Industrie- und Handelskammer zu Leipzig

Datenschutz

Datenschutz ist immer noch in aller Munde. Viele Unternehmen haben Sorge, die Anforderungen aus der EU-Datenschutz-Grundverordnung (DSGVO) und dem neunen Bundesdatenschutzgesetz (BDSG) nicht gesetzeskonform umsetzen zu können. Vielerlei Hilfestellungen gibt die Industrie- und Handelskammer zu Leipzig durch Informationsveranstaltungen und individuelle Beratungen. Zudem gibt es Merkblätter/Newsletter, mit den einzelne Thermen aus der DSGVO erklärt und Hinweise für kleine Unternehmen bzw. Existenzgründer gegeben werden. Auch der Sächsische Datenschutzbeauftragte gibt Hilfestellung bei der Umsetzung.

Die nachstehenden Fragen und Antworten sind aus den zahlreichen Kontakten mit Unternehmen entstanden und sollen eine schnelle Hilfestellung bei konkreten Problemen geben.

1. Welche Arten von Daten sind durch die DSVGO geschützt?

Alle Arten von personenbezogenen Daten werden durch die DSGVO geschützt und dies unabhängig davon, um welche Kategorie von Personen es geht, also ob es sich hierbei um

- Mitarbeiter-,
- Geschäftspartner-, Kunden- oder
- Lieferantendaten handelt.

Für die DSGVO gilt wie für alle weiteren Datenschutzgesetze: Sie sind immer dann zu beachten, wenn Unternehmen mit sog. personenbezogenen Daten umgehen. Hierunter versteht man alle Informationen, die sich direkt oder indirekt (z. B. über eine Kennung) auf einen Menschen (sog. „identifizierte oder identifizierbare natürliche Person“ bzw. „betroffene Person“) beziehen lassen. Um Angaben über eine bestimmte Person handelt es sich, wenn die Daten mit dem Namen der betroffenen Person verbunden sind oder sich aus dem Inhalt bzw. dem Zusammenhang der Bezug unmittelbar herstellen lässt.
Beispielsweise:

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail-Adresse
- Konto-, Kreditkartennummer
- Bonitätsdaten
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweisnummer, Sozialversicherungsnummer
- IP-Adresse
- genetische Daten und Krankendaten
- Werturteile wie zum Beispiel Zeugnisse
- Fotos

Sind Daten nicht personenbeziehbar (z. B. anonymisierte Statistikdaten), so sind Datenschutzgesetze nicht zu

beachten.

2. Ich habe nur Firmenkunden. Muss ich den Datenschutz trotzdem beachten?

Datenschutz gilt grundsätzlich auch im Geschäftsverkehr mit anderen Unternehmen. Einzelangaben über juristische Personen, wie zum Kapitalgesellschaften oder eingetragene Vereine, sind keine personenbezogenen Daten. Etwas anderes gilt nur, wenn sich die Angaben auch auf die hinter der juristischen Person stehenden Personen beziehen, das heißt auf sie „durchschlagen“. Dies kann beispielsweise bei der GmbH einer Einzelperson oder bei einer Einzelfirma der Fall sein.

In der Regel haben Sie bei Firmenkunden einen Ansprechpartner und erheben z. B. Name, personalisierte E-Mail-Adresse, Funktion im Unternehmen usw. Hierbei handelt es sich wiederum um personenbezogene Daten, da eine natürliche Person identifizierbar ist.

3. Gilt das Datenschutzrecht auch bei Dateien, die in Papierform verarbeitet werden?

Ja, die DSGVO unterscheidet nicht zwischen Papier- und elektronischer Verarbeitung. Bei einer papiergebundenen Datenverarbeitung muss aber eine strukturierte Sammlung von personenbezogenen Daten vorhanden sein. Kleine Notizen auf Blöcken oder „Post-it“ Aufkleber fallen also nicht darunter, wenn sie nicht geordnet abgelegt werden.

4. Wann können Daten rechtmäßig verarbeitet werden?

Für die Rechtmäßigkeit gibt es mehrere Rechtsgrundlagen. Im geschäftlichen Verkehr mit Kunden kommen insbesondere vertragliche Vereinbarungen und die Einwilligung in Betracht. Daneben können auch Gesetze eine Verarbeitung rechtfertigen.

5. Brauche ich für jede Datenerhebung/-verarbeitung immer eine Einwilligung?

Nein, Sie benötigen für jede Verarbeitung von personenbezogenen Daten eine datenschutzrechtliche Rechtsgrundlage (etwa Vertrag oder Anbahnung eines Vertrags, Einwilligung, Interessenabwägung berechtigtes Interesse). Die Rechtsgrundlage kann in bestimmten Fällen auch eine Einwilligung sein (z. B. Anmeldung zum Bezug eines Newsletters, Geburtstagsliste von Mitarbeitern). Beruht die Datenverarbeitung auf einer vertraglichen Basis, um den Vertrag abzuwickeln, sind Einwilligungen für die Erhebung und Verarbeitung der Daten nicht erforderlich. Aber Vorsicht: Sollen die so erhobenen Daten für andere Zwecke als die Vertragsabwicklung verarbeitet werden (z. B. Verwertung der Daten für eine Studie oder Weitergabe der Daten an Dritte), so bedarf es einer Einwilligung für den neuen Zweck.

6. Darf ich die Daten meiner Mitarbeiter verarbeiten?

Die Daten von Stellenbewerbern, Mitarbeitern und ausgeschiedenen Mitarbeitern dürfen nach § 26 BDSG zur Begründung, Durchführung und Beendigung des Arbeitsverhältnisses verarbeitet werden. Geht eine Datenverarbeitung aber über diesen Zweck hinaus, z. B. die Veröffentlichung von Fotos auf der Firmenhomepage, ist darüber hinaus eine Einwilligung erforderlich. Eine Einwilligung muss immer freiwillig sein. Es dürfen bei Verweigerung also keine Nachteile drohen.

7. Was ist ein Verzeichnis von Verarbeitungstätigkeiten?

Ein solches Verzeichnis ist eine Zusammenfassung von einzelnen Verarbeitungsvorgängen, bei denen personenbezogene Daten entweder automatisiert (=elektronisch) oder zunächst nicht automatisiert (=analog) verarbeitet werden, aber später in ein Dateisystem gespeichert werden sollen. Der Inhalt eines solchen Verzeichnisses ist gesetzlich geregelt. Das Verzeichnis muss wesentliche Angaben zur Verarbeitung beinhalten. Die Zwecke der Verarbeitung, die Beschreibung der betroffenen Datenkategorien und Personen sind aufzulisten. Eine bestimmte Form ist für das Verzeichnis nicht vorgesehen.

Alle Unternehmen, die personenbezogene Daten automatisiert oder nicht automatisiert verarbeiten und sie in einem Dateisystem speichern oder speichern wollen, müssen ein Verzeichnis über die Verarbeitungen führen.

Das Gesetz sieht eine Ausnahme vor: Unternehmen mit weniger als 250 Mitarbeitern sind von der Pflicht ein Verarbeitungsverzeichnis zu führen befreit. Aber auch nur dann, wenn die Verarbeitung selbst nicht ein Risiko birgt - das ist z. B. immer der Fall bei Scoring und Überwachungsmaßnahmen, die Verarbeitung nur gelegentlich erfolgt, und keine besonderen sensiblen Datenkategorien, wie z. B. Religions-, Gesundheitsdaten usw. betroffen sind. Die meisten Unternehmen verarbeiten regelmäßig Daten ihrer Mitarbeiter und Kunden, so dass die Ausnahmevorschrift in den meisten Fällen nicht greift und das Verarbeitungsverzeichnis geführt werden muss.

8. Benötigt mein Unternehmen einen Datenschutzbeauftragten, wenn ja, wer darf als solcher benannt werden?

Ja,

1. bei Unternehmen, deren Kerntätigkeit in der systematischen Überwachung oder Verarbeitung besonderer personenbezogener Daten besteht

2. wenn der Verantwortliche/Auftragsverarbeiter in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (z. B. regelmäßige Kommunikation per E-Mail

   oder

3. wenn der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgeabschätzung nach Art. 35 DSGVO unterliegen.

Das bedeutet, wenn besonders sensible Daten verarbeitet werden, wie zum Beispiel ethische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit, religiöse Überzeugungen, genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zur sexuellen Orientierung usw. – dann hat das Unternehmen unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen.

Datenschutzbeauftragter darf nur sein, wer sowohl in rechtlicher als auch in technischer Hinsicht über die erforderlichen Kenntnisse verfügt und nicht Gefahr läuft, kraft seiner Position in dem Unternehmen einer Interessenkollision ausgesetzt zu sein. Damit kommen also weder Führungskräfte mit Personalverantwortung noch solche aus dem IT-Bereich (intern/extern) infrage. Der Datenschutzbeauftragte kann sowohl ein Mitarbeiter des Unternehmens als auch eine externe Person sein. Soweit ein Mitarbeiter zum Datenschutzbeauftragten ernannt wird, genießt dieser einen besonderen Kündigungsschutz und kann auch nur aus einem wichtigen Grund seines Amtes enthoben werden. Der besondere Kündigungsschutz reicht sogar bis zu einem Jahr nach Beendigung seiner Tätigkeit als Datenschutzbeauftragter fort. Ob eine Befristung der Ernennung rechtlich wirksam ist, ist sehr umstritten.

9. Was ist eine Datenschutz-Folgenabschätzung?

Eine Datenschutz-Folgenabschätzung ist eine Abschätzung der Folgen einer Datenverarbeitung mit voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen. Diese ist immer dann durchzuführen, wenn besonders sensible, personenbezogene Daten verarbeitet werden oder die Datenverarbeitung dazu bestimmt war, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten. Sie hat den Zweck, rechtzeitig geeignete Maßnahmen ergreifen zu können, um das Risiko eines Schadens bei den Betroffenen zu minimieren.

10. Wann muss ein Verstoß gemeldet werden?

Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn z. B. der Verlust von Daten zu einem Risiko für die Rechte und Freiheiten der betroffenen Person führen kann. Der Verstoß muss innerhalb von 72 Stunden an die Datenschutzaufsicht gemeldet werden. Die Aufsichtsbehörden halten dafür ein Online-Meldeformular vor. Die betroffene Person muss ebenfalls informiert werden.

Stand: 24.01.2020

>zurück<