Technische und organisatorische Massnahmen (TOM)

Umsetzung der gesetzlichen Vorgaben nach DS-GVO Art.32 /BDSGneu

Hier können Sie sich einen Überblick verschaffen, welche technischen und organisatorischen Maßnahmen wir zum Schutz Ihrer Daten getroffen haben.

Vertraulichkeit

a. Zutrittskontrolle

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

- Es erfolgt eine ständige Zutrittskontrolle für die Büroräumlichkeiten durch die im Eingangsbereich sitzenden Kollegen.
- Eine differenzierte Zutrittsregelung erlaubt Mitarbeitern nur den Zutritt zu bestimmten Unternehmensräumlichkeiten.
- Unbefugten und insbesondere externen Personen ist der Zugang grundsätzlich verwehrt. Er kann erst nach ausdrücklicher Freigabe durch einen Mitarbeiter unter Benennung des Anlasses ermöglicht werden.
- Außerhalb der Geschäftszeiten werden die Büroräume und Fenster verschlossen.
- Es existieren sowohl Sicherheitsschlösser wie auch eine Schlüsselregelung.
- Die Server stehen in gesicherten Räumen.
- Datensicherungen auf portablen Sicherungsmedien (z.B. CD/DVD, Bänder) sind in zutrittsgeschützten Räumen oder in verschlossenen Schränken untergebracht.
- Soweit Datenverarbeitungsanlagen (z.B. Notebooks) oder Speichermedien (z.B. USB-Sticks) außerhalb der Büroräume eingesetzt werden, sind diese persönlich mitzuführen und/ oder in gesicherten Räumen oder verschlossenen Schränken aufzubewahren.

b. Zugangskontrolle

Unbefugten ist der Zugang und damit die Nutzung von Datenverarbeitungssystemen zu verwehren.

- Zur Nutzung der Systeme sind individuelle Anmeldedaten wie Benutzername und Passwort notwendig.
- Es existiert eine Passwort-Richtlinie.
- Nicht mehr benötigte Zugangsberechtigungen werden zeitnah entzogen.
- Es werden Logs der Benutzeranmeldungen erstellt. Die Arbeitsplatzrechner sind durch Anti-Viren-Software geschützt.
- Das Reinigungspersonal wird sorgfältig ausgesucht und durch den Arbeitgeber auf den Datenschutz verpflichtet.

c. 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.

- Es sind ausschließlich Personen, die mit der Erhebung, Nutzung und Verarbeitung der Daten im Rahmen der vereinbarten Auftragsverarbeitung betraut sind, berechtigt, die Daten zu lesen, zu kopieren, zu ändern oder zu löschen. In diesem Zusammenhang bestehen klare Regelungen zur Vergabe von Zugriffsberechtigungen, die einen differenzierten Zugriff (lesen, ändern, löschen) berücksichtigen und den Zugriff auf den verschiedenen Ebenen regeln.
- Papierunterlagen können beim Verlassen des Arbeitsplatzes vor unbefugter Kenntnisnahme bzw. unbefugtem Zugriff durch die Möglichkeit abschließbarer Schränke bzw. Fächer geschützt werden.
- Eine Firewall schützt Ihre Daten gegen einen Zugriff aus nicht vertrauenswürdigen Netzwerken (z.B. Internet).
- Die technischen Sicherheitseinrichtungen werden regelmäßig auf ihre Wirksamkeit hin geprüft.
- Papierdokumente und mobile Datenspeicher werden in abschließbaren Möbeln aufbewahrt (Clean-Desk-Prinzip).

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

- Im Hinblick auf personenbezogene Daten verschiedener Auftraggeber erfolgt eine logische Trennung der Daten (Mandantenprinzip).

Integrität

a. Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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.

- Die Verwendung von externen Datenträgern (USB-Stick, externe Festplatte, CDs, DVDs) außerhalb der geschützten Unternehmensumgebung ist nur zum Zwecke der Kundenberatung oder für das Halten von Vorträgen/ Präsentationen erlaubt. Externe Datenträger sind in diesen Fällen persönlich mitzuführen und/ oder in gesicherten Räumen oder verschlossenen Schränken aufzubewahren.
- Die datenschutzgerechte Datenvernichtung ist gewährleistet. Bei Papierdokumenten erfolgt sie durch einen Papierreißwolf gemäß dem vorgeschriebenen Schutzniveau. Bei Datenträgern (z.B. defekte Festplatte) erfolgt sie physikalisch.

b. 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.

- Um zu gewähren, dass im Nachhinein geprüft werden kann, ob, von wem und wann personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, erfolgt eine entsprechende Protokollierung auf Basis der individuellen Log-In-Daten der Nutzer.
- Differenzierte Zugriffsberechtigungen und Schreibschutzfunktionen der verwendeten Softwarelösungen verhindern, dass unbefugte Eingaben, Änderungen oder Löschungen vorgenommen werden können.

Verfügbarkeit und Belastbarkeit

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

- Die Daten sind durch ein Backup-Konzept gegen zufällige Zerstörung oder Verlust geschützt.
- Die Backups werden regelmäßig daraufhin getestet, ob ein reibungsloses Zurücksichern möglich ist.

b. Unverzügliche Wiederherstellbarkeit
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall unverzüglich wiederhergestellt werden können.

- Es existiert ein Konzept für die Wiederherstellung des Geschäftsbetriebs nach einem Notfall.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

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

- Mit Dienstleistern, die in unserem Auftrag personenbezogene Daten verarbeiten oder im Zusammenhang mit ihrer Tätigkeit Einblick und Zugriff auf personenbezogene Daten haben könnten, wird ein Vertrag zur Auftragsverarbeitung geschlossen.
- Aus der Leistungsbeschreibung, die als Grundlage der Auftragsverarbeitung zwischen Auftragnehmer und Auftraggeber vereinbart wird, gehen Art, Umfang und Zweck der Datenverarbeitung hervor.
- Die mit der Umsetzung der Auftragsverarbeitung befassten Mitarbeiter sind über den Leistungsumfang informiert.
- Für die vereinbarte Auftragsverarbeitung werden ggf. Cloud-Lösungen eingesetzt. Die Cloud-Datenkommunikation ist verschlüsselt.