



Technische und Organisatorische Maßnahmen (TOMs)

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt.

In den folgenden Abschnitten werden die aktuellen Sicherheitsmaßnahmen definiert, die der Verantwortliche bei der Verarbeitung zugrunde legt. Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung nach einer Risikobewertung Maßnahmen zu ergreifen, um folgende Zwecke zu erreichen:

- Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle);
- Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle);
- Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle);
- Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle);
- Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle);
- Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle);
- Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle);
- Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);
- Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellung);
- Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Zutrittskontrolle

Unbefugten wird der physische Zugang zu Einrichtungen, Gebäuden und Räumlichkeiten, in denen sich Datenverarbeitungssysteme befinden, die personenbezogenen Daten Betroffener verarbeiten oder nutzen, verwehrt.

Festgelegte Maßnahmen:

- Alle Gebäude werden durch angemessene, dem Stand der Technik und dem gebotenen Schutzbedarf entsprechende Maßnahmen geschützt.
- Gebäude sind durch den Stand der Technik und dem gebotenen Schutzbedarf entsprechende Zutrittskontrollsysteme gesichert.
- Die Vergabe der Zutrittsrechte an die berechtigten Personen erfolgt auf individueller Basis gemäß den Maßnahmen zur System- und Datenzugriffskontrolle. Gäste und Besucher in den Gebäuden müssen sich namentlich anmelden und von autorisierten Mitarbeitern begleitet werden.
- Sowohl die Mitarbeiter, als auch externes Personal müssen einen Ausweis sichtbar zur Identifikation tragen.

Zusätzliche Maßnahmen für Rechenzentren:

- Für Rechenzentren gelten dem Stand der Technik entsprechende Sicherheitsmaßnahmen (Überwachungskameras, Bewegungsmelder und Zugangskontrollmechanismen), um Anlagen und Einrichtungen von Rechenzentren vor dem Zugriff Unbefugter zu schützen. Zu den Systemen und zur

- Infrastruktur der Rechenzentren hat ausschließlich autorisiertes Personal Zugang.
- Der Zutritt von Fremdpersonal in Rechenzentren erfolgt nur in Begleitung von autorisiertem Personal.

Systemzugriffskontrolle

Datenverarbeitungssysteme, die zur Bereitstellung der vereinbarten Verarbeitung genutzt werden, werden vor einer nicht autorisierten Nutzung geschützt.

Festgelegte Maßnahmen:

- Die Gewährung des Zugriffs auf Systeme zur Speicherung und Verarbeitung personenbezogener Daten Betroffener erfolgt mittels eines mehrstufigen Rollen- und Berechtigungssystems. Das Vergeben und Entziehen der Rollen wird durch einen sicheren und festgelegten Prozess geregelt.
- Alle Nutzer greifen über eine eigene eindeutige Benutzerkennung auf die Systeme zu. Gruppenberechtigungen sind nicht zulässig.
- Der Umgang mit und die Festlegung von Kennwörtern ist in einer Kennwortrichtlinie festgelegt und die Weitergabe von Kennwörtern ist untersagt. Alle Kennwörter müssen den in der Kennwortrichtlinie festgelegten Mindestbedingungen erfüllen und werden in verschlüsselter Form gespeichert. Kennwortänderungen erfolgen bedarfsweise. Jeder Computer verfügt über einen kennwortgeschützten Bildschirmschoner.
- Das Unternehmensnetzwerk ist durch, dem Stand der Technik entsprechende Netzwerksicherheitsmaßnahmen (Firewalls, Virenschutz etc.) geschützt.
- Das Sicherheitspatch-Management gewährleistet die Anwendung entsprechender regelmäßiger Sicherheits-Updates.

Datenzugriffskontrolle

Personen, die zur Nutzung von Datenverarbeitungssystemen berechtigt sind, erhalten nur Zugriff auf die Personenbezogenen Daten, für die sie Zugriffsrechte besitzen, und personenbezogene Daten Betroffener dürfen bei der Verarbeitung, Nutzung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Festgelegte Maßnahmen:

- Es wird eine Klassifikation von Daten durchgeführt. Personenbezogene Daten Betroffener erhalten zumindest den gleichen Schutz wie „vertrauliche“ Informationen im Sinne der Datenklassifikation.
- Der Zugriff auf persönliche, vertrauliche oder sensible Informationen wird nur bei entsprechender Notwendigkeit gewährt („Need-to-know“-Prinzip). Mit anderen Worten, Mitarbeitern oder Dienstleistern wird der Zugriff nur auf diejenigen Informationen gewährt, die sie zur Erledigung ihrer Arbeitsaufgabe benötigen.
- Alle produktiven Serversysteme werden in Rechenzentren oder gleichwertig gesicherten Serverräumen betrieben. Die Sicherheitsmaßnahmen zum Schutz der Anwendungen zur Verarbeitung personenbezogener, vertraulicher und sonstiger sensibler Daten werden in regelmäßigen Abständen geprüft. Zu diesem Zweck werden interne und externe Sicherheitsüberprüfungen und Penetrationstests durchgeführt.
- Die Installation nicht genehmigter eigener Software oder sonstiger Software ist nicht gestattet.
- Durch ein entsprechendes Löschkonzept wird die Löschung nicht mehr benötigter Daten geregelt.
- Die betriebenen IT-Systeme und Infrastrukturen werden in Bezug auf Vertraulichkeitsrisiken zyklisch evaluiert und das Ergebnis der Evaluierung entsprechend berichtet.

Datenübertragungskontrolle

Die Datenübertragungskontrolle gewährleistet durch geeignete Maßnahmen (Verschlüsselung etc.), dass bei der Übertragung oder Speicherung personenbezogener Daten, außerhalb der Erbringung der vertragsgemäßen Verarbeitung nicht unbefugt verarbeitet werden kann.

Festgelegte Maßnahmen:

- Personenbezogene Daten Betroffener werden bei der externen Übermittlung mit demselben Schutzniveau wie bei einer internen Übermittlung geschützt.
- Für die Übertragung der Daten zwischen dem Verantwortlichen und dem Auftragsverarbeiter werden angemessene Sicherheitsmaßnahmen für die übertragenen personenbezogenen Daten Betroffener im Rahmen einer Vereinbarung festgelegt.

Dateneingabekontrolle

Es sind entsprechende, in den verwendeten IT-Systemen verfügbaren Möglichkeiten vor zu sehen, die es ermöglichen im Nachhinein zu untersuchen und festzustellen, ob und von wem personenbezogene Daten Betroffener erfasst, modifiziert oder gelöscht wurden.

Festgelegte Maßnahmen:

- Es wird ausschließlich autorisierten und zum Datenschutz verpflichtete Personen im Rahmen ihrer Arbeitsaufgabe der Zugriff auf personenbezogene Daten Betroffener erlaubt.

Auftragskontrolle

Der Auftragsverarbeiter verarbeitet ausschließlich personenbezogene Daten in Übereinstimmung mit der jeweiligen Vereinbarung und Weisungen des Verantwortlichen.

Festgelegte Maßnahmen:

- Das Unternehmen führt in angemessenen Zyklen Kontrollen durch, um die Einhaltung der Verträge zwischen Verantwortlichen und Auftragsverarbeitern oder anderen Serviceanbietern und IT-Dienstleistern zu gewährleisten.
- Sämtliche Mitarbeiter des Auftragsverarbeiters und der Unterauftragsverarbeiter sind schriftlich dem Datenschutz verpflichtet. Mit anderen Serviceanbieter und IT-Dienstleistern ist eine angemessene Vertraulichkeitsverpflichtung auf vertraglicher Basis vereinbart.

Verfügbarkeitskontrolle

Personenbezogene Daten werden vor versehentlicher oder nicht autorisierter Vernichtung oder Verlust geschützt.

Festgelegte Maßnahmen:

- Das Unternehmen verfügt über entsprechende Datensicherungs-Verfahren, um geschäftskritische Verarbeitungen kurzfristig wiederherstellen zu können.
- Im Unternehmen ist im Rechenzentrum ein ausfallsicheres Stromversorgungs-Konzept (USV, Batterien, Generatoren usw.) implementiert, um die Stromversorgung für geschäftskritische Verarbeitungen sicherzustellen.
- Es sind Eventualfallpläne (Business- und Disaster-Recovery-Strategien) ausgearbeitet und werden in angemessenen Zyklen getestet. Das betroffene Personal wird entsprechend geschult.
- Es werden zyklisch die betriebenen IT-Systeme und Infrastrukturen in Bezug auf Verfügbarkeitsrisiken evaluiert und das Ergebnis der Evaluierung entsprechend berichtet.

Trennungskontrolle

Eine Trennung personenbezogener Daten Betroffener, die für unterschiedliche Zwecke bzw. für unterschiedliche Betroffene erfasst werden.

Festgelegte Maßnahmen:

- Es sind technischen Möglichkeiten implementiert, um die Trennung von personenbezogenen Daten Betroffener zu ermöglichen.

Datenintegritätskontrolle

Personenbezogene Daten bleiben während der Verarbeitungstätigkeiten unversehrt, vollständig und aktuell.

Festgelegte Maßnahmen:

- Es wurde zum Schutz vor unautorisierten Änderungen eine mehrere Schichten umfassende Sicherheitsstrategie umgesetzt. Im Einzelnen handelt es sich um:
 - Dem Stand der Technik entsprechende IT-Sicherheitssysteme und -konzepte
 - Externe und interne Penetrationstests
 - Regelmäßige Prüfung der Sicherheitsmaßnahmen durch externe Prüfer
 - Zertifizierung der IT-Systeme und Infrastrukturen

- Standardisierte Verarbeitungsprozesse im IT-Betrieb
- Die betriebenen IT-Systeme und Infrastrukturen werden in Bezug auf Integritätsrisiken zyklisch evaluiert und das Ergebnis der Evaluierung entsprechend berichtet.

Wiederherstellungskontrolle

Personenbezogene Daten werden dem Stand der Technik entsprechend auf Datensicherungssysteme ausgelagert. Dabei wird präzise zwischen Datensicherungs- und Archivsysteme unterschieden. IT-Administratoren sind geschult und ausgebildet, die Datensicherungen dem geforderten Schutz entsprechend wiederherzustellen. Diese Szenarien werden in periodischen Abständen getestet (siehe Maßnahmen Wiederherstellbarkeit).

Festgelegte Maßnahmen:

- Daten werden entsprechend den festgelegten Zyklen gesichert und die Sicherungen dem Stand der Technik entsprechend verwahrt.
- Die Aufbewahrung von Datensicherungen ist im Sinne eines Löschkonzepts und mit Löschzyklen harmonisiert.