Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der
datatronic Software AG

Stand: 06.10.2021

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.

Die oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen.

Dokumentenverantwortlicher: Pascal Bühler (Vorstand)

Freigegeben am: 06.10.2021

Inhaltsverzeichnis

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

1.1. Zutrittskontrolle

Unter dem Begriff Zutrittskontrolle werden Maßnahmen verstanden, die es Unbefugten verwehren, sich den IT-Systemen, Datenverarbeitungsanlagen sowie den vertraulichen Akten und Datenträgern physisch zu nähern.

1.1.1. Technische Maßnahmen	
Maßnahme	Umsetzung
1.1.1.1. Alarmanlage	Alarmanlage sichert Fenster und Türen ab
1.1.1.2. Manuelles Schließsystem	Ja, ist an allen Türen vorhanden
1.1.1.3. Sicherheitsschlösser	Ja, sind an den beiden Eingangstüren vorhanden
1.1.2. Organisatorische Maßnahmen	
Maßnahme	Umsetzung
1.1.2.1. Schlüsselregelung / Liste	Ja, wird von der Personalabteilung verwaltet
1.1.2.2. Empfang / Rezeption / Pförtner	Ja, die Rezeption wird von den Damen der Auftragsabwicklung durchgeführt
1.1.2.3. Besucherbuch / Protokoll der Besucher	Ja, im Eingangsbereich müssen sich Besucher registrieren
1.1.2.4. Besucher in Begleitung durch Mitarbeiter	Ja
1.1.2.5. Sorgfalt bei Auswahl des Wachpersonals	Ja, hier ist ein zertifizierter Sicherheitsdienst beauftragt
1.1.2.6. Sorgfalt bei Auswahl Reinigungsdienste	Ja

1.2. Zugangskontrolle

Unter dem Begriff Zugangskontrolle werden Maßnahmen verstanden, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

1.2.1. Technische Maßnahmen

Maßnahme		Umsetzung
1.2.1.1.	Login mit Benutzername und Passwort	Ja, mit Passwortrichtlinien bezgl. Komplexität, gem. den momentanen Empfehlungen des BSI
1.2.1.2.	Login mit biometrischen Daten	Teilweise / besonders schützenswerte Bereiche werden mit Fingerabdruckscanner ausgestattet
1.2.1.3.	Anti-Viren-Software Server	Ja, Panda-Antivirus im Einsatz
1.2.1.4.	Anti-Virus-Software Clients	Ja, Panda-Antivirus im Einsatz
1.2.1.5.	Firewall	Ja, Securepoint RC 300 im Einsatz
1.2.1.6.	Intrusion Prevention Systeme	Ja, über Firewall
1.2.1.7.	Intrusion Detection Systeme	Ja, über Firewall
1.2.1.8.	Einsatz VPN bei Remote-Zugriffen	Ja, Open-VPN über Firewall
1.2.1.9.	Verschlüsselung von Datenträgern	Ja, über Bitlocker
1.2.1.10.	BIOS Schutz (separates Passwort)	Ja
1.2.1.11.	Automatische Desktopsperre	Ja, über Windows Bildschirmschoner
1.2.1.12.	Verschlüsselung von Notebooks / Tablet	Ja, über Bitlocker

1.2.2. Organisatorische Maßnahmen

Maßnahme		Umsetzung
1.2.2.1.	Verwalten von Benutzerberechtigungen	Ja, über Active Directory
1.2.2.2.	Zentrale Passwortvergabe	Ja, über interne Administration (PIT-Team)
1.2.2.3.	Richtlinie „Sicheres Passwort“	Ja, über PIT-Team
1.2.2.4.	Richtlinie „Löschen / Vernichten“	Ja, kann auf Anfrage zur Verfügung gestellt werden
1.2.2.5.	Anleitung „Manuelle Desktopsperre“	Ja, über PIT-Team

1.3. Zugriffskontrolle

Unter dem Begriff Zugriffskontrolle werden Maßnahmen verstanden, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

1.3.1.	**Technische Maßnahmen**	
Maßnahme		Umsetzung
1.3.1.1.	Externer Aktenvernichter (DIN 32757)	Ja, wird über Rhenus-Becker GmbH organisiert
1.3.1.2.	Physische Löschung von Datenträgern	Ja, durch komplexes überschreiben bzw. mechanische Zerstörung
1.3.1.3.	Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Ja, in der Sage ERP-Software und in der Sage HR-Software wird ein Mutationsprotokoll mitgeführt.
1.3.2.	**Organisatorische Maßnahmen**	
Maßnahme		Umsetzung
1.3.2.1.	Einsatz Berechtigungskonzepte	Ja, in der Sage ERP-Software und in der Sage HR-Software, sowie Sage CRM werden Berechtigungen auf Systemebene vergeben. Im Netzwerk erfolgt die User-Verwaltung über Active Directory
1.3.2.2.	Minimale Anzahl an Administratoren	Ja, drei Administratoren teilen sich die Aufgaben
1.3.2.3.	Datenschutztresor	Ja, im Vorstandsbüro vorhanden
1.3.2.4.	Verwaltung Benutzerrechte durch Administratoren	Ja

1.4. Trennungskontrolle

Unter dem Begriff Trennungskontrolle werden Maßnahmen verstanden die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

1.4.1. Technische Maßnahmen		
Maßnahme		Umsetzung
1.4.1.1.	Trennung von Produktiv- und Testumgebung	Ja, die Produktivumgebung besteht aus einem Windows 2-Knoten-Cluster sowie einem Backup-Server und einem HR-Server. Die Testumgebung ist auf Basis von VM-Ware vSphere auf 2 Servern realisiert. Außerdem existiert ein Domänencontroller-Server.
1.4.1.2.	Physikalische Trennung (Systeme / Datenbanken / Datenträger)	Ja, läuft auf unterschiedlichen virtuellen Maschinen
1.4.1.3.	Mandantenfähigkeit relevanter Anwendungen	Ja, alle Sage-Anwendungen sind Mandantenfähig
1.4.2. Organisatorische Maßnahmen		
Maßnahme		Umsetzung
1.4.2.1.	Steuerung über Berechtigungskonzept	Ja, in der Sage ERP-Software und in der Sage HR-Software, sowie Sage CRM werden Berechtigungen auf Systemebene vergeben. Im Netzwerk erfolgt die User-Verwaltung über Active Directory
1.4.2.2.	Festlegung von Datenbankrechten	Ja, über Benutzerverwaltung im MS-SQL-Server

1.5. Weitergabekontrolle

Unter dem Begriff Weitergabekontrolle werden Maßnahmen verstanden die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur kontrolliert und dokumentiert weitergegeben werden.

1.5.1. Technische Maßnahmen		
Maßnahme		Umsetzung
1.5.1.1.	Einsatz von VPN	Ja, über Securepoint RC-300 Firewall
1.5.1.2.	Protokollierung der Zugriffe und Abrufe	Ja, über die Applikation POPcon, die die Emails beim Provider abholt und an den Exchange-Server überträgt
1.5.1.3.	Bereitstellung über verschlüsselte Verbindungen wie sftp, https	Ja, über Sub-Domains beim Internet-Provider und den Reverse-Proxy der Firewall

1.6. Eingabekontrolle

Unter dem Begriff Eingabekontrolle werden Maßnahmen verstanden die feststellen, wer personenbezogene Daten in Systeme eingegeben, geändert oder entfernt hat und die die Überprüfbarkeit dessen gewährleisten.

1.6.1. Technische Maßnahmen

Maßnahme		Umsetzung
1.6.1.1.	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Ja, über das Mutationsprotokoll in den Sage-Anwendungen
1.6.1.2.	Manuelle oder automatisierte Kontrolle der Protokolle	Manuell

1.6.2. Organisatorische Maßnahmen

Maßnahme		Umsetzung
1.6.2.1.	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)	Ja, die Nachvollziehbarkeit ist über den angemeldeten Benutzer im Mutationsprotokoll gegeben
1.6.2.2.	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	Ja, wird über die Sage Administration verwaltet
1.6.2.3.	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden	Ja, die Mutationsprotokolle werden in der MS-SQL-Datenbank dauerhaft gespeichert
1.6.2.4.	Klare Zuständigkeiten für Löschungen	Ja, durch das PIT-Team

2. Verfügbarkeit (Art.32 Abs. 1 lit. b DSGVO)

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

2.1. Verfügbarkeitskontrolle

Unter dem Begriff Verfügbarkeitskontrolle werden Schutzmaßnahmen gegen einen zufälligen Verlust oder eine zufällige Zerstörung von elektronischen Daten, Akten und Datenträgern verstanden.

2.1.1. Technische Maßnahmen		
Maßnahme		Umsetzung
2.1.1.1.	Feuer- und Rauchmeldeanlagen	Ja
2.1.1.2.	Feuerlöscher Serverraum	Ja
2.1.1.3.	Serverraumüberwachung Temperatur und Feuchtigkeit	Ja
2.1.1.4.	Serverraum klimatisiert	Ja
2.1.1.5.	USV	Ja
2.1.1.6.	Schutzsteckdosenleisten Serverraum	Ja
2.1.1.7.	Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	Ja
2.1.1.8.	RAID System / Festplattenspiegelung	Ja
2.1.2.	**Organisatorische Maßnahmen**	
Maßnahme		Umsetzung
2.1.2.1.	Backup & Recovery-Konzept (ausformuliert)	Ja, mit Veeam-Backup & Replication. Sicherung erfolgt nach dem 3-2-1 Prinzip, wobei ein Datenträger der Wochensicherung außer Haus aufbewahrt wird.
2.1.2.2.	Kontrolle des Sicherungsvorgangs	Ja, durch PIT-Team
2.1.2.3.	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse	Ja, durch PIT-Team
2.1.2.4.	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums	Ja, in einem Datenschutz-Tresor
2.1.2.5.	Keine sanitären Anschlüsse im oder oberhalb des Serverraums	Ja
2.1.2.6.	Getrennte Partitionen für Betriebs-systeme und Daten	Ja

3. Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

3.1. Datenschutz-Management

Das Datenschutzmanagementsystem ist neben anderen Managementsystemen Teil der Gesamtorganisation. Mit dem DSMS werden die Datenschutzgrundsätze und Einzelanforderungen aus DSGVO, BDSG und anderen Datenschutzgesetzen strukturiert zusammengeführt und in die Unternehmensorganisation überführt.

3.1.1. Technische Maßnahmen	
Maßnahme	Umsetzung
3.1.1.1. Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Ja, VPN-Zugänge werden durch PIT-Team kontrolliert. Die Alarmanlage wird lt. Wartungsvertrag von einem externen Dienstleister regelmäßig kontrolliert.

3.1.2. Organisatorische Maßnahmen	
Maßnahme	Umsetzung
3.1.2.1. Interner / externer Datenschutzbeauftragter	Ja, ein externer Datenschutzbeauftragter ist bestellt.
3.1.2.2. Mitarbeiter geschult und auf Vertraulichkeit verpflichtet	Ja, die Mitarbeiter werden regelmäßig geschult.
3.1.2.3. Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich	Ja, die Mitarbeiter werden regelmäßig sensibilisiert.
3.1.2.4. Interner / externer Informationssicherheitsbeauftragter	Ja
3.1.2.5. Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt	Ja
3.1.2.6. Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach	Ja
3.1.2.7. Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden	Ja
3.1.2.8. Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)	Ja
3.1.2.9. Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen	Ja
3.1.2.10. Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen	Ja

3.1.2.11. Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen	Ja

3.2. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Durch technische und organisatorische Maßnahmen wird sichergestellt, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden. Dies gilt insbesondere für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

3.2.1. Technische Maßnahmen	
Maßnahme	Umsetzung
3.2.1.1. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	Ja
3.2.1.2. Einfache Ausübung des Widerrufrechts des Betroffenen	Ja
3.2.2. Organisatorische Maßnahmen	
Maßnahme	Umsetzung
Keine	

3.3. Auftragskontrolle (Auslagerung an Dritte)

Unter dem Begriff Auftragskontrolle werden Maßnahmen verstanden die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

3.3.1. Technische Maßnahmen

Maßnahme	Umsetzung
Keine	

3.3.2. Organisatorische Maßnahmen

Maßnahme		Umsetzung
3.3.2.1.	Vorherige Prüfung der vom Auftrag-nehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation	Ja
3.3.2.2.	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit	Ja
3.3.2.3.	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln	Ja
3.3.2.4.	Schriftliche Weisungen an den Auftragnehmer	Ja
3.3.2.5.	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis	Ja
3.3.2.6.	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht	Ja
3.3.2.7.	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer	Ja
3.3.2.8.	Regelung zum Einsatz weiterer Sub-unternehmer	Ja
3.3.2.9.	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	Ja