Technische und organisatorische Maßnahmen (TOM) der abl solutions GmbH i. S. d. Art. 32 DS-GVO i. V. m. § 64 BDSG

Stand: 19.12.2022

aufgenommen durch: Datenschutzbeauftragter

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 abl solutions GmbH erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DS-GVO

1.1. Zutrittskontrolle (§ 64 Abs. 3 S.1 Nr. 1 BDSG)

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unteranderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage am Eingang zur Büroeinheit und am Serverraum vorhanden	Schlüsselregelung für digitale und physische Schlüssel
Alarmanlage und Zugangsbeschränkung zum Bürogebäude im Erdgeschoss mit Zeitschaltuhr	Empfang
elektronisches Zugangskontrollsystem	Besucherbuch und Protokollierung der Besucher
Chipkarten / Transpondersysteme	Besucherausweise
elektronische Schließanlage am Eingangsbereich und am Serverraum	Besucher nur in Begleitung durch Mitarbeiter

zusätzliche elektronische Schließsysteme (Einzelbüros und IT-Administration)	Festlegungen für Heimarbeitsplätze: Richtlinie vorhanden

Sicherheitsschlösser bei manuellen Schließsystemen	Sorgfalt bei Auswahl Reinigungsdienste
Schließsystem mit Codesperre zusätzlich für Serverraum	
Sicherheitstüren bei Serverraum und Eingangstüren	
Gebäudeschächte gesichert	
Türen mit Knauf Außenseite (komplettes Gebäude)	
Videoüberwachung des Eingangsbereiches	
keine Wegweiser / Beschilderung zu sensiblen Bereichen	

1.2. Zugangskontrolle (§ 64 Abs. 3 S.1 Nr. 1 BDSG) und Datenträgerkontrolle (§ 64 Abs. 3 S.1 Nr. 2 BDSG)

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Root Passwort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Software-produkte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	**Organisatorische Maßnahmen**
Login mit Benutzername + Passwort (2-Wege-Authentifizierung bei VPN)	Verwalten von Benutzerberechtigungen (restriktiv)
Login mit biometrischen Daten/ Entsperr PIN bei Mobilfunkgeräten	individuelle Benutzerprofile
Anti-Virus-Software für Server	zentrale Passwortvergabe
Anti-Virus-Software für Clients	Passwort-Richtlinie
Firewall Systeme	Löschkonzept

Intrusion Detection System	Richtlinie zur aufgeräumten Arbeitsumgebung („Clean Desk“)

Intrusion Prevention System	Richtlinie zur Informationssicherheit
Mobile Device Management	Mobile Device Policy
Einsatz VPN bei Remote-Zugriffen	Anleitung „Manuelle Desktopsperre“
Verschlüsselung von Datenträgern	
Verschlüsselung von Smartphones	
BIOS Schutz (separates Passwort)	
keine mobilen Speichermedien im Einsatz	
automatische Desktopsperre	
Verschlüsselung von Notebooks / Tablets	
Einsatz von Hash- & Salt-Verfahren	

1.3. Zugriffskontrolle (§ 64 Abs. 3 S.1 Nr. 5 BDSG)

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten, personenbezogenen Daten Zugang haben.

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 der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Aktenschredder (mind. Stufe 4, cross cut)	Einsatz restriktiver Berechtigungskonzepte
Datentonnen vorhanden	minimale Anzahl an Administratoren
externer Aktenvernichter (DIN 66399)	Verwaltung Benutzerrechte durch Administratoren (restriktiv)
physische Löschung von Datenträgern	Regelung der Fernwartung

Datenträgertonne für Entsorgung Hardware-abfälle durch zertifizierten Dienstleister	Fernwartung nur bei Anwesenheit von Mit-arbeitern
systembedingte Protokollierung von Zugrif-fen auf Anwendungen	
VPN	

1.4. Trennungskontrolle (§ 64 Abs. 3 S.1 Nr. 14 BDSG)

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet wer-den können.

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 Testumge-bung	Steuerung über restriktives Berechtigungs-konzept
physische Trennung (Systeme / Datenbanken / Datenträger)	Festlegung von Datenbankrechten
Mandantenfähigkeit relevanter Anwendun-gen	Datensätze sind mit Zweckattributen verse-hen
Logische Mandantentrennung	getrennte Speicherstrukturen (insbesondere Ordner, Datenbanken, Datenbankinstanzen)

1.5. Pseudonymisierung

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten findet in einer Weise statt, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zu-geordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt wer-den und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1. Weitergabekontrolle und Transportkontrolle (§ 64 Abs. 3 S.1 Nr. 8 BDSG)

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	**Organisatorische Maßnahmen**
E-Mail-Verschlüsselung (TLS)	Dokumentation der Datenempfänger
Einsatz von VPN	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Protokollierung der Zugriffe und Abrufe	Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
Papierakten nur bei gesetzlichen Schriftformerfordernis vorhanden	persönliche Übergabe mit Protokoll
Bereitstellung über verschlüsselte Verbindungen (z. B. sftp, https)	Mitarbeiterunterweisung-/Verpflichtung
Nutzung von Signaturverfahren (digitale Signatur)	
Daten, die als „*confidential*“ oder „*highly confidential*“ eingestuft werden, dürfen ausschließlich verschlüsselt über Cryptshare ausgetauscht werden.	

2.2. Eingabekontrolle, Speicherkontrolle (§ 64 Abs. 3 S.1 Nr. 3 BDSG) und Benutzerkontrolle (§ 64 Abs. 3 S.1 Nr. 4 BDSG)

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	**Organisatorische Maßnahmen**
systembedingte Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
Schutz vor Spionage-/Schadsoftware	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines restriktiven Berechtigungskonzepts
Netzwerkzugriffskontrolle	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden (bei Dokumenten, die der gesetzlichen Schriftform erfordern)
Revisionssichere Daten- und Dokumentensicherung	klare Zuständigkeiten für Löschungen (Löschkonzept vorhanden)
	Benutzerzugriffsregelungen nach dem Need-To-Know-Prinzip

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1. Verfügbarkeitskontrolle (§ 64 Abs. 3 S.1 Nr. 13 BDSG), Datenintegrität (§ 64 S.1 Abs. 3 Nr.11 BDSG), Zuverlässigkeit (§ 64 Abs. 3 S.1 Nr. 10 BDSG) und Wiederherstellbarkeit (§ 64 Abs. 3 S.1 Nr. 13 BDSG)

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept
Feuerlöscher für Serverraum	Kontrolle des Sicherungsvorgangs
Spezialfußboden im Serverraum	Testen von Datenwiederherstellungen
Serverraumüberwachung Temperatur und Feuchtigkeit	keine sanitären Anschlüsse im oder oberhalb des Serverraums
Serverraum klimatisiert	Notfallplan
USV (unterbrechungsfreie Stromversor-gung)	getrennte Partitionen für Betriebssysteme und Daten
Schutzsteckdosenleisten Serverraum	vorausschauende Ressourcenplanung
RAID-System / Festplattenspiegelung	Sicherheitskonzepte
Videoüberwachung des Serverraums	Test- und Freigabeverfahren für Hardware und Software
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	keine Beschilderung sensibler Bereiche
Penetrationstests	
Prüfsummenbildung	
Redundante Systeme/Komponenten	
Datensicherung anderer Brand- und Gebäu-deabschnitt	
Brandschutzwände und -tür	

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Informationssicherheits- und Datenschutz-Management im Einsatz	Externer Datenschutzbeauftragter Rechtsanwalt Thomas Costard Rechtsanwaltskanzlei Costard Kanzlei für IT-Recht und Datenschutz EUROCOM Businesspark Lina-Ammon-Straße 9 90471 Nürnberg Telefon: 0911/ 790 30 34 Telefax: 0911/ 790 30 35 E-Mail: info@it-rechtsberater.de Webseite: www.it-rechtsberater.de
Sicherheitszertifizierung nach ISO 27001	Mitarbeiter geschult und auf Vertraulichkeit / Einhaltung der Anforderungen der Datenschutz-Grundverordnung / Fernmeldegeheimnis verpflichtet
Zertifizierung nach ISO 9001	regelmäßige Sensibilisierung der Mitarbeiter: mindestens jährlich
eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird in regelmäßigen Abständen durchgeführt	Informationssicherheitsbeauftragter: Herr Benjamin Becker Office: +49 911 477157-57 E-Mail: benjamin.becker@abl-solutions.com
	Datenschutz-Folgenabschätzung (DS-FA) wird bei Bedarf durchgeführt
	Umsetzung der Informationspflichten nach Art. 13 und 14 DS-GVO
	definierte Prozesse zur Bearbeitung und Unterstützung von Auskunftsanfragen seitens Betroffener ist vorhanden
	Prüfung aller Verarbeitungstätigkeiten auf Einhaltung der Datenschutzgrundsätze durch den Datenschutzbeauftragten
	Einbeziehung des Datenschutzbeauftragten in alle datenschutzrelevanten Bereiche

4.2. 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
Einsatz von Virenscanner und automatischer Aktualisierung	Prozess zum Umgang mit Datenschutzverletzungen und Sicherheitsvorfällen
Einsatz von Spamfilter und regelmäßige Aktualisierung	Richtlinie zum Umgang mit technischen Schwachstellen
Intrusion Prevention System	Einbindung von Datenschutzbeauftragten und Informationssicherheitsbeauftragten in Sicherheitsvorfälle und potenzielle Datenschutzverletzungen
Intrusion Detection System	Dokumentation von Sicherheitsvorfällen und Datenschutzverletzungen via Ticketsystem
	formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenschutzverletzungen: Richtlinie vorhanden

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

data protection by design / data protection by default

Es werden grundsätzlich nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

4.4. Auftragskontrolle (§ 64 Abs. 3 S.1 Nr. 13 BDSG)

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Organisatorische Maßnahmen
vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation im Rahmen einer Zuverlässigkeitsprüfung
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (in Bezug auf Datenschutz und Datensicherheit)
Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standarddatenschutzklauseln
schriftliche Weisungen an den Auftragnehmer
Verpflichtung der Mitarbeiter des Auftragnehmers auf die Einhaltung der Anforderungen der Datenschutz-Grundverordnung
Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftrag-nehmer bei Vorliegen Bestellpflicht
Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
Regelung zum Einsatz weiterer Subunternehmer
Sicherstellung der Vernichtung bzw. Rückgabe von Daten nach Beendigung des Auftrags
Auditierung des Dienstleisters (im Bedarfsfall)