

Bundesdatenschutzgesetz (BDSG-alt)

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, 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 dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Art. 32 DSGVO Sicherheit der Verarbeitung (BDSG-neu)

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
 - a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
 - b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
 - c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
 - d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

der

Mustermann GmbH
Musterstr. 123
12345 Musterstadt

1. Zutrittskontrolle

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

- | | |
|--|---|
| <input type="checkbox"/> Alarmanlage | <input type="checkbox"/> Absicherung von Gebäudeschächten |
| <input type="checkbox"/> Automatisches Zugangskontrollsystem | <input type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| <input type="checkbox"/> Schließsystem mit Codesperre | <input type="checkbox"/> Manuelles Schließsystem |
| <input type="checkbox"/> Biometrische Zugangssperren | <input type="checkbox"/> Videoüberwachung der Zugänge |
| <input type="checkbox"/> Lichtschranken / Bewegungsmelder | <input type="checkbox"/> Sicherheitsschlösser |
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- | | |
|---|--|
| <input type="checkbox"/> Zuordnung von Benutzerrechten | <input type="checkbox"/> Erstellen von Benutzerprofilen |
| <input type="checkbox"/> Passwortvergabe | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren |
| <input type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen |
| <input type="checkbox"/> Gehäuseverriegelungen | <input type="checkbox"/> Einsatz von VPN-Technologie |
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.) | <input type="checkbox"/> Sicherheitsschlösser |
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen | <input type="checkbox"/> Verschlüsselung von mobilen Datenträgern |
| <input type="checkbox"/> Verschlüsselung von Smartphone-Inhalten | <input type="checkbox"/> Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |

- | | |
|--|--|
| <input type="checkbox"/> Einsatz von Anti-Viren-Software | <input type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks |
| <input type="checkbox"/> Einsatz einer Hardware-Firewall | <input type="checkbox"/> Einsatz einer Software-Firewall |

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.

- | | |
|---|--|
| <input type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input type="checkbox"/> Verwaltung der Rechte durch Systemadministrator |
| <input type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung | <input type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| <input type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input type="checkbox"/> Protokollierung der Vernichtung |
| <input type="checkbox"/> Verschlüsselung von Datenträgern | |

4. 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.

- | | |
|---|---|
| <input type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input type="checkbox"/> E-Mail-Verschlüsselung | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| <input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen | |

5. 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.

- | | |
|--|--|
| <input type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| <input type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts | |

6. Auftragskontrolle

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

- | | |
|---|--|
| <input type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | <input type="checkbox"/> vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| <input type="checkbox"/> schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG | <input type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG) |
| <input type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt | <input type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| <input type="checkbox"/> Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart | <input type="checkbox"/> laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |
| <input type="checkbox"/> Vertragsstrafen bei Verstößen | |

7. Verfügbarkeitskontrolle

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

- | | |
|---|--|
| <input type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) | <input type="checkbox"/> Klimaanlage in Serverräumen |
| <input type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input type="checkbox"/> Schutzsteckdosenleisten in Serverräumen |
| <input type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input type="checkbox"/> Feuerlöschgeräte in Serverräumen |
| <input type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | <input type="checkbox"/> Erstellen eines Backup- & Recoveryconcept |
| <input type="checkbox"/> Testen von Datenwiederherstellung | <input type="checkbox"/> Erstellen eines Notfallplans |
| <input type="checkbox"/> Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort | <input type="checkbox"/> Serverräume nicht unter sanitären Anlagen |
| <input type="checkbox"/> In Hochwassergebieten: Serverräume über der Wassergrenze | |

8. Trennungsgebot

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

- | | |
|--|---|
| <input type="checkbox"/> physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | <input type="checkbox"/> Logische Mandantentrennung (softwareseitig) |
| <input type="checkbox"/> Erstellung eines Berechtigungskonzepts | <input type="checkbox"/> Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |
| <input type="checkbox"/> Versehen der Datensätze mit Zweckattributen/Datenfeldern | <input type="checkbox"/> Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
| <input type="checkbox"/> Festlegung von Datenbankrechten | <input type="checkbox"/> Trennung von Produktiv- und Testsystem |

XX.XX.XXXX

Datum

Max Mustermann

Verantwortlicher für die Erstellung (in Druckbuchstaben)

Unterschrift des Verantwortlichen