraum	
<input checked="" type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zu dem Serverraum	
<input checked="" type="checkbox"/> Überspannungsschutz	

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

6.1. Datenschutzmaßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf / Berechtigung (Intranet)	<input checked="" type="checkbox"/> Interner Datenschutzbeauftragter
<input checked="" type="checkbox"/> Sicherheitszertifizierung nach TÜV RDC	<input checked="" type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet.
<input checked="" type="checkbox"/> Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	<input checked="" type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
	<input checked="" type="checkbox"/> Interner Informationssicherheitsbeauftragter
	<input checked="" type="checkbox"/> Die Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt (DSFA)
	<input checked="" type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	<input checked="" type="checkbox"/> Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen vorhanden

6.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
<input checked="" type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
<input checked="" type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
<input checked="" type="checkbox"/> Intrusion Detection System (IDS)	<input checked="" type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen

<input checked="" type="checkbox"/> Intrusion Prevention System (IPS)	<input checked="" type="checkbox"/> Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
---	--

6.3. Datenschutzfreundliche Voreinstellungen

Privacy by design / privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
<input checked="" type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	

6.4. Auftragskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
	<input checked="" type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	<input checked="" type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln oder anderer Garantien
	<input checked="" type="checkbox"/> Schriftliche Weisungen (E-Mail, Ticket) an den Auftragnehmer
	<input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	<input checked="" type="checkbox"/> Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht

	<input checked="" type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	<input checked="" type="checkbox"/> Regelung zum Einsatz weiterer Subunternehmer
	<input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7. Gültigkeit und Dokumenten-Management

Dieses Dokument ist ab Freigabe gültig.

Der Eigentümer des Dokuments ist der Informationssicherheitsbeauftragte (ISB), der das Dokument mindestens einmal jährlich prüfen und ggf. aktualisieren muss.