Technische und organisatorische Maßnahmen des Auftragnehmers

Zur Gewährleistung von Datenschutz und Datensicherheit

actiware®
CONSULTING

Autor: ACTIWARE GmbH

Version: 3_3

Stand: 01.09.22

Inhaltsverzeichnis

1 Gegenstand der technischen und organisatorischen Maßnahmen 2
2 Vertraulichkeit 2
2.1 Zutrittskontrolle 2
2.2 Zugangskontrolle 3
2.4 Zugriffskontrolle 4
2.5 Trennungskontrolle 4
2.6 Pseudonymisierung 5
3 Integrität 6
3.1 Weitergabekontrolle 6
3.2 Eingabekontrolle 6
4 Verfügbarkeit und Belastbarkeit 7
4.1 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit 7
5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 8
5.1 Datenschutz-Management 8
5.2 Incident-Response-Management 9
5.3 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen 9
5.4 Auftragskontrolle 10

1 Gegenstand der technischen und organisatorischen Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten und zu verbessern hat. Ziel ist die Gewährleistung der **Vertraulichkeit, Integrität, Belastbarkeit und Verfügbarkeit** der im Auftrag verarbeiteten Informationen.

2 Vertraulichkeit

Gemäß Artikel 32 Abs. 1 lit. b DS-GVO.

2.1 Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Gebäudesicherung ▪ Pforte ▪ Außerhalb der Bürozeiten verschlossene Außentüren	▪ Pforte während Bürozeiten mit Empfangspersonal besetzt
▪ Sicherung der Räume ▪ Sicherheitsschlösser ▪ Schlüsselverwaltung	▪ Schlüsselliste
▪ Sicherheitsbereiche mit gesonderter Zutrittsberechtigung und Zutrittskontrolle ▪ Serverraum	▪ Vergabe der Schlüssel nach dem Least Privilege Prinzip ▪ Arbeitsanweisung zum Verschluss der Büros
▪ Besucherregelung ▪ Abholen an der Pforte ▪ Aufenthalt nur in gesonderten Räumen ▪ Bewegen nur in Begleitung	▪ Besucherregelung ▪ Abholen an der Pforte ▪ Aufenthalt nur in gesonderten Räumen ▪ Bewegen nur in Begleitung

2.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Zugang zu Rechnern/Systemen (Authentifizierung) ▪ Benutzerkennung mit Passwort	▪ Passwortregeln laut Passwortkonzept ▪ Wechsel alle 90 Tage ▪ Mindestens 10 Zeichen lang ▪ Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen. ▪ Das Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten: - Großbuchstaben (A bis Z) - Kleinbuchstaben (a bis z) - Zahlen zur Basis 10 (0 bis 9) - Nicht alphabetische Zeichen (zum Beispiel !, $, #, %)
▪ Passworthistorie	▪ Vermeiden von Trivialpasswörtern ▪ Kenntnisnahme vermeiden
	▪ Regelung zur Speicherung in Passworttresoren
▪ Firewall-Appliance zum Schutz der Netzwerkinfrastruktur mit Updateservice	
▪ Windows-Firewall auf Servern	▪ Regelmäßige Regel Anpassung durch die Administration
▪ Client-Firewall Bitdefender Endpoint Security Tools mit Updateservice	
	▪ Regelmäßige Prüfung der Zugriffsprotokolle
▪ Festplattenverschlüsselung von Notebooks nach dem Stand der Technik	

2.4 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Technische Maßnahmen	Organisatorische Maßnahmen

▪ Benutzerkennung nach Berechtigungs-konzept mit Passwort nach Passwort-Konzept s. o.	▪ Berechtigungskonzept
	  ▪ Least Privilege Prinzip
	  ▪ Regelmäßige Prüfung der Berechtigungen
	  ▪ Zeitliche Beschränkungen hoch sensibler Zugänge
	  ▪ Berechtigungen werden durch die Administration aufgrund schriftlicher Anweisungen durch die Bereichsleitungen gesetzt

▪ Datenträgerverwaltung	
	▪ Aktenschränke mit sensiblen oder personenbezogenen Daten sind außerhalb der Bürostunden verschlossen
	▪ Clean Desk Policy

2.5 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Trennung von Produktiv- und Testsystemen	
▪ Getrennte Ordnerstrukturen (Auftragsdatenverarbeitung)	
▪ Separate Tables innerhalb von Datenbanken	
▪ Getrennte Datenbanken	
	▪ Berechtigungsstrukturen im Active Directory

2.6 Pseudonymisierung

Gemäß Artikel 32 Abs. 1 lit. a, Art. 25 Abs. 1 DS-GVO.

Maßnahmen, die gewährleisten, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Die zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

Technische Maßnahmen	Organisatorische Maßnahmen
	▪ Eine Pseudonymisierung der Daten ist aufgrund des Umfangs und der Art der Datenverarbeitung standardmäßig nicht vorgesehen, wird aber im Bedarfsfall umgesetzt.

3 Integrität

Gemäß Artikel 32 Abs. 1 lit. b DS-GVO.

3.1 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Sicherung bei der elektronischen Übertragung ▪ Verschlüsselung nach dem Stand der Technik ▪ Zertifikatsgestützte VPN ▪ Verwendung sicherer Verschlüsselungstechnologie nach dem Stand in der Firewall	▪ Regelpflege siehe oben
▪ Sicherung beim Transport ▪ Verschlüsselung nach dem Stand der Technik ▪ Sicherung bei der Übermittlung durch zertifikatsgestützte VPN	
▪ Zertifizierte Datenvernichtung nach DIN-Norm 66399, der Schutzklasse 3 (höchster Schutzbedarf) und der Sicherheitsstufe H5.	

3.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Protokollierung	
▪ Benutzeridentifikation	
▪ Berechtigungssystem laut Berechtigungskonzept	
▪ Transkriptionsprotokolle	
	▪ Wichtige Einträge in Akten mit Handzeichen versehen

4 Verfügbarkeit und Belastbarkeit

Gemäß Artikel 32 Abs. 1 lit. b und c DS-GVO.

4.1 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

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

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Brandschutzmaßnahmen ▪ Überwachte Einhaltung der Brandschutzvorschriften ▪ Generelles Rauchverbot	
▪ Überspannungsschutz	
▪ Unterbrechungsfreie Stromversorgung ○ Regelmäßiger Selbsttest	
▪ Schutz gegen Wasser	
▪ Klimaanlage mit regelmäßiger Wartung	
▪ RAID (Festplattenspiegelung)	
▪ Backup	▪ Sicherungskonzept
▪ Desaster Recovery	▪ Vollständige Datensicherung, die es ermöglicht, auch bei Totalverlust der Echt- und Backup-Systeme in angemessener Zeit den Betrieb auf Notfall-Hardware (z.B. Containersysteme) weiterführen zu können.
▪ Virenschutzkonzept	
▪ Schutz vor Diebstahl durch verschlossene Serverräume und Netzwerkschränke	

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Gemäß Artikel 32 Abs. 1 lit. d DS-GVO; Artikel 25 Abs. 1 DS-GVO.

5.1 Datenschutz-Management

Die Datenschutz-Grundverordnung bringt für Unternehmen umfassende Nachweispflichten mit sich (sog. „accountability"). Sinn dieses Verfahrens ist es, einen kontinuierlichen Verbesserungsprozess zu etablieren. Im Rahmen dieses Verfahrens werden die technischen und organisatorischen Maßnahmen erst erdacht und geplant („plan"), im „Kleinen Kreis" getestet („do"), die Wirksamkeit überprüft („check"), gegebenenfalls angepasst und dann im „Großen" eingeführt („act"). Dies schließt regelmäßige Schulungen der Mitarbeiter ein.

Technische Maßnahmen	Organisatorische Maßnahmen
	▪ Umsetzung von Schulungsmaßnahmen nach entsprechender Schulungsplanung
	▪ Umsetzung der Grundsätze Datenschutz und technische und organisatorische Maßnahmen
	▪ Verpflichtung auf die Schweigepflicht über Betriebs- und Geschäftsgeheimnisse und die DSGVO
	▪ Verpflichtung auf das Fernmeldegeheimnis und ggf. weitere Schweigepflichten
	▪ Vertreter für alle betriebsnotwendigen Aufgaben/Funktionen sind definiert und festgelegt
	▪ Regelmäßige Datenschutzaudits
	▪ Sicherstellung von regelmäßiger Auswertung der Protokolle der Zugriffe auf personenbezogene Daten durch interne Audits
	▪ Unregelmäßigkeiten (insbesondere Logins und Zugriffsversuche) werden dokumentiert und für einen Zeitraum von 12 Monaten ab Beendigung des Auftrages/Tätigkeit aufbewahrt
	▪ Regelungen und Richtlinien über Betrieb und Abläufe der Datenverarbeitung und Datensicherungsmaßnahmen
	▪ Ordnungsgemäßer Umgang mit Daten, Dateien und Formularen

5.2 Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
	▪ Prozess zur Bearbeitung von Datenschutzvorfällen zur Wahrung der Fristen mit unverzüglicher Benachrichtigung der Betroffenen ▪ Prozess zur Bearbeitung von Betroffenen-Anfragen unter Wahrung der Fristen ▪ Prozess zur Beantwortung von Behörden-Anfragen unter Wahrung der Fristen

5.3 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Gemäß Artikel 25 Abs. 2 DS-GVO.

Datenschutz durch Technikgestaltung: Schon bei der Planung und Gestaltung digitaler Technologien werden datenschutzrechtliche Anforderungen berücksichtigt.

Datenschutz durch datenschutzfreundliche Voreinstellungen ist der Grundsatz, wonach eine Organisation (der Verantwortliche) sicherstellt, dass durch Voreinstellung nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden (ohne Eingreifen des Nutzers).

Privacy By Design und Privacy By Default

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Customizing von Datenfeldern programmieren	▪ Datenschutz durch datenschutzfreundliche Voreinstellungen im Auslieferungseinstellungen
▪ Minimierung der Verarbeitung von personenbezogenen Daten (Anlassbezogen)	
▪ Verschlüsselung nach dem Stand von geheimen personenbezogenen Daten	

5.4 Auftragskontrolle

Ohne entsprechende Weisung des Auftraggebers darf der Auftragnehmer keine Auftragsdatenverarbeitung i.S.d. Art. 28 DS-GVO vornehmen (Beispiele: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen).

Technische Maßnahmen	Organisatorische Maßnahmen
	▪ Sorgfältige Auswahl der Auftragsverarbeiter gem. Art. 28 Abs. 1 mit Abschluss eines AV-Vertrages
	▪ Definierte Weisungsbefugnisse
	▪ Die Weisungen des Verantwortlichen werden vom Auftragsverarbeiter revisionssicher protokolliert und dokumentiert
	▪ Vereinbarung von Kontrollrechten
	▪ Vor-Ort Kontrolle
	▪ Stichprobenprüfung und regelmäßige Überprüfungen
	▪ IT-, Wach-, Reinigungs-, Entsorgungs- und Transportpersonal und andere Dienstleister werden sorgfältig ausgewählt
	▪ Risikobeurteilung