Anlage -

Technische und Organisatorische Maßnahmen (TOMS) ADOLF WÜRTH GMBH & CO. KG

Inhaltsverzeichnis

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
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☒ Biometrische Zugangssperren	☒ Besucherbuch / Protokoll der Besucher
☒ Chipkarten/Transpondersysteme	☒ Mitarbeiter- / Besucherausweise
☒ Manuelles Schließsystem	☒ Besucher in Begleitung durch Mitarbeiter
☒ Sicherheitsschlösser	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Absicherung der Gebäudeschächte	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Türen mit blindgeschalteter Klinke Außenseite	
☒ Klingelanlage mit Kamera	
☒ Videoüberwachung der Eingänge	
☒ Videoüberwachung im Innenbereich	
☒ 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
☒ Login mit Benutzer + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Zertifikatbasierte Zugriffberechtigung	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Policy für Passwortvergabe (Wechseldauer, Komplexität)
☒ Anti-Virus-Software-Clients (Desktops,	☒ Besucherbuch / Protokoll der Besucher

Laptops, Windows-Tablets)	
☒ Firewall	☒ Mitarbeiter- / Besucherausweise
☒ Intrusion Prevention Systeme	☒ Besucher in Begleitung durch Mitarbeiter
☒ Einsatz von VPN bei Remote-Zugriffen	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Verschlüsselung von Datenträgern	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Verschlüsselung von Notebooks/Tablet (Windows)	☒ IT-Verfahren sicheres Passwort
☒ BIOS Schutz (separates Passwort)	☒ IT-Verfahren Löschen/Vernichten
☒ Überwachung externer Schnittstellen (USB)	☒ IT-Verfahren „Clean Desk“
☒ Automatische Desktopsperre	☒ Allg. Richtlinie Datenschutz und/oder Sicherheit
	☒ IT-Verfahren Mobile Device
	☒ 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**
☒ Aktenschredder	☒ Einsatz Berechtigungskonzept
☒ Externer Aktenvernichter (DIN 66399)	☒ Minimale Anzahl an Administratoren
☒ Physische Zerstörung von Datenträgern (DIN 66399)	☒ Datenschutztresor
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Verwaltung Benutzerrechte durch Administratoren
☒ 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
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Festlegung von Datenbankrechten

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
☒ Einsatz von VPN	☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Protokollierung der Zugriffe und Abrufe	
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☒ 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
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☒ Manuelle Kontrolle der Protokolle	☒ Vergabe von Rechten zur Eingabe, Änderung, Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☒ 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
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung (Temperatur, Feuchtigkeit)	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse.
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV (unterbrechungsfreie Stromversorgung)	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☒ Schutzsteckdosen Serverraum	☒ Getrennte Partitionen für Betriebssystem und Daten
☒ Datenschutztresor (S60DIS, S120DIS andere geeignete Normen mit Quelldichtung etc.)	
☒ RAID System / Festplattenspiegelung	

☒ Videoüberwachung Serverraum	
☒ Alarmmeldung bei unberechtigtem Zutritt zu dem Serverraum	
☒ Überspannungsschutz	

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

6.1. Datenschutzmaßnahmen

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf / Berechtigung (Intranet)	☒ Interner Datenschutzbeauftragter
☒ Sicherheitszertifizierung nach ISO 22237	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet.
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
	☒ Interner Informationssicherheitsbeauftragter
	☒ Die Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt (DSFA)
	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen vorhanden

6.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	**Organisatorische Maßnahmen**

☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen
☒ Intrusion Prevention System (IPS)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvor- fällen und Datenpannen

6.3. Datenschutzfreundliche Voreinstellungen

Privacy by design / privacy by default

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung des Widerrufrechts 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**
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf

	Datenschutz und Datensicherheit)
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln oder anderer Garantien
	☒ Schriftliche Weisungen (E-Mail, Ticket) an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ 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.