FAQs: Häufig gestellte Fragen zur DSGVO – und die Antworten darauf

Für wen gilt die DSGVO?
Die DSGVO gilt für alle Stellen, für Behörden (öffentliche Stellen) genauso wie für Unternehmen (nicht-öffentliche Stellen). Sobald personenbezogene Daten (zum Beispiel Adressen, Bankverbindungen, Geburtsdaten, Bewerbungsbögen, Telefonnummern, E-Mail-Adressen) erhoben, verarbeitet, weitergeleitet oder gelöscht werden, müssen die geltenden Pflichten und Regeln zum Thema Datenschutz angewendet werden, unabhängig von der Anzahl der Mitarbeiter. Die DSGVO betrifft demzufolge auch Einzelunternehmen und den B-to-B-Bereich.

Ich bin Einzelmakler und verarbeite Gesundheitsdaten. Benötige ich einen Datenschutzbeauftragten?
Einen Datenschutzbeauftragten benötigen Sie nur, wenn Sie sehr umfangreich (massenhaft) Gesundheitsdaten verarbeiten. Das machen regelmäßig nur Krankenhäuser oder Suchmaschinen. Nach derzeitigem Stand trifft dies auf Einzelmakler ganz überwiegend nicht zu.

Welche Form muss die Einwilligung haben, die bei Kunden einzuholen ist?
Wir empfehlen die elektronische oder schriftliche Form. Eine Einwilligung per E-Mail reicht aus, wenn zum Beispiel der Kunde nach einem Telefonat und anschließender Zusendung einer E-Mail seine Zustimmung per E-Mail erteilt. Sie benötigen in diesem Fall keine Unterschrift des Kunden. Protokollieren Sie die Zustimmung in seiner Kundenakte.

Muss ich die Einwilligungen von Bestandskunden erneuern?
Wenn Sie eine rechtswirksame Einwilligungserklärung Ihrer Kunden haben, müssen Sie keine neue Einwilligung einholen. Dennoch können Sie Ihre Bestandskunden über die geänderten Informationspflichten und die insoweit neuen Datenschutzhinweise in Kenntnis setzen. Dies kann auch per E-Mail erfolgen.

Was ist bei der Einwilligung zum Erhalt eines Newsletters zu beachten?
Bei dieser Einwilligung ist das Double-Opt-In Verfahren anzuwenden.

1. Der Nutzer trägt seine E-Mail Adresse in ein Formularfeld ein und willigt mittels Opt-In Verfahren (er setzt aktiv ein Häkchen in die Checkbox) in den Erhalt des Newsletters ein, der durch das Absenden des Formulars bestellt wird.
2. Der Nutzer erhält eine Verifizierungs-E-Mail an die hinterlegte Adresse, die einen Bestätigungslink enthält. Diesen Link klickt der Nutzer an, um den Newsletter erfolgreich zu abonnieren. Beide Schritte müssen mit entsprechenden Zeitstempeln und nicht-anonymisierter IP-Adresse gespeichert werden.

Welche Rechte haben Betroffene?

Recht auf Auskunft
Jede betroffene Person (zum Beispiel ein Kunde) kann mit einem formlosen Antrag eine Auskunft über alle bei Ihnen gespeicherten personenbezogenen Daten sowie insbesondere eine Kopie dieser Daten verlangen.

Recht auf Berichtigung
Mit diesem Recht kann die betroffene Person von Ihnen unverzüglich die Berichtigung unrichtiger eigener personenbezogener Daten verlangen.

Recht auf Löschung/Recht auf Vergessenwerden
Auf Verlangen der betroffenen Person sind sämtliche personenbezogenen Daten zu löschen, soweit nicht gesetzliche Aufbewahrungspflichten oder eigene berechtigte Interessen (Geltendmachung oder Abwehr von Ansprüchen) entgegenstehen. Außerdem müssen Sie sicherstellen, dass auch Dritte, denen Sie die Daten weitergegeben haben, dem Löschungswunsch Folge leisten.

Recht auf Datenübertragbarkeit
Jede betroffene Person kann verlangen, dass Sie sämtliche Daten so zur Verfügung stellen, dass diese problemlos zum Beispiel zu einem Wettbewerber „mitgenommen" werden können. Die betroffene Person hat sogar ein Recht darauf, dass Sie die Daten unmittelbar an einen anderen (zum Beispiel einem Wettbewerber) weitergeben.

Widerspruchsrecht
Mit dem Widerspruchsrecht kann die betroffene Person der Verarbeitung der eigenen Daten zu Werbezwecken widersprechen. Bei Vorliegen besonderer Gründe kann auch einer ursprünglich rechtmäßigen Verarbeitung widersprochen werden.

Automatisierte Entscheidung im Einzelfall
Jede betroffene Person hat das Recht, dass keine Entscheidung über sie erfolgt, die ausschließlich auf einer automatisierten Verarbeitung basiert. (Beispiel: Bonitätsprüfung und -einstufung ausschließlich auf Grundlage automatisierter Verarbeitungen).

Recht auf Widerruf einer Einwilligung
Jede betroffene Person hat das Recht, eine einmal erteilte Einwilligung jederzeit zu widerrufen. Dies muss genauso einfach möglich sein wie die Einwilligung selbst.

Welche Angaben zu den beauftragten Dienstleistern (Empfängern) gehören in die Einwilligungserklärung?
Die DSGVO gibt in Art. 13 Abs. 1 lit e) vor, dass in der Einwilligungserklärung gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten mitgeteilt werden. Eine Nennung der einzelnen konkreten Empfänger ist nicht erforderlich.

Reicht es aus, wenn der Kunde unserer Datenschutzerklärung per E-Mail zustimmt?
Es reicht, wenn der Kunde seine Zustimmung per E-Mail erteilt. Sie benötigen in diesem Fall keine Unterschrift des Kunden. Protokolieren Sie die Zustimmung in seiner Kundenakte.

Wie muss ich E-Mails verschlüsseln? Reicht eine vorhandene SSL-Verschlüsselung der ausgehenden E-Mail aus?
Die Transportverschlüsselung von E-Mails mit TLS ist für die reine Kommunikation, also den Text der E-Mail, sowie die genutzten Kontaktdaten ausreichend.

Wie muss die Verschlüsselung von E-Mail Anhängen erfolgen?
Sobald Sie jedoch Anhänge versenden (wie Anträge, Fragebögen oder Ähnliches), in denen personenbezogene Daten enthalten sind, empfehlen wir diese Anhänge mit einer gängigen Verschlüsselungsmethode zu sichern (Zip-Datei verschlüsseln, Zertifikate einsetzen).

Welche Programme kann ich zur Verschlüsselung nutzen?
Diese Frage wird im Datenschutzkonzept in der Anlage 1: Datensicherheitskonzept im Kapitel "Technische und Organisatorische Maßnahmen nach DSGVO / § 64 BDSG (neu)" Punkt 3 beantwortet.

Wie nehme ich eine Pseudonymisierung vor?
Unabhängig davon, ob Sie mit einem Kundenverwaltungsprogramm arbeiten oder mit einer klassischen Ordnerstruktur, erreichen Sie eine Pseudonymisierung bereits durch eine Verschlüsselung des Datensatzes. Die Verschlüsselung stellt insoweit einen Unterfall der Pseudonymisierung dar. Eine Pseudonymisierung können Sie zum Beispiel über Kreuztabellen lösen: Sie erfassen die personenbezogen Daten in zwei verschiedenen Tabellen. Tabelle 1 enthält alle personenbezogen Daten der Kunden und die entsprechende individuelle Kunden- oder Vertragsnummer, Kunden-ID, etc., Tabelle 2 enthält die entsprechende individuelle Kunden- oder Vertragsnummer und alle Angaben zu Angeboten und dem Vertragswerk. Tabelle 2 sollten Sie separat von Tabelle 1 auf einem getrennten Ort (externe Festplatte) speichern.

Mit wem muss ich einen Auftragsverarbeitungsvertrag (AVV) abschließen?
Einen solchen Vertrag müssen Sie mit Personen oder Firmen schließen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, zum Beispiel mit dem Büro, das Ihre Lohnabrechnung übernimmt, mit Aktenvernichtern, IT-Dienstleistern usw. Eine Reinigungskraft sollte keinen Zugang zu personenbezogenen Daten haben, wir empfehlen Ihnen eine „Clean-Desk-Policy“, ein AVV ist dann nicht notwendig.

Muss ich mit Google, Microsoft, Telekom (Telefon und E-Mailadressen) einen AVV schließen?
Wenn Sie Google, Microsoft oder die Telekom nicht mit der Verarbeitung sensibler Daten (Erhebung, Speicherung oder Ähnliches) beauftragt haben, benötigen Sie keinen solchen Vertrag.

Darf ich Whatsapp weiterhin für die Kundenkommunikation nutzen?
Grundsätzlich ist eine rechtskonforme Nutzung des Messenger-Dienstes wohl möglich. Es ist jedoch erforderlich, dass Sie von **jedem** geschäftlichen Kontakt die Einwilligung einholen, dass seine Daten an Whatsapp übermittelt werden dürfen. Das gilt **insbesondere**, wenn dieser Kontakt Whatsapp selbst nicht nutzt. Denn: Whatsapp greift **alle** Kontaktdaten aus dem Telefonbuch des Nutzers ab. Außerdem ist von den Kontakten, mit denen Sie Daten wie Bilder oder Ähnliches über Whatsapp tauschen wollen, ebenfalls eine Einwilligung zur Weitergabe dieser Daten an Whatsapp erforderlich. Soweit Sie nicht von **allen** dienstlichen Kontakten eine Einwilligung vorliegen haben, müssen Sie Whatsapp von diesem Handy entfernen. Die Nutzung eines Diensthandys, auf dem ausschließlich Kontakte liegen, die Ihnen eine Einwilligung erteilt haben, wäre die Konsequenz. Vor diesem Hintergrund halten wir eine berufliche Nutzung von Whatsapp derzeit für nicht empfehlenswert

Darf ich Daten ins Ausland übermitteln?
Innerhalb der Europäischen Union (EU) ist eine Datenübermittlung beim Vorliegen einer entsprechenden Rechtsgrundlage möglich, da die DSGVO in der ganzen EU gilt. Für andere Staaten muss entweder ein Angemessenheitsbeschluss der EU-Kommission oder ein Datenschutzübereinkommen vorliegen. Für die USA ist es das „Privacy Shield“, in dem alle Unternehmen gelistet und zertifiziert sind (https://www.privacyshield.gov/list). Gemäß Art. 46 Abs. 1 DSGVO werden Datenübermittlungen in einen unsicheren Drittstaat erlaubt, wenn die verantwortliche Stelle oder der Auftragsverarbeiter geeignete Garantien vorsieht. Für den Betroffenen müssen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Die sogenannten „Binding Corporate Rules (BCR)“ müssen von den Aufsichtsbehörden genehmigt werden. In Artikel 47 Abs. 2 DSGVO wird der Mindestumfang genau definiert.

Quelle: Kanzlei Wirth-Rechtsanwälte, Berlin