FAQ-LISTE

Fragen und Antworten zur Datenschutz-Grundverordnung (DSGVO)

Frage: Welche Unternehmen sind von der DSGVO betroffen?

Antwort: Von der neuen Verordnung sind alle Unternehmen in der EU betroffen, unabhängig von der Größe, Mitarbeiterzahl oder Umsatz des Unternehmens. Das heißt: Kleine Handwerksbetriebe mit zwei bis drei Mitarbeitern sind genauso betroffen wie große Konzerne.

Frage: Wann tritt die DSGVO in Kraft?

Antwort: Die Verordnung ist bereits 2016 in Kraft getreten. Die EU hat den Unternehmen jedoch eine zweijährige Übergangsfrist gewährt. Ab 25. Mai 2018 ist sie dann in allen EU-Mitgliedsstaaten anwendbar.

Frage: Welche Daten unterliegen der DSGVO?

Antwort: Das Datenschutzrecht gilt ausschließlich für personenbezogene Daten, denn das Ziel ist, die Privatsphäre des Einzelnen zu schützen. Demnach sind u.a. folgende Daten betroffen:

- Kundendaten
- Lieferantendaten
- Mitarbeiterdaten

Unternehmensdaten sind nicht geschützt.

Frage: Was genau sind personenbezogene Daten?

Antwort: Im Detail sind folgende Daten gemeint:

- allgemeine Personendaten: Name, Geburtsdatum, Geburtsort, Postanschrift, E-Mail-Adresse, Rufnummern usw.
- Kennnummern: Sozialversicherungsnummer, Steueridentifikationsnummer, Nummer bei der Krankenkasse, Personalausweisnummer usw.
- Bankdaten: Kontostände, Kontonummern, Kreditinformationen, usw.
- körperliche Merkmale: Geschlecht, Haut-, Haar- und Augenfarbe, Statur usw.
- Vermögen und Besitz: Immobilien, Fahrzeuge, Grundbucheintragungen, Kfz-Kennzeichen, usw.
- Werturteile: Schul-, Hochschul- und Arbeitszeugnisse usw.
- Kundendaten: Bestellungen, Adressdaten, Kontodaten usw.
- Online-Daten: IP-Adresse, Standortdaten usw.
- u. v. m.

Darüber hinaus gibt es (laut § 4 Absatz 9 BDSG) die besonderen personenbezogenen Daten.
Die Vorschriften zur Sammlung und Verarbeitung dieser Daten sind wesentlich strenger. Es handelt sich um folgende Daten:

- Angaben über rassische sowie ethnische Herkunft

- politische Ansichten
- religiöse und philosophische Überzeugung
- Gewerkschaftszugehörigkeit
- Angaben zur Gesundheit
- Angaben zur Sexualität

Frage: Wann darf ich personenbezogene Daten verarbeiten?

Antwort: Oberster Grundsatz des alten wie neuen Datenschutzrechts ist das Verbotsprinzip: Jede Verarbeitung personenbezogener Daten ist verboten. Es sei denn, der Zweck der Datenspeicherung ist gerechtfertigt.

Das ist z. B. dann der Fall, wenn ein Vertrag mit der betroffenen Person besteht: Der Betreiber eines Online-Shops darf die Adressdaten des Kunden an einen Logistikdienstleister weitergeben, damit die Ware ausgeliefert werden kann. Die Datenspeicherung darf aber nur so erfolgen, wie es für die Vertragserfüllung notwendig ist.

Frage: Was sind die Kernforderungen der DSGVO?

Antwort: Die Datenschutzgrundverordnung enthält eine Vielzahl komplexer Inhalte. Für Sie als Kleinunternehmer sind vor allem folgende Forderungen relevant:

Recht auf Vergessen /Löschung
Ein wichtiger Teil der DSGVO sind die Rechte der Betroffenen. Daten müssen auf Verlangen eines Kunden gelöscht werden, wenn der Zweck, für den die Daten gespeichert wurden, nicht mehr besteht. Aber auch dann, wenn der Kunde seine Einwilligung zur Datenspeicherung widerruft oder wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

Auskunftsrecht
Der Kunde kann, wie in der bisherigen Verordnung auch, jederzeit Auskunft darüber verlangen, welche Daten von ihm gespeichert und wie diese verarbeitet werden. Diese Auskunft muss unverzüglich erteilt werden. Dies bedeutet, dass in jedem Unternehmen ein Prozess geschaffen werden muss, der den Auskunftsansprüchen gerecht wird.

Meldepflicht
Die Meldepflicht von Datenpannen, die z. B. durch Hacker-Angriffe, Verlust eines Datenträgers oder mobilen Endgeräts verursacht werden, sind mit der neuen DSGVO deutlich umfangreicher geworden: Bisher war nur im Ausnahmefall eine Meldung erforderlich, nach neuem Recht muss jede Datenschutzverletzung binnen 72 Stunden der Behörde – unter Umständen auch den Betroffenen – gemeldet werden. Deshalb sollte jedes Unternehmen über einen internen Prozess verfügen, der im Falle von Datenlecks zum Einsatz kommt.

Frage: Was mache ich mit Daten in Dokumenten, für die Aufbewahrungsfristen bestehen?

Antwort: Wenn Aufbewahrungspflichten für bestimmte Dokumente bestehen, dürfen diese gespeichert werden, auch wenn sie personenbezogene Daten enthalten. Die Pflicht zur Löschung wird in diesen Fällen ausgesetzt. Das ist zum Beispiel bei Rechnungen der Fall (Aufbewahrungspflicht 10 Jahre) und bei geschäftlichen Briefen /E-Mails (Aufbewahrungspflicht 6 Jahre).

Frage: Welche Bereiche im Unternehmen sind von der DSGVO betroffen?

Antwort: Wichtige Bereiche im Unternehmen, auf die ein besonderes Augenmerk gelegt werden sollte, sind u.a.

- EDV
- Vertrieb
- Einkauf
- Personalabteilung

Frage: Was passiert, wenn ich die DSGVO nicht fristgerecht umgesetzt habe?

Antwort: Experten gehen davon aus, dass bis zum Stichtag nicht alle Unternehmen die DSGVO bereits umgesetzt haben. Insofern werden Prüfer voraussichtlich nicht sofort von umfassenden Strafmaßnahmen Gebrauch machen. Unternehmer sind jedoch gut beraten, das Thema nicht zu ignorieren. Denn wer nachweisen kann, dass bereits an der Umsetzung der DSGVO gearbeitet wird, kann bei einer Prüfung auf Nachsicht und Unterstützung seitens der Behörden hoffen.

Doch Vorsicht: Nicht nur Behörden, sondern auch Kunden oder z. B. ehemalige Mitarbeiter können Auskunft über die gespeicherten Daten verlangen. Wer diesen Anforderungen nicht unverzüglich nachkommt, kann juristisch belangt werden. Experte warnen bereits jetzt davor, dass die Abmahnanwälte schon in den Startlöchern stehen.

Frage: Welche Bußgelder drohen tatsächlich?

Antwort: Bisher waren Bußgelder von maximal 300 000 Euro vorgesehen, was in der Praxis meistens auf Beträge zwischen 5000 und 10 000 Euro hinauslief. Zukünftig sollen Verstöße gegen den Datenschutz erheblich schärfer bestraft werden. Der Höchstbetrag kann nun bis zu vier Prozent des Jahresumsatzes oder bis zu 20 Millionen Euro betragen – je nachdem, welche Summe höher liegt. Dadurch werden auch die tatsächlich zu zahlenden Bußgelder drastisch ansteigen.

Frage: Muss ich in meinem Unternehmen einen Datenschutzbeauftragen haben?

Antwort: Wenn sich in Ihrer Firma mehr als 10 Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, sollten Sie einen Datenschutzbeauftragen vorweisen können. Unternehmen mit mehr als 20 Mitarbeitern benötigen zwingend einen Datenschutzbeauftragten. Hier sollte ein geeigneter Mitarbeiter entsprechend ausgebildet bzw. geschult werden.

Frage: Wer ist bei Verstößen gegen die DSGVO verantwortlich?

Antwort: Prinzipiell ist der Inhaber oder Geschäftsführer eines Unternehmens verantwortlich und nicht der Datenschutzbeauftragte oder der Leiter der EDV! Stellen Sie daher in Ihrem Unternehmen sicher, dass die neuen Vorschriften von allen Mitarbeitern eingehalten werden.