audatis®
Datenschutz und Informationssicherheit | CONSULTING

Checkliste: Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen wurden nach §9 BDSG für folgende verantwortliche Stelle getroffen:

Musterstein GmbH
Musterweg 2 – 4
12345 Musterhausen

1. Zutrittskontrolle

Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

	Technische Maßnahmen		Organisatorische Maßnahmen
☐	Alarmanlage	☐	Personenkontrolle beim Pförtne / Empfang
☐	Absicherung von Gebäudeschächten	☐	Protokollierung der Besucher / Besucherbuch
☐	Automatisches Zugangskontrollsystem	☐	Schlüsselregelung / Schlüsselbuch
☐	Biometrische Zugangssperren	☐	Sorgfältige Auswahl von Sicherheitspersonal
☐	Chipkarten- / Transponder-Schließsystem	☐	Tragepflicht von Mitarbeiter- / Gästeausweisen
☐	Lichtschranken / Bewegungsmelder	☐	Videoüberwachung der Zugänge
☐	Manuelles Schließsystem		
☐	Schließsystem mit Codesperre		
☐	Sicherheitsschlösser		

2. Zugangskontrolle

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen
☐	Authentifikation mit Benutzer + Passwort	☐	Benutzerberechtigungen verwalten
☐	Authentifikation mit biometrischen Daten	☐	Erstellen von Benutzerprofilen
☐	Einsatz von Anti-Viren-Software	☐	Passwortvergabe/Passwortregeln
☐	Einsatz von Firewalls	☐	Personenkontrolle beim Pförtner/Empfang
☐	Einsatz von Mobile Device Management	☐	Protokollierung der Besucher/Besucherbuch
☐	Einsatz von VPN-Technologie	☐	Schlüsselregelung/Schlüsselbuch
☐	Gehäuseverriegelungen	☐	Sorgfältige Auswahl von Reinigungspersonal
☐	Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)	☐	Sorgfältige Auswahl von Sicherheitspersonal
☐	Verschlüsselung von Datenträgern		
☐	Verschlüsselung von Smartphones		

3. Zugriffskontrolle

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.

	Technische Maßnahmen		Organisatorische Maßnahmen
☐	Einsatz von Aktenvernichtern	☐	Anzahl der Administratoren auf das »Notwendigste« reduzieren
☐	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)	☐	Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
☐	Physische Löschung von Datenträgern vor deren Wiederverwendung	☐	Erstellen eines Berechtigungskonzepts
☐	Protokollierung der Vernichtung von Daten	☐	Passwortrichtlinie inkl. Länge und Wechsel
☐	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☐	Sichere Aufbewahrung von Datenträgern
☐	Verschlüsselung von Datenträgern	☐	Verwaltung der Benutzerrechte durch Systemadministratoren
☐	Verschlüsselung von Smartphones		

4. Weitergabekontrolle

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
☐	Einrichtungen von VPN-Tunneln	☐	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
☐	E-Mail-Verschlüsselung	☐	Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
☐	Sichere Transportbehälter/-verpackungen	☐	Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
		☐	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

5. Eingabekontrolle

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
☐	Protokollierung der Eingabe, Änderung und Löschung von Daten	☐	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
		☐	Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
		☐	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

6. Auftragskontrolle

Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen
		☐	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
		☐	Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
		☐	Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungs-vertrag) i.S.d. § 11 Abs. 2 BDSG
		☐	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
		☐	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
		☐	Vertragsstrafen bei Verstößen
		☐	Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
		☐	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren

7. Verfügbarkeitskontrolle

Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

	Technische Maßnahmen		Organisatorische Maßnahmen
☐	Feuerlöschgeräte in Serverräumen	☐	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
☐	Feuer- und Rauchmeldeanlagen	☐	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
☐	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☐	Erstellen eines Backup- & Recoverykonzepts
☐	Klimaanlage in Serverräumen	☐	Erstellen eines Notfallplans
☐	Schutzsteckdosenleisten in Serverräumen	☐	Testen von Datenwiederherstellung
☐	Unterbrechungsfreie Stromversorgung (USV)	☐	Serverräume nicht unter sanitären Anlagen
		☐	In Hochwassergebieten: Serverräume über der Wassergrenze

8. Trennungsgebot

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen
☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	☐	Erstellung eines Berechtigungskonzepts
☐	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	☐	Festlegung von Datenbankrechten
☐	Trennung von Produktiv- und Testsystem	☐	Logische Mandantentrennung (softwareseitig)
☐	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden	☐	Versehen der Datensätze mit Zweckattributen/Datenfeldern

Mit freundlicher Empfehlung von audatis® Consulting – Datenschutz und Informationssicherheit

Hauptsitz/Büro Ostwestfalen
Wittekindstr. 3 | 32051 Herford
Fon: 05221 85496-90
Fax: 05221 85496-99
E-Mail: info@audatis.de
Internet: www.audatis.de

Büro Rhein-Main-Neckar
Wehrstr. 30 | 69488 Birkenau

Büro Rhein-Ruhr
Wöhlerstr. 16 a | 50823 Köln