IBS Technology

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

Stand
22.05.2024

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 og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeitgem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

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 unter anderem 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
Automatisches Zugangskontrollsystem	Schlüsselregelung / Liste
Chipschlüssel	Empfang / Rezeption / Pförtner
Türen mit Knauf Außenseite	Besucher in Begleitung durch Mitarbeiter
Regelmäßige Überprüfung und Aktualisierung der Benutzerrechte und Zugriffe in benutzerbasierten Anwendungen (Tickets, Salesforce, Office 365, …)	Sorgfalt bei Auswahl Reinigungsdienste
Multi-Faktor-Authentifizierung	

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, 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 (mit MFA)	Verwalten von Benutzerberechtigungen
Anti-Virus-Software Clients	Erstellen von Benutzerprofilen
Firewall	Richtlinie „Sicheres Passwort"
Einsatz VPN bei Remote-Zugriffen (mit MFA)	Anleitung „Manuelle Desktopsperre"
Gemeinsam genutzte Zugangsdaten verschlüsselt und per Rechtesystem zugänglich	Anleitung „2FA mit Smartphone"
Einsatz von 2-Faktor-Authentifierung (MFA)	Prinzip der minimalen Rechtevergabe

1.3. 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 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 3, cross cut)	Einsatz Berechtigungskonzepte
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Minimale Anzahl an Administratoren
	Verwaltung Benutzerrechte durch Administratoren

1.4. 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
Physikalische Trennung (Systeme / Datenbanken / Datenträger)	Festlegung von Datenbankrechten

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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 technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

1.6. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von personenbezogenen Daten.

Technische Maßnahmen	Organisatorische Maßnahmen
Digitales Berechtigungskonzept (Zugänge innerhalb von IBS per Microsoft Office und CRM per Salesforce ebenfalls kontrolliert durch Microsoft Azure SSO)	Vergabe von Zugriffsberechtigungen je nach Position und Verantwortung

Differenzierte Berechtigungen für lesen, löschen und ändern	Entzug der Berechtigung nach Projekt- oder Beteiligungsabschluss
Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem	Nutzung von getrennten Benutzernamen zwecks klarer Protokollierung
Protokollierung von Zugriffen auf Anwendungen	Verwaltung der Rechte durch Systemadministratoren
Implementierung von Verschlüsselungsmechanismen für sensible Daten und Zugangsdaten	Anzahl der Administratoren auf das „Notwendigste“ reduziert
	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel gemäß BSI

Siehe auch 2.2 Eingabekontrolle.

1.7. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern

Technische Maßnahmen	Organisatorische Maßnahmen
Verschlüsselung von (mobilen) Datenträgern	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
Protokollierung der Vernichtung	Nutzung von getrennten Benutzernamen zwecks klarer Protokollierung
Sichere Aufbewahrung von Datenträgern	

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

2.1. 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. 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
Einsatz von VPN / Sichere VPN-Technologie	Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
Protokollierung der Zugriffe und Abrufe	Dokumente zwecks Unterzeichnung per DocuSign (Protokollierung durch DocuSign)
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	Gesicherte Transportbehälter
E-Mail-Verschlüsselung	Überprüfung der Übermittlungswege (Sender und Empfänger)
	Kontrolle der Datenempfänger und entsprechende Dokumentation dieser Empfänger

2.2. 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. 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

Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Klare Zuständigkeiten für Löschungen
	Regelmäßige Überprüfung der Protokolle und Audits, um die Integrität der Daten sicherzustellen
	Nutzung von Anomalieerkennungstools soweit verfügbar in Anwendungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
Antiviren Schutz auf den Systemen	Cloud-Backup Funktionen
Aktive Firewall in den Betriebssystemen	
Firewall in Router-Systemen	

Die IBS Technology GmbH verfügt über keinerlei Serversysteme. Daten werden primär über die Cloud (Microsoft Office 365 und Salesforce) verwaltet. Hierfür gelten die Datenschutzvereinbarungen und technischen und organisatorischen Maßnahmen der Anbieter.

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

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	Interner Datenschutzbeauftragter, Kontaktdaten: IBS, Eser Esen
	Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
	Regelmäßige Sensibilisierungsmaßnahmen je nach Gesetzeslage und Empfehlung durch das BSI

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
Einsatz von Spamfilter und regelmäßige Aktualisierung	Einbindung von DSB in Sicherheitsvorfälle und Datenpannen

Einsatz von Virenscanner und regelmäßige Aktualisierung	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

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	

4.4. Auftragskontrolle (Outsourcing an Dritte)

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.

Technische Maßnahmen	Organisatorische Maßnahmen
Fernzugriff nur mit VPN mit aktueller Verschlüsselungstechnik und Benutzername und Passwort	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	Schriftliche Weisungen an den Auftragnehmer
	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

IBS Technology GmbH
Ferdinand-Porsche-Str. 11
60386 - Frankfurt am Main
Germany

☎ +49 (0)69 4089 7658
www.ibs-technology.com