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.*

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

1. Zugangskontrolle

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | Zuordnung von Benutzerrechten |  | Erstellen von Benutzerprofilen |
|  | Passwortvergabe |  | Authentifikation mit biometrischen Verfahren |
|  | Authentifikation mit Benutzername / Passwort |  | Zuordnung von Benutzerprofilen zu IT-Systemen |
|  | Gehäuseverriegelungen |  | Einsatz von VPN-Technologie |
|  | Sperren von externen Schnittstellen (USB etc.) |  | Sicherheitsschlösser |
|  | Schlüsselregelung (Schlüsselausgabe etc.) |  | Personenkontrolle beim Pförtner / Empfang |
|  | Protokollierung der Besucher |  | Sorgfältige Auswahl von Reinigungspersonal |
|  | Sorgfältige Auswahl von Wachpersonal |  | Tragepflicht von Berechtigungsausweisen |
|  | Einsatz von Intrustion-Detection-Systemen |  | Verschlüsselung von mobilen Datenträgern |
|  | Verschlüsselung von Smartphone-Inhalten |  | Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |
|  | Einsatz von Anti-Viren-Software |  | Verschlüsselung von Datenträgern in Laptops / Notebooks |
|  | Einsatz einer Hardware-Firewall |  | Einsatz einer Software-Firewall |

1. 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.*

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

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.*

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

1. 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.*

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

1. Auftragskontrolle

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

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

1. Verfügbarkeitskontrolle

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

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

1. Trennungsgebot

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

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

|  |  |  |
| --- | --- | --- |
| xx.xx.xxxx |  | Max Mustermann |
| Datum |  | Verantwortlicher für die Erstellung (in Druckbuchstaben) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  | Unterschrift des Verantwortlichen |