

MUSTER 4
Technische und organisatorische Maßnahmen

WICHTIGE INFORMATIONEN ZUR NUTZUNG VORAB

1. Dieses MUSTER 4 ist eine Orientierungshilfe. Es stellt ein unverbindliches Beispiel dar und erhebt keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Aussagen orientieren sich an einem kleinen Architekturbüro. Jedes Architekturbüro muss sich individuell mit den Anforderungen des Datenschutzes auseinandersetzen. Die Inhalte des Musters können nicht pauschal übernommen werden, sondern sind entsprechend auf Ihr Architekturbüro anzupassen. Das bedeutet für Sie: Sie müssen klären, welche technischen und organisatorischen Maßnahmen bei Ihnen getroffen werden (müssen) und diese auf dem anliegenden Muster entsprechend ankreuzen. Nichtzutreffende Angaben sind nicht anzukreuzen, fehlende Angaben sind zu ergänzen.
2. Die Bundesarchitektenkammer übernimmt für dieses Muster keine Haftung und keine Gewähr. Dieses Muster ersetzt keine individuelle Rechtsberatung.
3. Zur Auslegung der DSGVO gibt es noch viele offene Fragen. Zudem gibt es regelmäßig neue Gesetzgebungsvorhaben auf europäischer und nationaler Ebene, die eine Anpassung der Datenschutz Compliance in Unternehmen erfordern. Deshalb ist es möglich, dass wir das Muster im Laufe der nächsten Wochen und Monate ändern bzw. anpassen werden. Datenschutzrecht ist kein einmaliges Projekt; Sie müssen sich dauerhaft und regelmäßig damit beschäftigen. Deshalb bitten wir Sie, regelmäßig auf www.architektendatenschutz.de nachzuschauen und unsere Hinweise und Änderungen zu beachten.

Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen wurden getroffen:

A. Zutrittskontrolle

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

1. Technische Maßnahmen

Alarmanlage

Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)

Schlüsselregelung (Schlüsselverwaltung, Schlüsselausgabe etc.)

Sicherheitsschlösser

2. Organisatorische Maßnahmen

Protokollierung der Besucher / Besucherbuch

Schlüsselregelung / Schlüsselbuch

Videoüberwachung der Zugänge

B. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (insbesondere durch den Einsatz von Verschlüsselungsverfahren, die dem jeweils aktuellen Stand der Technik entsprechen).

1. Technische Maßnahmen

Authentifikation mit Benutzer + Passwort

Aktuelle Anti-Viren-Software

Aktuelle Firewall

VPN-Technologie

Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung

E-Mail-Verschlüsselung

Verschlüsselung von Datenträgern

2. Organisatorische Maßnahmen

Zuordnung und Verwaltung der Benutzerberechtigungen

Erstellen von Benutzerprofilen

Passwortvergabe / Passwortregeln (inkl. regelmäßigen Änderungen)

Automatische Sperrung des Arbeitsplatzes

Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen

Protokollierung von Übermittlungen

Erstellung einer Übersicht von Datenträgern, Aus- und Eingang

C. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1. Technische Maßnahmen

Einsatz von Aktenvernichter

Einsatz von Datenträgervernichter

Einsatz von Dienstleistern unter Beachtung von DIN 66399

Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

Verschlüsselung von Datenträgern

Verschlüsselung von Smartphones

2. Organisatorische Maßnahmen

Verwaltung der Benutzerrechte durch System-Administrator

Anzahl der Administratoren auf das "Notwendigste" reduziert

Erstellung eines Berechtigungsplans

Passwortrichtlinie inkl. Länge und Wechsel

Sichere Aufbewahrung von Datenträgern

Ordnungsgemäße Vernichtung von Datenträgern

Löschungskonzept für Daten

Protokollierung der Vernichtung von Daten

Protokollieren von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

D. 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 werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

1. Technische Maßnahmen

Einrichtungen von VPN-Tunneln

E-Mail-Verschlüsselung

2. Organisatorische Maßnahmen

Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

Erstellung einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

E. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind und Vertragsdaten jederzeit ihrem Ursprung zugeordnet werden können (Authentizitätskontrolle).

1. Technische Maßnahmen:

Protokollierung der Eingabe, Änderung und Löschung von Daten

2. Organisatorische Maßnahmen:

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

Protokollauswertungsroutinen/-systeme vorhanden

Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

F. Auftragskontrolle

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

1. Technische Maßnahmen:

2. Organisatorische Maßnahmen:

Vorhandene Vereinbarungen zur Auftragsverarbeitung

Kontrolle der Vertragsausführung

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

G. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies umfasst insbesondere die Gewährleistung der Belastbarkeit der Systeme und Dienste, die Verwahrung der Vertragsdaten nach den Grundsätzen einer ordnungsgemäßen Datensicherung sowie regelmäßige Datensicherungen, einschließlich regelmäßiger Back-ups, im erforderlichen Umfang.

1. Technische Maßnahmen:

Unterbrechungsfreie Stromversorgung (USV)

Überspannungsschutz

Schutz gegen Umwelteinflüsse (Sturm, Wasser)

Feuer- und Rauchmeldeanlagen

Feuerlöscher in Serverraum

Klimaanlage in Serverraum

Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverraum

Schutzsteckdosen in Serverraum

2. Organisatorische Maßnahmen:

Erstellen eines Notfallplans

Alarmmeldung bei unberechtigten Zutritten zu Serverraum

Testen von Datenwiederherstellung

Serverraum nicht unter sanitären Anlagen

Serverraum über Wassergrenze (in Hochwassergebiet)

Erstellen eines Backup- (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort) und Recoverykonzepts

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Spiegelung von Festplatten (z. B. RAID-Verfahren)

H. Trennungsgebot

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

1. Technische Maßnahmen:

Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Bei pseudonymisierten Daten: Trennung der Zuordnungsdaten und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

2. Organisatorische Maßnahmen:

Festlegung Technologie von Datenbankrechten

Festlegung von Datenbankrechten

Erstellung eines Berechtigungskonzepts

I. Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

1. Technische Maßnahmen:

Zulässigkeit eines Datentransfers in Drittländer ist gegeben

2. Organisatorische Maßnahmen

Führung eines Verarbeitungsverzeichnisses

Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

J. Allgemeine Maßnahmen

Ist ein betrieblicher Datenschutzbeauftragter bestellt?

Nein

Ja

Name: _____

Funktion: _____

E-Mail: _____

Telefon: _____

Mitarbeiter wurden über Datenschutzrecht und Datensicherheit geschult:

Am: _____/Von: _____

Alle Mitarbeiter sind auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.

Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z.B. technisch unterstützt oder durch Externe).

Ein Datensicherheitskonzept / Informationssicherheitsmanagement ist vorhanden.

Ein Datenschutzkonzept ist vorhanden.

Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am _____ und Bestätigung s. Anlage _____).

Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am _____ und Bestätigung s. Anlage _____).

Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.