Mitgliederinformation

Bundesverband Möbelspedition und Logistik (AMÖ) e.V.

Datenschutzgrundverordnung

Überblick über die Pflichten der Unternehmer nach DSGVO

Durch die Datenschutzgrundverordnung (DSGVO) werden die datenschutzspezifischen Verpflichtungen der Unternehmer deutlich ausgeweitet. Diese sind dazu verpflichtet, die Grundsätze und Regeln der DSGVO einzuhalten. Diese Mitgliederinformation soll Sie über die wesentlichen Pflichten aufklären und bei ihrer Umsetzung unterstützen.

Bearbeitungsstand: 16. Februar 2018

Herausgeber:
Bundesverband Möbelspedition und Logistik (AMÖ) e.V.
65795 Hattersheim / Main, Schulstraße 53
Telefon: (0 61 90) 98 98 13; Telefax: (0 61 90) 98 98 20
Internet: www.amoe.de / www.umzug.org; E-Mail: info@amoe.de

Die Unternehmer sind in Zukunft für die Einhaltung aller in der DSGVO genannten Grundsätze verantwortlich. Sie müssen die Grundsätze allerdings nicht nur beachten, sondern deren Einhaltung auch nachweisen können („Rechenschaftspflicht“). Um diesen Nachweis erbringen zu können, müssen die Unternehmer geeignete technische und organisatorische Maßnahmen ergreifen.

1. Datenschutzrechtliche Prinzipien

Um die Anforderungen und Zielrichtung dieser Maßnahmen besser verstehen zu können, ist es notwendig, sich mit den datenschutzrechtlichen Prinzipien der DSGVO auseinanderzusetzen.

a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Art. 5 Abs. 1 lit. a DSGVO legt fest, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

In dieser Vorschrift finden sich die Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben und der Transparenz.

<u>Rechtmäßigkeit - Verbot mit Erlaubnisvorbehalt:</u>

Grundsätzlich ist die Verarbeitung personenbezogener Daten verboten. Nur, wenn eine gesetzlich festgelegte Ausnahme vorliegt, dürfen Daten überhaupt erhoben und verarbeitet werden.

Hier wird die historische Entwicklung des Datenschutzrechtes deutlich. Das Bundesverfassungsgericht entschied im Jahre 1983, dass der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst ist. Datenschutz erhielt somit Grundrechtsstatus und sollte viele Jahre allein dem Schutz des Bürgers vor staatlichen Eingriffen dienen. Daher ist ein Eingriff in dieses Recht, wie immer im Verfassungsrecht, nur zulässig, wenn er aufgrund einer verfassungsgemäßen Grundlage erfolgt. Auch wenn der Anwendungsbereich des Datenschutzrechtes heute auch auf die Privatwirtschaft ausgedehnt ist, behielt dieses Prinzip des Verbots mit Erlaubnisvorbehalt seine Geltung.

Die Erhebung und Verarbeitung von Daten ist daher immer verboten, außer es liegt eine gesetzliche Ausnahme vor. Diese möglichen Ausnahmen regelt Art. 6 DSGVO.

Zulässig ist eine Datenverarbeitung nur dann, wenn

- die betroffene Person ihre Einwilligung erteilt hat;
- sie für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen;

- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt;

- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

- wenn sie im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich ist oder

- sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen (z. B. mögliches berechtigtes Interesse an der Weitergabe innerhalb eines Konzerns).

Praxistipp:

<u>Mitarbeiterdaten:</u>

Für die Verarbeitung von Mitarbeiterdaten gelten in Deutschland Sonderregelungen. § 26 Abs. 1 Satz eins BDSG 2018 regelt, dass Mitarbeiterdaten für die Begründung und Durchführung von Beschäftigungsverhältnissen erhoben, verarbeitet und gespeichert werden dürfen. Hierfür bedarf es aufgrund der gesetzlichen Ausnahme keiner zusätzlichen Erlaubnis.

In vielen Fällen werden die Daten der Mitarbeiter aber auch über dieses Maß hinaus verwendet. In vielen Fällen enthält die Homepage der Unternehmen auch Mitarbeiterprofile, um so für den Kunden ein leichtes Auffinden des konkreten Ansprechpartners zu ermöglichen. Diese Fälle der Veröffentlichung bedürfen in aller Regel der ausdrücklichen Einwilligung des Mitarbeiters. Bei sogenannten „Funktionsträgern“ die als offizielle Ansprechpartner fungieren, ist die Veröffentlichung der Basiskommunikationsdaten ohne Einwilligung zulässig. Da es in diesem Bereich allerdings häufig zu Abgrenzungsschwierigkeiten kommt, empfiehlt es sich, stets eine Einwilligung einzuholen. Sollen zusätzlich auch Fotos der Mitarbeiter auf der Homepage veröffentlicht werden, bedarf es hierfür ohnehin zwingend eine Einwilligung.

<u>Kundendaten:</u>

Die Verarbeitung von Kundendaten fällt unter die Ausnahmeregelung der DSGVO, da diese für die Erfüllung eines Vertrages notwendig sind. Sofern Angebote unterbreitet oder Verträge abgeschlossen werden sollen, dürfen die erforderlichen Daten verarbeitet werden, ohne dass es einer Einwilligung des Kunden bedarf. Nach Abschluss der Vertragsdurchführung sind Spediteure dazu berechtigt, die Daten gemäß Art. 6 Abs. 1 lit. c DSGVO im Rahmen ihrer steuerrechtlichen Verpflichtungen weiterhin zu speichern.

Im Rahmen der Angebotserstellung werden allerdings auch häufig Daten erhoben, die nicht zur Durchführung des Vertrages unmittelbar notwendig sind.

So werden persönliche Verhältnisse, das Vorhandensein von Haustieren oder persönliche Vorlieben erfasst ohne, dass diese unmittelbar zur Auftragsabwicklung nötig wären. Ob diese Daten unter eine gesetzliche Ausnahme fallen (Wahrung eines berechtigten Interesses des Verantwortlichen) oder ihre Speicherung einer Einwilligung bedarf, ist nicht abschließend geklärt.

Praxisgerecht ist es, vorerst von einem gesetzlichen Ausnahmetatbestand auszugehen. Allerdings sollte jedenfalls gedanklich stets eine Abwägung erfolgen, ob aufgenommene Daten für die Auftragsdurchführung tatsächlich von Nutzen sind und die Interessen des Kunden nicht zu sehr belasten.

Das gleiche gilt für die Durchführung nachvertraglicher Maßnahmen. Häufig werden Kunden nach erfolgreichem Abschluss des Auftrages Bewertungsanfragen übersandt. Sofern solche Maßnahmen der Qualitätssicherung durchgeführt werden sollen, ist auch in diesem Fall ungeklärt, ob es einer Einwilligung des Kunden bedarf.

Als Anlage zu dieser Information erhalten Sie eine Erläuterung und Beispielformulierungen für mögliche Einwilligungserklärungen.

Verarbeitung nach Treu und Glauben

Die richtige Übersetzung für dieses Erfordernis wäre wahrscheinlich das Wort „fair“. In der Begründung der Datenschutzrichtlinie wurde die Datenerhebung durch verborgene Geräte hier als Beispiel genannt.

Transparenz

Die betroffene Person muss zum einen stets nachvollziehen können, wer welche Daten zu welchem Zeitpunkt aus welchen Gründen und zu welchem Zweck verarbeitet. Gefordert ist also ein transparenter und nachvollziehbarer Verarbeitungsprozess. Im Mittelpunkt stehen hier also transparente Informationen über die Person, die Daten verarbeitet und auf welche Weise diese verarbeitet werden. Ausfluss des Transparenzgebots sind also sämtliche Informationspflichten und der Auskunftsanspruch des Betroffenen.

b. Zweckbindung

Art. 5 Abs. 1 lit. b DSGVO nennt als zweites Prinzip des Datenschutzes die Zweckbindung. „Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden...“

Die Zweckbindung soll dem Umstand Rechnung tragen, dass bei automatisierten Verarbeitungsprozessen die Person, deren Daten weiterverarbeitet werden, in der Regel nicht anwesend ist und einer Weiterverarbeitung weder zustimmen noch widersprechen kann. Daher sollen die Personen vorher darüber informiert werden, wofür ihre Daten exakt verarbeitet werden.

In der Praxis sollte man sich hier um eine möglichst detaillierte und einfach verständliche Darlegung der Verarbeitungsprozesse bemühen. Es sollte genau bezeichnet werden, wofür Daten erhoben und ob und wie diese weiterverarbeitet werden.

Sollen Daten weiterverarbeitet oder andere weitergegeben werden, muss die Zweckbindung auch beim Folgenutzer sichergestellt werden. Macht der Betroffene von seinem Recht auf Berichtigung oder seinem Recht auf Löschung Gebrauch oder schränkt er die Verarbeitung nach Art. 18 DSGVO ein, so muss dies auch allen weiteren Empfängern der Daten mitgeteilt werden.

Praxistipp:

Macht ein Kunde von einem dieser Rechte Gebrauch, so sind diese Änderungen zwingend auch eingesetzten Subunternehmern oder anderen an der Vertragserfüllung Beteiligten, wie Agenten oder im Ausland ansässigen Helfern, mitzuteilen, die in den Prozess eingebunden waren und Datensätze erhalten haben.

c. Datenminimierung

Art. 5 Abs. 1 lit. c DSGVO legt fest, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

Zur Beachtung dieses Prinzips müssen sich Unternehmer stets fragen, ob die Daten zur Erfüllung des jeweiligen Zwecks (Auftragserfüllung / Arbeitsverhältnis) tatsächlich erhoben und gespeichert werden müssen.

Praxistipp:

Wie bereits an anderer Stelle erörtert, sind zahlreiche erhobene Daten nicht nötig, um Aufträge auszuführen. Notwendig sind Angaben zu der Belade- und Entladestelle, sowie zu den auftraggebenden Personen, Absendern und Empfängern. Ausreichend sind hier Angaben zur Identität und Anschrift, sowie Kontaktdaten. Nicht notwendig ist die Verarbeitung von hierüber hinausgehenden Daten.

Gute Beispiele bieten hier erneut Kunden- und Mitarbeiterdaten. Werden im Rahmen eines Umzugs beispielsweise Fotos gemacht, um das Umzugsvolumen zu ermitteln, sind diese zur Durchführung des Auftrages notwendig. Zur Erfüllung der steuerlichen Verpflichtungen benötigt man sie allerdings nicht. Das gleiche gilt für sämtliche Daten die zur besseren Kundenbetreuung erhoben werden. Familienstand, sonstige persönliche Verhältnisse, körperliche Einschränkungen und das Vorhandensein von Haustieren sind zur Erfüllung der Aufbewahrungspflichten nicht nötig. Diese Daten sollten nach Auftragsdurchführung gelöscht werden, sofern das berechtigte Interesse nicht fortbesteht.

Im Bereich von Bewerbungsverfahren werden ebenfalls nicht erhebliche Daten erfasst. Wird beispielsweise der Eingang einer Bewerbung vermerkt, um die

Einhaltung der Bewerbungsfrist zu kontrollieren, ist diese Angabe nach Ablauf der Frist für das weitere Bewerbungsverfahrens nicht mehr nötig und muss gelöscht werden. Alle Datenverarbeitungsprozesse in den Unternehmen sollten streng mit der Frage „sind die erhobenen Daten zur Erreichung des Zweckes erforderlich?“ überprüft und Regeln für deren Löschung formuliert werden.

d. Richtigkeit

Laut Art. 5 Abs. 1 lit. d DSGVO müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Bei der Erhebung der Daten müssen diese richtig sein. Darüber hinaus müssen Maßnahmen zur Kontrolle eingeführt werden. Empfehlenswert könnte es zum Beispiel sein, zu festgelegten Zeitpunkten Datensätze zu kontrollieren. Sämtliche Daten, wie zum Beispiel Kontakte, die nicht mehr erheblich sind, sind dann zu löschen. Datensätze die weiterhin erheblich sind, sind gegebenenfalls zu korrigieren.

e. Speicherbegrenzung

Art. 5 Abs. 1 lit. e DSGVO legt fest, dass personenbezogene Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Die Vorschrift verlangt, dass ein Bezug zwischen Daten nur hergestellt wird, wenn dies für den Zweck erforderlich ist. Im Bereich der Spedition werden diese Fälle selten vorkommen, da die Unternehmer schon aus steuerlichen Gründen verpflichtet sind, Daten über zehn Jahre aufzubewahren, die eine Identifizierung von Personen ermöglichen.

f. Integrität und Vertraulichkeit

Art. 5 Abs. 1 lit. f DSGVO legt fest, dass personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogene Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Daten müssen vor unberechtigtem Zugriff geschützt werden. Gemeint ist hier nicht nur der Zugriff von außen. Es müssen also nicht nur Systeme eingeführt werden, die Daten vor Zugriffen von Fremden schützen. Auch eine Datenverarbeitung, Datenveränderung oder Datenergänzung durch intern nicht hierfür zugelassene Mitarbeiter müssen von den Unternehmern verhindert werden.

g. Rechenschaftspflicht

Die Unternehmen trifft gemäß Art. 5 Abs. 2 DSGVO zukünftig eine Rechenschaft- und Nachweispflicht über die Einhaltung der datenschutzrechtlichen Prinzipien, die oben beschrieben wurden. Der Unternehmer ist für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich und muss deren Einhaltung nachweisen können. Um diese Verpflichtungen erfüllen zu können, ist der Unternehmer nach Art. 24 DSGVO verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen.

Welche diese Maßnahmen sind, wird in der DSGVO nicht konkret genannt. Es ist eine Risikoabwägung durchzuführen, die die Angemessenheit der Maßnahmen im Hinblick auf den Stand der Technik, der Kosten und der Art, des Umfangs und der Zwecke der Datenverarbeitung sowie die Eintrittswahrscheinlichkeit von Risiken für die betroffenen Personen berücksichtigt.

Art. 32 DSGVO gibt eine Hilfestellung in dem er Maßnahmen benennt, die folgendes einschließen sollten:

- Die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- Die Fähigkeit, die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Zu diesen technischen und organisatorischen Maßnahmen zählt die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten, die Meldung und die Benachrichtigung nach den Art. 33 ff. DSGVO, der Nachweis von erteilten Einwilligungen und der Nachweis fehlenden Verschuldens.

Datenschutzfolgeabschätzung

Art. 35 DSGVO fordert eine Datenschutzfolgeabschätzung, wenn ein Verfahren voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen birgt. Diese Fälle dürften in der Möbelspedition selten vorkommen. Vorstellbar ist dies allerdings, wenn besonders sensible Daten, wie zum Beispiel Gesundheitsdaten beim Transport von Krankenakten, betroffen sind. In diesen Fällen ist stets eine Datenschutzfolgeabschätzung zwingend vorgeschrieben.

Als erster Schritt ist zu prüfen, ob ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Wird ein solches Risiko bejaht, muss überprüft werden, ob die Sicherheitsvorkehrungen zum Schutz der Daten ausreichend sind. Es muss ein

Nachweis erfolgen, dass die DSGVO eingehalten und die Interessen der Betroffenen beachtet wurden.

Kommt der Unternehmer zu dem Ergebnis, dass trotz aller Maßnahmen das Risiko gleichwohl hoch bleibt, muss eine Meldung an die Aufsichtsbehörde erfolgen (Art. 36 DSGVO).

Meldepflicht bei Datenschutzverletzungen

Immer wenn personenbezogene Daten vernichtet, verloren oder verändert werden oder unbefugt offen gelegt werden, sind die Unternehmer verpflichtet, diese Verletzungen binnen 72 Stunden dem Bundesdatenschutzbeauftragten zu melden.

Es kommt nicht darauf an, ob die Datenschutzverletzung vorsätzlich oder versehentlich geschehen ist, sondern lediglich darauf, dass der Unternehmer von der Datenpanne Kenntnis erlangt und ihm eine sinnvolle Meldung möglich ist. Liegen noch nicht alle Informationen vor, sieht die DSGVO auch eine schrittweise Meldung vor.

Lediglich, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der Betroffenen führt, kann der Unternehmer auf eine Meldung verzichten. Hier ist einer Prognoseentscheidung zu treffen. Zu berücksichtigen sind zum Beispiel die Auswirkungen, wenn bestimmte Daten in die Hände Dritter gelangen, mögliche Schäden für Betroffene, Verluste der Vertraulichkeit von Daten, insbesondere, wenn diese einem Berufsgeheimnis unterliegen, die Menge der betroffenen Daten und die Ziele und Fähigkeiten Dritter die Zugang erhalten.

Erfolgt eine Meldung, unterliegt diese keinerlei Formanforderungen. Die Meldefrist beträgt 72 Stunden nach Bekanntwerden der Datenpanne, sofern eine Meldung in dieser Zeit sachdienlich möglich ist.

Auftragsdatenverarbeitung:

In vielen Fällen wird ein Auftragsdatenverarbeiter eingesetzt. Häufig werden zum Beispiel Lohnbuchhaltung oder Rechnungsstellung ausgelagert. In solchen Fällen muss gewährleistet werden, dass hinreichend Garantien für eine ordnungsgemäße Datenverarbeitung vorliegen (Art 28 DSGVO).

Aufgrund der zahlreichen an den Einsatz eines Auftragsdatenverarbeiters geknüpften Rechtsfolgen werden wir über dieses Thema gesondert informieren.

Verzeichnis von Verarbeitungstätigkeiten

Jedes Unternehmen muss ein schriftliches Verzeichnis aller Verarbeitungstätigkeiten führen. Hierfür ist es nötig, alle intern durchgeführten Datenverarbeitungsprozesse genau zu überprüfen und sich einen Überblick über die Zwecke der Verarbeitung zu verschaffen. Das ist wichtig, um überhaupt in der Lage zu sein, Datenschutzrisiken aufzudecken und in der Folge geeignete technische und organisatorische Maßnahmen zu treffen.

Art. 30 Abs. 4 DSGVO statuiert die Pflicht des Unternehmens, das Verzeichnis den Behörden auf Verlangen vorzulegen

Das Verzeichnis enthält unter anderem folgende Angaben:

- Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
- Die Zwecke der Datenverarbeitung
- Eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Empfänger / Kategorien von Empfängern personenbezogener Daten
- Übermittlung von Daten in ein Drittland
- Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Die Verpflichtung zur Führung des Verzeichnisses entfällt für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen. Diese Regelung stellt allerdings nur scheinbar eine Erleichterung dar. Die Ausnahme soll nur gelten, wenn nur gelegentlich Verarbeitungstätigkeiten anfallen und keine besonders sensiblen Daten berührt sind und mit der Verarbeitung auch sonst kein Risiko für die betroffenen Personen einhergeht.

Da in Möbelspeditionen in der Regel mindestens Personal- und Kundendatenbanken geführt werden, ist davon auszugehen, dass hier nicht nur eine gelegentliche Verarbeitung erfolgt und die Ausnahme keine Geltung hat.

Unterlässt der Unternehmer das Erstellen der Verfahrensübersicht, drohen Bußgelder bis zu 10 Millionen € oder bis zu 2 % des weltweiten Umsatzes des Unternehmens im letzten Jahr.

Der Erstellung eines Verarbeitungsverzeichnisses widmen wir uns im Rahmen einer eigenen Mitgliederinformation.

Ist ein entsprechendes Verzeichnis von Verarbeitungstätigkeiten erstellt worden, sollte ein System zum Datenschutzmanagement eingeführt werden.

Datenschutzmanagement

Planung:

Ein erster Schritt zur Implementierung eines Datenschutzmanagements ist, nachdem die Bearbeitungsprozesse durch das Verzeichnis von Verarbeitungstätigkeiten festgestellt wurden, eine Datenschutzpolitik festzulegen. Hierbei sollten folgende Punkte festgeschrieben werden:

- Die Zuständigkeiten für den Datenschutz im Unternehmen (hierzu gehört auch die Einbindung und Aufgabenstellung des betrieblichen Datenschutzbeauftragten - über die Verpflichtung zur Bestellung eines Datenschutzbeauftragten haben wir bereits im Rahmen der Mitgliederinformation „Info_1_Der Datenschutzbeauftragte nach der DSGVO“ umfassend informiert.)

- Die Sensibilisierung und Schulung der Mitarbeiter

- Verpflichtung auf das Datengeheimnis (auch, wenn es hier keine gesetzliche Vorschrift mehr gibt, ist dennoch eine Verpflichtung der Mitarbeiter auf das Datengeheimnis anzuraten. Ansonsten muss sichergestellt werden, dass Mitarbeiter nur Daten im Rahmen ihrer Aufgabenerfüllung verarbeiten. Ist ein Auftragsverarbeiter eingesetzt, ist für diesen vorgeschrieben, dass die Mitarbeiter verpflichtet werden.)

- Die Durchführung von Kontrollen, ob die getroffene Regelungen/Anweisungen auch eingehalten werden

- Den Einsatz datenschutzfreundlicher Technologien

- Den Stand der Technik als Anforderung an die IT-Sicherheit

- Die Führung des Verzeichnisses von Verarbeitungstätigkeiten

- Ein Prozess zum Abschluss von Auftragsverarbeitungen

- Den Prozess zur Umsetzung der Betroffenenrechte und der Transparenz der Datenverarbeitung

- Den Prozess zur Durchführung einer Risikobewertung

- Den Prozess zur Durchführung von Datenschutzfolgeabschätzungen und einer eventuellen Meldung an die Aufsichtsbehörde

- Den Prozess zur Meldung von Verletzungen des Datenschutzes (Datenpannen)

Umsetzung

Ist der Planungsprozess abgeschlossen, sind die getroffenen Maßnahmen zu konkretisieren und in die Praxis umzusetzen. Dazu gehört eine ausreichende Dokumentation sowie die geeigneten technisch-organisatorischen Maßnahmen.

Erfolgskontrolle und Überwachung

Auch nach Implementierung der neuen Maßnahmen ist eine ständige Überprüfung auf deren Wirksamkeit erforderlich. Hierfür sollten bestimmte Fristen festgelegt und Verantwortlichkeiten verteilt werden.

Optimierung und Verbesserung

Wird im Rahmen der Erfolgskontrolle und Überwachung festgestellt, dass Anpassungen notwendig sind, sind diese vorzunehmen. Die DSGVO verlangt hinsichtlich technischer Sicherheitsmaßnahmen eine kontinuierliche Anpassung an technische Entwicklungen.

Praxistipp:

Vielen Unternehmern wird es bei der großen Anzahl von neuen Pflichten schwer fallen, ihren individuellen Umsetzungsbedarf zu ermitteln. Das bayerische Landesamt für Datenschutz hat einen Fragebogen entwickelt, der es auf einfache Weise ermöglicht, sich einen ersten Überblick zu verschaffen. Sie erhalten diesen Fragebogen als Anlage.

Das könnte Sie auch interessieren:

Info_1_Der Datenschutzbeauftragte nach der DSGVO
Info_2_Anschriften der Datenschutzaufsichtsbehörden der Länder

Es folgt:

Info_4_Die Rechte der betroffenen Person