EU-DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

AB 25.MAI 2018 FÜR ALLE UNTERNEHMEN VERPFLICHTEND

Die neue EU-Datenschutz-Grundverordnung (DSGVO) ist ab dem 25. Mai 2018 für alle Unternehmen verpflichtend. Diese sollten für die neuen Regeln gerüstet sein.

HINTERGRUND

Die neue DSGVO soll die Rechte der Dateninhaber stärken, ihnen mehr Kontrolle über die eigenen personenbezogenen Daten geben. Bei Verstoß drohen hohe Bußgelder, um Unternehmen bei der Umsetzung der datenschutzrechtlichen Anforderungen verstärkt in die Pflicht zu nehmen.

ZIEL

Die neue Datenschutz-Grundverordnung nutzen, um im Unternehmen mit personenbezogenen Daten sicher und verantwortungsvoll umzugehen. Dabei ist es wichtig zu gewährleisten bzw. zu wissen, dass die grundsätzlichen Datenverarbeitungsregeln im Unternehmen verinnerlicht werden, welche Voraussetzungen für die Erhebung von personenbezogenen Daten gegeben sein müssen, in welcher Form das Datenschutzsystem dokumentiert werden muss, welche Schutzvorkehrungen getroffen werden müssen, was bei der Zusammenarbeit mit Dienstleistern oder verschiedenen Unternehmenszweigen beachtet werden muss, dass betreffende Personen ausführlich über die Erhebung ihrer personenbezogenen Daten informiert werden.

EU-Datenschutz-Grundverordnung

Grundbegriffe kurz erklärt

Personenbezogene Daten - Was zählt alles dazu?

Es handelt sich um Daten, die den Menschen (natürliche Personen) betreffen. Daten von Unternehmen (juristische Personen) sind nicht betroffen. Personenbezogen sind Daten, die

einem Menschen direkt zugeordnet sind (bspw.: Max Mustermann hat blonde Haare/Max Mustermann wohnt in der Musterstraße 419/Max Mustermann besitzt einen Golf)

in Kombination einen Menschen identifizieren und ihm zugeordnet werden können (bspw.: Der Halter des Nummernschilds XY hat blonde Haare/Der Besitzer der Fahrgestellnummer XY wohnt in der Musterstraße 419/ Der Inhaber der Kontonummer XY besitzt einen Golf)

Datenverarbeitung - ab wann trifft dieser Begriff zu?

Datenverarbeitung beginnt dann, wenn Daten handschriftlich oder digital notiert und aufbewahrt werden. In der Regel werden nicht nur Kundendaten verarbeitet. Auch die Daten der Mitarbeiter unterliegen dem Datenschutz.

EU-DATENSCHUTZ-GRUNDVERORDNUNG

IN 6 SCHRITTEN ZUR SICHEREN DATENVERARBEITUNG

EINLEITUNG

Gültig ist die neue EU-Datenschutz-Grundverordnung (DSGVO) bereits seit 2016. Nach zweijähriger Übergangsfrist sind die neuen Regeln ab dem 25. Mai 2018 für alle Unternehmen verpflichtend umzusetzen. 99 Artikel, die bei manchen Verantwortlichen für Verunsicherung sorgen, zumal bei Verstößen künftig hohe Bußgelder drohen. Besonders kleine Betriebe fühlen sich den neuen Anforderungen mitunter nicht gewachsen. Mit kühlem Kopf und klarer Struktur wird aber schnell deutlich, dass die DSGVO wahrlich kein Hexenwerk ist. Deshalb gibt TÜV Rheinland einen kompakten und verständlichen Überblick, damit Unternehmen beim Datenschutz auch zukünftig auf der sicheren Seite sind. Denn die neue DSGVO sollte nicht als Bedrohung, sondern als Chance gesehen werden, mit personenbezogenen Daten sicher und verantwortungsvoll umzugehen.

Werden folgende 6 Schritte im Unternehmen angewendet, ist der Datenschutz nach der DSGVO in hohem Maße gewährleistet. Es versteht sich von selbst, dass die eingeführten Regelungen und Verarbeitungsgrundsätze regelmäßig überprüft werden müssen. Im Unternehmen sollte mit personenbezogenen Daten sehr sorgsam umgegangen werden. Betroffene müssen stets wissen, wie lange und warum sie welche persönlichen Daten in fremde Hände geben – schließlich möchte jeder die Kontrolle über seine Eigentümer besitzen.

1. GRUNDSÄTZE VERINNERLICHEN

Diese Dinge sind bei der Datenverarbeitung immer zu berücksichtigen:

- Was nicht ausdrücklich erlaubt ist, ist verboten.
- Die erhobenen Daten müssen einem klaren Zweck dienen und dürfen nicht für andere Zwecke verwendet werden. (bspw.: Eine Autoscheibe soll repariert werden. Name und Telefonnummer des Kunden werden zu diesem Zweck gespeichert. Ein Anruf darf jedoch nur erfolgen, wenn es sich um diesen konkreten Auftrag handelt.)
- Es dürfen nur Daten erhoben werden, die dem Zweck dienen – je weniger, desto besser. (bspw.: Beim Kauf eines Autos spielt der Familienstand oder die Haarfarbe des Kunden keine Rolle. Diese Daten dürfen somit auch nicht erhoben werden.)
- Daten dürfen nur gespeichert werden, solange sie dem eigentlichen Zweck dienen oder Gesetze es verlangen. (bspw.: Rechnungsbelege mit den erforderlichen Daten des Kunden müssen aus steuerlichen Gründen zehn Jahre gespeichert werden. Danach aber müssen sämtliche Daten des Kunden vernichtet werden.)
- Das Unternehmen trägt bei der Verarbeitung stets die Verantwortung und muss die Einhaltung des Datenschutzes zu jeder Zeit nachweisen können.
- Das Unternehmen muss sicherstellen, dass die erhobenen Daten vor dem Zugriff Unbefugter sicher sind. (bspw.: Firewalls und Virenschutzprogramme/Passwortschutz/Abschließbare Aktenschränke)

DSGVO-Artikel zur Nachlese: Art. 5 und Art. 25

2. VORAUSSETZUNGEN KENNEN

In diesen Fällen ist eine Datenverarbeitung erlaubt:

- Wenn die Daten für die Beschäftigung eines Arbeitnehmers zwingend erforderlich sind (bspw.: Lohnunterlagen und Krankheitstage speichern)
- Wenn diese zur Erfüllung eines Auftrags nötig sind (bspw.: Namen und Bankverbindung, um beim Autokauf mögliche Ratenzahlungen zu veranlassen)
- Wenn diese im Vorfeld eines Vertrags nötig sind (bspw.: E-Mail-Adresse, um dem Kunden auf seinen Wunsch einen Kostenvoranschlag senden zu können)
- Wenn berechtigte Interessen des Unternehmensschwerer wiegen als das berechtigte Interesse des Einzelnen am Schutz seiner Daten (Achtung: Werbung liegt zwar im Interesse des Unternehmens, überwiegt in der Regel jedoch nicht die Interessen der Person, deren Daten verarbeitet werden. Im Einzelfall sind jedoch Ausnahmen möglich.) In allen anderen Fällen ist die Verarbeitung von personenbezogenen Daten nur erlaubt, wenn der Betroffene in die Verarbeitung eingewilligt hat.

DSGVO-Artikel zur Nachlese: Art. 6 bis 11

Tipp: Einwilligungen sollten im Sinne der möglichen Beweisführung immer in schriftlicher Form vorliegen. (Mehr zum Thema Einwilligungen unter Schritt 5.)

3. DATENSCHUTZSYSTEM DOKUMENTIEREN

Das Datenschutzmanagement im Unternehmen muss in einem sogenannten „Verzeichnis von Verarbeitungstätigkeiten“ beschrieben werden.
Dieses muss unter anderem enthalten:

- Die Kontaktdaten des Datenschutzbeauftragten

Tipp: Auch externe Experten können als Datenschutzbeauftragten benannt werden. (Achtung: Ein Datenschutzbeauftragter ist dann verpflichtend, wenn mindestens zehn Mitarbeiter regelmäßig mit der Verarbeitung personenbezogener Daten beschäftigt sind.)

- Zu welchen Zwecken Daten im Unternehmen verarbeitet werden (bspw.: Auftragsabwicklung, Werbung)
- Welchen Personengruppen diese Daten gehören (bspw.: Kunden, Mitarbeiter, Zulieferer)
- Vorgesehene Fristen für die Löschung der Daten (bspw.: Rechnungsdaten werden nach zehn Jahren automatisch gelöscht)
- Falls zutreffend: Empfänger-Gruppen der Daten, keine konkreten (Firmen-) Namen (bspw.: Zulieferer, die z.B. eine Fahrgestellnummer für die Bestellung von Ersatzteilen bekommen könnten/Steuerberater, die Daten der Mitarbeiter benötigen könnten)
- Eine Beschreibung der technischen und organisatorischen Maßnahmen bzw. Schutzvorkehrungen (mehr dazu unter Schritt 4)
- Eine Bewertung des Risikos, dass im Verarbeitungsprozess Daten beschädigt, verloren oder geraubt werden können

DSGVO-Artikel zur Nachlese: Art. 30

4. SCHUTZVORKEHRUNGEN TREFFEN

Im Unternehmen muss, so gut es geht, sichergestellt werden, dass

- Unbefugte keinen Zugang zu den personenbezogenen Daten bekommen können (bspw.: Geschützter, abschließbarer Ort für den betreffenden Computer bzw. Server oder auch Aktenordner) (Achtung: Beim Entsorgen von Kopien besonders sorgfältig sein. Keine lesbaren Dokumente einfach ins Altpapier geben.)
- handelnde Person und Zeitpunkt der Verarbeitung stets zugeordnet werden können (bspw.: durch individuelle Benutzernamen)

- die Daten, so gut es geht, vor Zerstörung geschützt sind und notfalls wiederhergestellt werden können (bspw.: Server stehen in kühlen, trockenen Räumen/Laptop wird ausschließlich in gepolsterten und gesicherten Taschen transportiert/Regelmäßige Sicherheitskopien)

DSGVO-Artikel zur Nachlese: Art. 32

5. ZUSAMMENARBEIT MIT DIENSTLEISTERN DEFINIEREN

Werden personenbezogene Daten an Dienstleister, beispielsweise einen Zulassungsdienst, übermittelt, so muss geprüft werden, ob mit diesen ein Vertrag zur Auftragsverarbeitung (AV) geschlossen werden muss. Das gilt auch für die verschiedenen GmbHs (o.Ä.) eines Unternehmens.
Der AV-Vertrag muss unter anderem enthalten:

- Eine Beschreibung des Auftrags (bspw.: Der Dienstleister ist für die Zulassung von Fahrzeugen zuständig)
- Die Dauer des Auftrags
- Zweck der Datenverarbeitung und die Art der personenbezogenen Daten (bspw.: Die Fahrgestellnummer ist für die Zulassung zwingend nötig)
- Die betroffenen Personengruppen (bspw.: Kunde und Sachbearbeiter einer Behörde)
- Die erforderlichen technischen und organisatorischen Maßnahmen (Der Dienstleister erfüllt die unter Schritt 4 definierten Schutzvorkehrungen)

Achtung: Bei einer Auftragsverarbeitung können das beauftragende Unternehmen und der Dienstleister bei Datenschutzvergehen gegenüber dem Betroffenen gemeinsam haften.

DSGVO-Artikel zur Nachlese: Art. 24 bis 43 und Art. 44 bis 50

6. GENAUESTENS INFORMIEREN UND BEGRÜNDEN

Wann immer personenbezogene Daten erhoben werden, muss das der betroffenen Person ausführlich mitgeteilt werden. (Achtung: Diese Formulierung bspw. reicht bei weitem nicht: Wir erheben Ihre Daten, um Ihr Auto reparieren zu können.)
Betroffene Personen müssen so ausführlich und transparent wie irgend möglich über die geplante und bereits erfolgte Datenverarbeitung aufgeklärt werden. Die Informationen oder auch Einwilligungserklärungen müssen
enthalten:

- Wer erhebt die Daten?
- Um welche Daten geht es genau?
- Zu welchem Zweck werden die Daten erhoben?
- Sollen diese Daten an Dritte weitergegeben werden? Falls ja, warum und an wen?
- Wann werden die Daten wieder gelöscht?

Zudem muss die betroffene Person auf ihr Recht auf Auskunft, Löschung und jederzeit möglichen Widerspruch einer Einwilligung hingewiesen werden. Dazu müssen Prozesse im Unternehmen etabliert werden, um die Rechte des Kunden jederzeit erfüllen zu können. All diese Informationen, Einwilligungsunterlagen und auch Widerspruchsmöglichkeiten müssen so einfach und verständlich wie möglich formuliert sein.

DSGVO-Artikel zur Nachlese: Art. 12 bis 22

EU-DATENSCHUTZ-GRUNDVERORDNUNG

WAS TUN BEI DATENPANNEN?

Gründe für mögliche Datenpannen gibt es viele, vom Hackerangriff bis hin zum gestohlenen Laptop. Könnte der Schutz nicht mehr gegeben sein, ist das unverzüglich und möglichst binnen 72 Stunden der Datenschutzaufsichtsbehörde des betreffenden Bundeslandes zu melden. In der Meldung muss unter anderem der Vorfall, die Zahl der betroffenen Personen und die Art der gefährdeten Daten (bspw. Adressdaten oder Kontodaten) genannt werden.