FAQ ZUR DSGVO

Kunden fragen – unser Experte antwortet!

Haben auch Sie konkrete Fragen zur DSGVO? Der **Fachanwalt und Autor Dr. Martin Schirmbacher** hat bereits zahlreiche Fragen beantwortet, die unsere Kunden in seiner Online-Schulung gestellt haben. Profitieren auch Sie von diesem Wissen!

Allgemeine Fragen

Wie soll ein Ein-Mann-Unternehmen bezüglich DSGVO vorgehen?

Antwort: Auch für ein Ein-Mann-Unternehmen gilt die DSGVO. Allerdings ist ein Datenschutzbeauftragter nicht zu bestellen. Mein Rat ist: Führen Sie ein Verarbeitungsverzeichnis und beachten Sie die Betroffenenrechte und Meldepflichten. Aktualisieren Sie vor allen Dingen die Datenschutzhinweise auf Ihrer Website. Viele Interessenverbände haben inzwischen Muster zur Verfügung gestellt. Falls Sie hier nicht fündig werden, sollten Sie sich Rechtsrat einholen.

Aufbewahrungsfristen nach deutschem Recht vs. DSGVO: was gilt?

Antwort: Hier gilt nicht entweder/oder! Wenn das deutsche Recht eine Pflicht zur Aufbewahrung von Unterlagen vorsieht, liegt in der Regel auch eine Rechtfertigung nach der DSGVO vor. Allerdings muss im Einzelnen geprüft werden, worauf sich die Löschfrist bezieht. Nur solche personenbezogenen Daten dürfen gespeichert bleiben, die aufgrund des jeweiligen Gesetzes von der Aufbewahrungspflicht umfasst sind.

Welche Behörde prüft denn, ob die Vorschriften nach DSGVO eingehalten werden?

Antwort: Zuständig ist jeweils die Aufsichtsbehörde am Sitz des Unternehmens. In Deutschland hat jedes Bundesland eine für den Datenschutz im nicht öffentlichen Bereich zuständige Behörde. Eine vollständige Liste gibt es hier: www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

An wen kann ich mich wenden, wenn ich weitere Fragen zur DSGVO habe?

Antwort: Die Datenschutzbehörden sind grundsätzlich gehalten, Unternehmen bei der Umsetzung der Vorgaben der DSGVO zu unterstützen. Einzelne Fragen kann man daher an die Aufsichtsbehörde richten. Ansonsten ist empfehlenswert, Datenschutzberater oder spezialisierte Rechtsanwälte zu konsultieren.

Fragen zum Verarbeitungsverzeichnis

Wer muss ein Verarbeitungsverzeichnis erstellen?

Antwort: Jedes Unternehmen, das personenbezogene Daten verarbeitet, muss im Zweifel in der Lage sein nachzuweisen, dass es sich datenschutzkonform verhält. Es besteht eine Verpflichtung, ein Verzeichnis über die Verarbeitungstätigkeiten zu führen, wenn das Unternehmen mehr als 250 Mitarbeiter hat. Doch auch Unternehmen mit weniger Angestellten müssen ein solches Verzeichnis führen, wenn die Verarbeitung nicht nur gelegentlich erfolgt oder besondere Datenkategorien, etwa Gesundheitsdaten, verarbeitet werden. Wann eine Verarbeitung nicht nur gelegentlich erfolgt, ist bisher nicht klar. Man wird davon ausgehen müssen, dass die allermeisten Unternehmen ein Verzeichnis führen müssen.

Wie muss ein Verarbeitungsverzeichnis aussehen?

Antwort: Der Mindestinhalt des Verzeichnisses ergibt sich aus Art. 30 DSGVO. Danach muss Name und Zweck der Datenverarbeitung und die Rechtsgrundlage angegeben werden. Für jedes einzelne Verfahren müssen die betroffenen Personengruppen und die konkrete Art der Daten angegeben werden. Gesondert zu kennzeichnen ist, wenn es sich um besondere Arten personenbezogener Daten handelt (z. B. Gesundheitsdaten).

Zudem bietet es sich an, jedem Verfahren eine kurze Beschreibung beizufügen. Diese muss nicht jedes Detail enthalten, es sollte aber deutlich werden, wie die Datenverarbeitung erfolgt. Hierzu kann es sinnvoll sein, aus dem Verzeichnis auf eine ausführlichere Prozessbeschreibung zu verweisen.

Bisweilen schwierig aber notwendig ist die Angabe, wie lange die Daten zu speichern sind. Dazu bedarf es zunächst eines Löschkonzepts, aus dem sich die einzelnen Löschfristen ergeben.

Weitere Informationspflichten beziehen sich auf die Angabe einer allgemeinen Beschreibung der eingesetzten technischen und organisatorischen Maßnahmen für den Datenschutz. Hierbei spielt insbesondere ein Zugriffsberechtigungskonzept eine wichtige Rolle. Angegeben werden muss zudem, wenn die Daten außerhalb der europäischen Union verarbeitet werden sollen.

Das Verzeichnis kann elektronisch, etwa in Excel oder Word geführt werden. Viele Verbände haben für ihre Mitglieder Musterverzeichnisse entwickelt. Auf dieser Webseite stellt Lexware Ihnen ein Muster zur Verfügung: https://www.lexware.de/dsgvo/mustervorlagen

Fragen zu Kundendaten

Muss ich bei meinen Kunden eine Einwilligungserklärung einholen oder ggf. nur bei neuen Kunden nach dem 25. Mai 2018?

Antwort: Ob eine Einwilligung erforderlich ist oder ob die Datenverarbeitung etwa auf einen Vertrag oder berechtigte Interessen gestützt werden kann, muss für jeden einzelnen Datenverarbeitungsvorgang isoliert betrachtet werden. Für Newsletter- Werbung per E-Mail ist in jedem Falle eine Einwilligung erforderlich. Dabei gelten jedoch in der Regel bisher eingeholte Einwilligungen weiter.

Muss jeder Kunde angeschrieben und darüber informiert werden, welche Daten wir von ihm speichern?

Antwort: In der Tat sieht die Verordnung vor, dass die Betroffenen über jede Datenverarbeitung zu informieren sind. Online kann dies über die Website erfolgen. Bei Katalogbestellungen sollte die Erklärung zum Datenschutz im Katalog abgedruckt werden. Am Point-of-Sale können Datenschutzinformationen ausgelegt werden. Schwierig ist die Information aber zum Beispiel am Telefon. Inwieweit Medienbrüche zulässig sind und etwa ein Verweis auf die Website erfolgen kann, ist bisher unklar.

Reicht es, wenn auf der Homepage eine Datenschutzerklärung zu finden ist oder muss man diese von seinen Kunden unterschreiben lassen?

Antwort: Für Online-Bestellungen ist es ausreichend, wenn die Hinweise zum Datenschutz in der Datenschutzerklärung zu finden sind. Dabei sollte die Erklärung unmittelbar bei der Datenerhebung verlinkt sein. Eine ausdrückliche Bestätigung wie: „Ich habe die Datenschutzerklärung gelesen und bin damit einverstanden“, oder gar eine Unterschrift sind nicht erforderlich.

Darf ich öffentlich zugängliche Daten in meinem CRM-System speichern?

Antwort: Datenschutzrechtlich stellt sich die Frage nur bei personenbezogenen Daten. Für reine Unternehmenskennzahlen etwa gibt es keine datenschutzrechtlichen Beschränkungen.

Auch die Erhebung und Nutzung von öffentlich zugänglichen personenbezogenen Daten ist grundsätzlich gestattet. Problematisch kann aber die gezielte Anreicherung von bereits vorhandenen Informationen im CRM sein. Hier sollte man sich genau anschauen, ob eine einwilligungsbedürftige Profilbildung vorliegt. Außerdem muss der Betroffene über die Datenerhebung informiert werden.

Darf ich meinen Kunden noch zum Geburtstag gratulieren/frohe Weihnachten wünschen?

Antwort: Unproblematisch ist das, wenn eine Einwilligung des Kunden vorliegt. Ansonsten ist es in der Tat schwierig. Möglich ist allenfalls ein postalischer Gruß. Und dafür sind die beteiligten Interessen miteinander abzuwägen. Während für die Unternehmen der Kundenservice und die Umsatzmehrung spricht, haben die Kunden ein Interesse daran, dass ihr Geburtsdatum nicht für Werbezwecke verwendet wird.

Am Ende kommt es auf die vernünftigen Erwartungen der Kunden an. Wer sich in einer intensiven Kundenbeziehung befindet und bisher Geburtstagswünsche erhalten hat, wird damit auch in Zukunft rechnen. Wer z. B. sein Geburtsdatum angeben musste, um die Volljährigkeit zu prüfen, wird nicht mit einem Geburtstagsgruß rechnen.

Fragen zum Datenschutzbeauftragten

Welche Unternehmen benötigen einen Datenschutzbeauftragten?

Antwort: In Deutschland brauchen alle Unternehmen einen Datenschutzbeauftragten, bei denen mehr als 10 Mitarbeiter ständig mit der Datenverarbeitung befasst sind.

Außerdem muss ein Datenschutzbeauftragter ernannt werden, wenn die Kerntätigkeit des Unternehmens in einer Datenverarbeitung liegt, die mit der Überwachung von Personen zusammenhängt. Auch wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten, insbesondere Gesundheitsdaten besteht, muss ein Datenschutzbeauftragter bestellt werden. Darunter fallen jedenfalls Krankenhäuser und Labore.

Benötigen Unternehmen/Freiberufler, die besonders sensible Daten verarbeiten, wie etwa Steuerberater, Ärzte und Anwälte, einen Datenschutzbeauftragten auch bei weniger als 10 Mitarbeitern?

Antwort: Nein. Allein die Tatsache, dass auch sensible Daten verarbeitet werden, führt nicht zur Pflicht, einen Datenschutzbeauftragten benennen zu müssen.

Wer im Unternehmen soll/darf Datenschutzbeauftragter werden – GF, IT-ler, Assistentin?

Antwort: Die Anforderungen an einen Datenschutzbeauftragten sind nicht hoch. Die Person muss ein Mindestmaß an Sachkunde aufweisen, sollte also jedenfalls eine entsprechende Schulung durchlaufen haben. Allerdings sind Mitglieder der Geschäftsleitung davon ausgeschlossen, Datenschutzbeauftragter zu werden. Auch der IT-Leiter sollte nicht die Stelle sein, die die Einhaltung der Datenschutzvorschriften im Unternehmen prüft.

Fragen zu Mitarbeiterdaten

Sollte man zur Sicherheit einen § in den Arbeitsvertrag aufnehmen, damit die Mitarbeiter unterschreiben können, dass sie mit der Datenverarbeitung einverstanden sind?

Antwort: Es kommt darauf an, für welche Datenverarbeitung die Einwilligung gelten soll. Für die Standardprozesse ist das nicht erforderlich – und auch nicht sinnvoll. Eine Einwilligung im Arbeitsverhältnis ist meist problematisch. Oberstes Gebot ist die Freiwilligkeit. Nur wenn die Einwilligung wirklich aus freien Stücken erfolgt, ist sie wirksam. Außerdem kann sie jederzeit widerrufen werden, weshalb sie deutlich weniger als Rechtsgrundlage für die Verarbeitung von Daten im Arbeitsverhältnis geeignet ist.

Muss ich jeden Mitarbeiter darüber informieren, was wir im Personalstammblatt speichern?

Antwort: Ja. Das kann zum Beispiel als Anlage zum Arbeitsvertrag geschehen.

Spezielle Fragen

Welche Auswirkungen hat die DSGVO auf (Zahn-) Arztpraxen?

Antwort: Arztpraxen sind zunächst einmal Unternehmen wie andere auch, so dass die allgemeinen Voraussetzungen gelten. Die Bundeszahnärztekammer hat ein Merkblatt veröffentlicht, in dem viele Details angesprochen sind: www.bzaek.de/fileadmin/PDFs/b/datenschutz_zahnarzt.pdf

DSGVO bei Vereinen – auf was ist zu achten?

Antwort: Auch für Vereine gilt die DSGVO. Das bedeutet zum Beispiel, dass ggf. ein Datenschutzbeauftragter zu bestellen ist und insbesondere das Mitgliedermanagement auf den Prüfstand gehört.

Was müssen wir als Kleinunternehmen (Druckerei unter 10 Mitarbeiter) tun, wenn wir Adressdaten von Kunden zum Druck von Mailings erhalten. Reicht eine Einwilligungserklärung für die Verwendung der Adressen?

Antwort: Als Druckerei verarbeitet Sie die Daten im Auftrag Ihrer Kunden. Sie sollten sich einen Standardvertrag für eine Datenverarbeitung im Auftrag fertigen lassen und den Kunden jeweils akzeptieren lassen. Das geht auch online und möglicherweise sogar als Annex zu Ihren AGB.

Hinweis: Die Beantwortung der Fragen erfolgt nach bestem Wissen und neuestem Kenntnisstand. Die Komplexität und der ständige Wandel der Rechtsmaterie machen es jedoch unabdingbar, insoweit jegliche Haftung und Gewähr auszuschließen.