DATENSCHUTZ – D09

Stand: August 2023

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

FAQ zur DSGVO

Die umfangreichen Vorschriften der DSGVO stellen gerade kleinere und mittlere Unternehmen vor die Frage: Wo fange ich an? Was muss ich tun? Mit Hilfe dieser FAQ wollen wir Ihnen die Umsetzung der DSGVO erleichtern.

1. Für wen gilt das Datenschutzrecht?

Die DSGVO gilt für alle Verarbeitungen, die sich an EU-Bürger richten und personenbezogene Daten von EU-Bürgern erfassen.

Beispiel: *Ein amerikanisches Unternehmen bietet in seinem Online-Shop Waren an deutsche Kunden an. Für den Vertragsabschluss werden personenbezogene Daten des deutschen Kunden verarbeitet. In diesem Fall hat das amerikanische Unternehmen die Regelungen der DSGVO zu beachten.*

2. Was gilt in Deutschland?

Die Datenschutzgrundverordnung gilt unmittelbar auch in Deutschland. Neben der DSGVO gelten in Deutschland zudem weitere datenschutzrechtliche Spezialgesetze, wie etwa das Bundesdatenschutzgesetz (BDSG). Das BDSG ist immer in Verbindung mit der DSGVO zu lesen. Dort finden sich Konkretisierungen, insbesondere zum betrieblichen Datenschutzbeauftragten oder zum Beschäftigtendatenschutz.

3. Welche Arten von Daten sind durch die DSGVO geschützt?

Die DSGVO gilt, wenn Unternehmen sog. personenbezogene Daten verarbeiten.

Personenbezogene Daten sind alle Informationen, die sich direkt oder indirekt (z. B. über eine Kennung) auf einen Menschen 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.

Darunter fallen beispielsweise:

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail-Adresse
- Konto-, Kreditkartennummer

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland │ 66104 Saarbrücken │ Büroanschrift: Franz-Josef-Röder-Straße 9 │ 66119 Saarbrücken
Tel. 0681/9520-0 │ Fax 0681/9520-888 │ E-Mail: info@saarland.ihk.de │ Internet: www.saarland.ihk.de

- Bonitätsdaten
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweisnummer, Sozialversicherungsnummer
- IP-Adresse
- genetische Daten und Krankendaten
- Fotos

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

Durch die DSGVO werden alle Arten von personenbezogenen Daten geschützt, unabhängig davon, um welche Kategorie von Personen es geht, also ob es sich hierbei um

- Mitarbeiter-,
- Geschäftspartner-, Kunden- oder
- Lieferantendaten

handelt.

4. Müssen auch Kleingewerbetreibende die DSGVO beachten?

Ja, die DSGVO gilt sowohl für große als auch für kleine Unternehmen. Kleine Unternehmen sind lediglich von einzelnen wenigen Pflichten ausgenommen; dies betrifft etwa unter Umständen die Pflicht zur Bestellung eines Datenschutzbeauftragten.

➔**D06** „Betrieblicher Datenschutzbeauftragter, Kennzahl 2356

Ansonsten müssen auch von kleineren Unternehmen sämtliche Vorgaben umgesetzt werden, denn unter die DSGVO fällt jede Stelle – also jedes Unternehmen, unabhängig von der Mitarbeiterzahl oder Branche – die personenbezogene Daten innerhalb der EU verarbeitet.

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

Datenschutz gilt grundsätzlich auch im Geschäftsverkehr mit anderen Unternehmen. Einzelangaben über juristische Personen, wie z. B über Kapitalgesellschaften oder eingetragene Vereine, sind keine personenbezogenen Daten. Etwas anderes gilt, 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 Ein-Mann-GmbH der Fall sein.

In der Regel haben Sie bei Firmenkunden einen **Ansprechpartner** und erheben Daten wie Name, personalisierte E-Mail-Adresse, Funktion im Unternehmen usw. Hierbei handelt es sich um personenbezogene Daten, sodass die DSGVO zu beachten ist.

6. Wie sieht eine Einwilligung aus?

Die Einwilligung setzt eine **freiwillige, informierte und eindeutige Handlung** voraus. Unwirksam sind Erklärungen, die bei einem **„klaren Ungleichgewicht“** zwischen Verantwortlichen und Betroffenen getroffen werden. **Minderjährige** unter 16 Jahren können keine wirksamen Einwilligungserklärungen abgeben. Es bedarf vielmehr der Einwilligung der Erziehungsberechtigten. Gekoppelte Einwilligungen, also bei dem ein Vertragsschluss von der Verarbeitung personenbezogener Daten abhängig gemacht wird (z.B. Kauf im Onlineshop nur möglich, wenn Newsletter abonniert wird), sind unwirksam, wenn sie sich auf Daten erstrecken, die zur Erfüllung des Vertrages nicht erforderlich sind (sog. **Kopplungsverbot**).

Vorangekreuzte Kästchen reichen nicht aus. Der Betroffene muss seine Einwilligung **aktiv** abgeben. Es muss zudem die Möglichkeit bestehen und auch darüber informiert werden, die Einwilligung **jederzeit widerrufen** zu können.

➔**D02** „Einwilligung nach der DSGVO“, Kennzahl 2356

7. Welche Informationspflichten bestehen?

Die DSGVO sieht eine Vielzahl von Informationspflichten vor. Dazu gehören z.B. Informationen zur Rechtsgrundlage für die Verarbeitung, Angaben zur Dauer der Speicherung und Angaben zu möglichen Empfängern der Daten. Die Informationen müssen in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache gegeben werden.

➔**D05** „Informationspflichten nach der DSGVO“, Kennzahl 2356

Praxistipp: *Die Informationen können beispielsweise im Rahmen der Datenschutzerklärung auf der Homepage bereitgestellt werden.*

➔**D07** „Die Datenschutzerklärung nach der DSGVO“, Kennzahl 2356

8. Welche Dokumentationspflichten bestehen? Was bedeutet die Rechenschaftspflicht?

Zweck der DSGVO ist es vor allem, mehr Transparenz über Datenverarbeitungen gegenüber dem Betroffenen zu schaffen und dessen Rechte (Auskunft über gespeicherte Daten, Berichtigung oder Löschen von Daten etc.) zu stärken.

Die DSGVO betont die Verantwortlichkeit, die Unternehmen für die Einhaltung des Datenschutzes haben. Sie müssen gegenüber der Landesdatenschutzaufsicht nachweisen können, dass Sie aktiv Maßnahmen zur Einhaltung der Datenschutzprinzipien und zur Sicherung der Datenverarbeitung umsetzt haben und ihre Datenverarbeitung datenschutzkonform ist (sog. **Rechenschaftspflicht**, Art. 5 Abs. 2 DSGVO). Dies gelingt nur über eine umfassende Dokumentation (Datenschutz-Management-System).

➔**D04** „Dokumentationspflichten nach der DSGVO“, Kennzahl 2356

9. Verzeichnis von Verarbeitungstätigkeiten: Brauche ich sowas?

In diesem Verzeichnis müssen alle Verarbeitungsprozesse personenbezogener Daten erfasst werden. Da die meisten Unternehmen nicht nur gelegentlich personenbezogene Daten verarbeiten, sind auch die meisten Unternehmen verpflichtet, ein solches Verzeichnis zu führen.

➔**D11** „Verzeichnis von Verarbeitungstätigkeiten“, Kennzahl 2356

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

Für die Verarbeitung von personenbezogenen Daten benötigen Sie eine datenschutzrechtliche Rechtsgrundlage (**Grundsatz des Verbots mit Erlaubnisvorbehalt**). Rechtsgrundlage kann sein:

- der Vertrag
- eine Einwilligung
- das Gesetz oder
- ein berechtigtes Interesse.

Beruht die Datenverarbeitung auf einer vertraglichen Basis, um den Vertrag abzuwickeln, sind Einwilligungen für die Erhebung und Verarbeitung der Daten nicht erforderlich.

Aber: Sollen die so erhobenen Daten für andere Zwecke als die Vertragsabwicklung verarbeitet werden (z. B. Versand von Newslettern, E-Mail-Grüße zum Geburtstag), so bedarf es einer Einwilligung für den neuen Zweck.

11. Wann müssen personenbezogene Daten gelöscht werden?

Personenbezogene Daten müssen grundsätzlich gelöscht werden, wenn diese für den Geschäftsprozess **nicht mehr erforderlich** sind, d.h. der Zweck, für den sie erhoben worden sind, erfüllt ist. Dabei sind jedoch die **gesetzlichen Aufbewahrungsfristen** zu beachten, z. B 6 bzw. 10 Jahre bei Geschäftsbriefen. Grundsätzlich empfiehlt sich für jedes Unternehmen, ein sog. „Löschkonzept“ aufzusetzen. Dies ist wichtig, um dem Grundsatz der Datenminimierung nach der DSGVO nachzukommen.

12. Benötigt mein Unternehmen einen Datenschutzbeauftragten?

Die Verpflichtung, einen **betrieblichen Datenschutzbeauftragten** zu bestellen, besteht, soweit im **Betrieb in der Regel mindestens zwanzig Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Eine Verpflichtung besteht auch dann, wenn die **Kerntätigkeit** des Unternehmens die regelmäßige und systematische Beobachtung Betroffener umfasst oder die **Kerntätigkeit** in der massenhaften Verarbeitung sensibler Daten besteht (Art. 37 DSGVO).

Beispiel: *Die Verarbeitung von Gesundheitsdaten durch einen Versicherungsvermittler stellt nicht seine Kerntätigkeit dar. Aus diesem Grund benötigt er einen Datenschutzbeauftragten nur, wenn er in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.*

➔ **D06** „Betrieblicher Datenschutzbeauftragter“, Kennzahl 2356

Achtung: *Auch wenn keine Bestellpflicht besteht, muss trotzdem der Datenschutz im Unternehmen gewahrt und die genannten Maßnahmen ergriffen werden. Aufgaben, die klassischerweise dem Datenschutzbeauftragten übertragen werden, muss dann die Geschäftsführung selbst erledigen. Datenschutz ist und bleibt Chefsache*!

13. Was muss ich bei der Berechnung der Personenanzahl von 20 beachten?

Grundsätzlich sind sämtliche Personen, die mit der entsprechenden Verarbeitung beschäftigt sind, zu berücksichtigen, unabhängig von ihrem arbeitsrechtlichen Status als Arbeitnehmer, freie Mitarbeiter, Auszubildende, Praktikanten, Teilzeitkräfte, etc.

Eine zeitweise und kurzfristige Unter- bzw. Überschreitung der maßgeblichen Personenzahl ist unerheblich. Die Person muss regelmäßig mit der automatisierten Verarbeitung beschäftigt sein.

Automatisierte Verarbeitung meint IT-gestützte Datenverarbeitung, wie sie mittels Mainframe, Personal Computern (Desktop und Laptop Computern), aber mittlerweile auch mittels Smartphones, Tablet PCs und anderen mobilen Endgeräten erfolgt.

Der Begriff "ständig“ bedeutet nicht notwendig dauernd, verlangt aber, dass die Tätigkeit **auf Dauer angelegt** ist und die betreffende Person immer dann Daten verarbeitet, wenn es notwendig ist, selbst wenn die Tätigkeit nur in zeitlichen Abständen (z. B. monatlich) anfällt.

14. Wer kann betrieblicher Datenschutzbeauftragter werden?

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 bis zu einem Jahr nach Beendigung seiner Tätigkeit als Datenschutzbeauftragter fort.

Schulungen und Seminare zum Datenschutz können Sie im WIS - Weiterbildungs-Informations-System unter www.wis.ihk.de finden. Informationen zum IHK-Zertifikatslehrgang „Koordinator für Datenschutz, Datensicherheit und IT-Sicherheit (IHK)“ finden Sie hier.

15. Wo finde ich einen externen Datenschutzbeauftragten? Worauf ist bei der Beauftragung zu achten?

Vereine und Berufsverbände, wie etwa die Gesellschaft für Datenschutz und Datensicherheit e.V. (https://www.gdd.de/der-datenschutzbeauftragte) oder der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. https://www.bvdnet.de/), können Ihnen konkrete Kontakte vermitteln können. Rechtsanwälte aus dem Bereich Datenschutzrecht finden Sie bei unter www.saaranwalt.de.

Bei der Auswahl eines externen Datenschutzbeauftragten empfiehlt es sich, mehrere Angebote mit Referenzen einzuholen und die Leistungen und Kosten zu vergleichen. Sie sollten für das Angebot vordefinieren, welche Leistungen Sie abgedeckt sehen wollen (z. B. Beratung im Alltagsgeschäft. Erstellung/Überprüfung von Dokumenten (Verarbeitungsverzeichnis, Datenschutzerklärung, technisch-organisatorische Maßnahmen)).

16. Gilt das Datenschutzrecht auch bei Papierakten?

Ja, die DSGVO unterscheidet nicht zwischen der Verarbeitung von Daten auf Papier oder in elektronischer Form. 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.

17. Darf ich die Daten meiner Mitarbeiter verarbeiten?

Die Daten von Bewerbern, 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 eine Einwilligung erforderlich.

Die Mitarbeiter sind über die Datenverarbeitung zu informieren. Dabei sind die Vorgaben des Art. 13 DSGVO zu beachten.

➔**D10** „Beschäftigtendatenschutz nach der DSGVO“, Kennzahl 2356

18. Auftragsverarbeitung (AV)

Das Unternehmen als verantwortliche Stelle ist für die Rechtmäßigkeit der Verarbeitung auch dann verantwortlich, wenn es dazu einen externen Dienstleister beauftragt (z.B. für die Betreuung der Unternehmenshomepage). Der externe Dienstleister hat in diesem Fall Zugriff auf die personenbezogenen Daten. In einem solchen Falle muss er neben dem eigentlichen Auftrag (= Betreuung der Homepage) noch eine Vereinbarung über die Auftragsverarbeitung geschlossen werden. Der Auftragsverarbeiter muss sorgfältig ausgewählt werden, d.h. es dürfen nur solche Auftragsverarbeiter eingesetzt werden, die angemessene technische und organisatorische Maßnahmen zum Schutz der Daten getroffen haben und so eine Garantie für einen ausreichenden Datenschutz bieten.

Eine Auftragsverarbeitung liegt nur dann vor, wenn der Dienstleister streng nach einem zuvor definierten Verfahren vorgeht, keinen eigenen Gestaltungs- und Ermessenspielraum hat und gegenüber dem Auftraggeber im Hinblick auf die Ausführung der vereinbarten Tätigkeit weisungsgebunden ist. Kurzum: Wenn man den Dienstleister sinnbildlich als „verlängerte Werkbank“ des Auftraggebers betrachten kann.

Darunter fallen z. B. auch sog. Trackingsysteme, mit denen nachvollzogen werden kann, wer welche Webseiten besucht hat. Gibt es zudem dadurch Auslandsbezug, weil das Tracking-Unternehmen seinen Sitz z. B. in den USA hat, müssen weitere datenschutzrechtliche Anforderungen erfüllt werden. Gleiches gilt für die Nutzung von Cloud-Anwendungen oder die Verwendung von Social Plugins auf den Webseiten, also die Einbindung sozialer Medien.

Liegt eine AV vor, ist eine vorherige Einwilligung der Kunden, deren Daten verarbeitet werden, nicht erforderlich.

➔**D12** „Auftragsverarbeitung nach der DSGVO“, Kennzahl 2356

Einen Mustervertrag finden Sie hier:
https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/datenschutz/ds-gvo/kurzpapiere/Auftragsverarbeitungsvertrag_Formulierungshilfe_3-2018_web.pdf

Weitere Informationen finden Sie im Kurzpapier der Datenschutzkonferenz (DSK)
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

19. Muss ich auch das Thema Datensicherheit beachten?

Ja, die DSGVO verknüpft erstmalig Datenschutz und Datensicherheit. Die personenbezogenen Daten, die in dem Unternehmen verarbeitet werden, müssen technisch und organisatorisch geschützt werden, indem sog. **technisch-organisatorische Maßnahmen (TOMs)** getroffen werden. Wie diese ausgestaltet sind, hängt von der Schutzwürdigkeit der Daten, den Zugriffsmöglichkeiten und der Intensität der Verarbeitung ab. Aber schon aus eigenem Interesse sollte jedes Unternehmen seine Daten – ob personenbezogen oder nicht – ausreichend gegen Fremdzugriffe schützen. Das betrifft auch den Schutz vor Feuer und Wasser, so dass – verschlüsselte - Sicherungskopien an einem anderen Ort aufbewahrt werden sollten.

20. Was ist eine Datenschutz-Folgenabschätzung?

Vor Einführung eines neuen Verfahrens im Unternehmen muss eine **Risikobewertung** vorgenommen werden. Stellt sich bei der Risikobewertung heraus, dass durch die geplante Datenverarbeitung voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten** des Betroffenen bestehen, muss eine Datenschutz-Folgenabschätzung durchgeführt werden.

Ein hohes Risiko besteht insbesondere, wenn sensible Daten verarbeitet werden. Liegt ein hohes Risiko vor, muss zudem die **Aufsichtsbehörde konsultiert** werden.

Eine Liste mit Verarbeitungstätigkeiten, bei denen eine Datenschutz-Folgenabschätzung zwingend notwendig ist, finden Sie hier:

https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/Download/dsfa_muss_liste_dsk_de.pdf

Wie eine Datenschutz-Folgenabschätzung auszusehen kann, können Sie hier nachlesen:
https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/datenschutz-folgenabschaetzung/

21. Welche Rechte stehen dem Betroffenen zu?

Der Betroffene hat das Recht auf Auskunft, Berichtigung, Löschung, auf Einschränkung der Verarbeitung, ein Widerspruchsrecht gegen die Verarbeitung, das Recht auf Datenübertragbarkeit, ein Beschwerderecht sowie ein Widerrufsrecht.

➔**D05** „Informationspflichten nach der DSGVO“, Kennzahl 2356

Praxistipp: *Unternehmen müssen in der Lage sein, bei Anfragen von Betroffenen die Informationen innerhalb bestimmter Fristen zur Verfügung zu stellen. Es sollte deswegen ein Datenschutzmanagement implementiert werden, um rechtzeitig auf solche Anfragen reagieren zu können.*

22. Wer ist Aufsichtsbehörde für saarländische Unternehmen?

Aufsichtsbehörde im Saarland ist:

Unabhängiges Datenschutzzentrum Saarland
Fritz-Dobisch-Str. 12, 66111 Saarbrücken
Tel: 0681 94781-0
Fax: 0681 94781-29
E-Mail: poststelle@datenschutz.saarland.de
https://datenschutz.saarland.de/

23. Wie erfolgt eine Überprüfung durch die Datenschutzaufsicht?

Die Landesdatenschutzbeauftragten haben vielfältige Möglichkeiten, die Datenverarbeitung eines Unternehmens zu überprüfen. So kann die Aufsicht aus einem bestimmten Anlass – z. B. wegen einer Beschwerde eines Kunden, die Vorlage des Verarbeitungsverzeichnisses verlangen und dadurch die einzelnen Verfahren in dem Unternehmen überprüfen. Dazu kann die Aufsicht das Unternehmen aufsuchen oder sich die Unterlagen übersenden lassen. Sie kann auch ohne Anlass das Unternehmen aufsuchen.

Nach der Prüfung erhält das Unternehmen Gelegenheit zur Stellungnahme, wenn es Beanstandungen gibt. Die Aufsichtsbehörde prüft dann, welche Maßnahmen sie ergreift, die bis zur Verhängung von Bußgeldern oder zur Aufforderung, die Verarbeitung einzustellen, gehen können.

24. Wann liegt eine Datenpanne vor

Bei einer Datenpanne handelt es sich um eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung personenbezogener Daten führt. Datenpannen sind der Aufsichtsbehörde **unverzüglich und möglichst binnen 72 Stunden**, nachdem dem Unternehmer die Verletzung bekannt wurde, zu melden, wenn ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Die betroffene Person ist ebenfalls unverzüglich über die Verletzung zu informieren. Die Meldung kann hier erfolgen.

Praxistipp: *Unternehmen sollten ein Verfahren implementieren, um zu gewährleisten, dass Datenpannen unverzüglich gemeldet werden. Datenpannen, die voraussichtlich nicht zu einem hohen Risiko führen, sollten aus Beweisgründen ebenfalls dokumentiert werden.*

25. Mit welchen Sanktionen ist bei Verstößen zu rechnen?

Bei Verstößen gegen Datenschutzbestimmungen sieht die DSGVO empfindliche Geldstrafen vor. Die Höhe dieser Strafen kann bei besonders schlimmen Vergehen bis zu 20 Millionen Euro oder vier Prozent des letzten Jahresumsatzes betragen. Hier hat es im Vergleich zum bisherigen Recht erhebliche Verschärfungen gegeben.