DATENSCHUTZ – D09

Stand: März 2018

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

FAQ zur Datenschutzgrundverordnung

Die umfangreichen Vorschriften der Datenschutzgrundverordnung (DSGVO) stellen gerade kleinere und mittlere Unternehmen vor die Frage: Wo fange ich an? Was muss ich tun? Für den einen oder anderen Unternehmer sollte es beruhigend sein zu hören, dass sich in Deutschland nicht allzu viel durch die DSGVO ändert. Wer sich im Unternehmen schon bisher um den Datenschutz gekümmert hat, sollte auch in Zukunft trotz der höheren Sanktionen nicht viel zu befürchten haben. Trotzdem sind die bisherigen Verfahren zu prüfen und an die neuen Datenschutzregelungen bis zum 25. Mai 2018 anzupassen.

Mit Hilfe dieser FAQ wollen wir Ihnen einen Überblick über die Neuerungen geben und die Umsetzung der DSGVO erleichtern.

1. Wann tritt die Datenschutzgrundverordnung in Kraft?

Die Datenschutzgrundverordnung ist bereits nach langen Verhandlungen am 25. Mai 2016 in Kraft getreten. Sie sieht eine Übergangsfrist von zwei Jahren vor. In dieser Zeit sollen Unternehmen die Möglichkeit haben, die bisherigen Prozesse an die Neuregelungen anzupassen. Sie **gilt unmittelbar** in allen EU-Staaten **ab dem 25. Mai 2018**. Ab diesem Datum ist die Überprüfung der Einhaltung der Vorschriften durch die Aufsichtsbehörden möglich.

2. Was gilt in Deutschland?

Die Datenschutzgrundverordnung gilt direkt auch in Deutschland. Das BDSG (neu), das ebenfalls zum 25. Mai 2018 in Kraft tritt, ist immer in Verbindung mit der DSGVO zu lesen.

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

3. 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/

4. Was sind die wichtigsten Änderungen?

a) Anwendungsbereich
Der Anwendungsbereich des Datenschutzrechts wird wesentlich erweitert. Die DSGVO gilt für alle Verarbeitungen, die sich an EU-Bürger richten und personenbezogene Daten von EU-Bürgern verarbeiten.

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.*

b) Zweckänderung
Es gilt auch nach neuem Recht der Grundsatz der Zweckbindung. Die Daten dürfen nur für den Zweck genutzt werden, für den sie auch erhoben wurden. Wurde der Verwendungszweck geändert, hatte das das BDSG nicht geregelt. Das ist nun anders. Nach Art. 6 Abs. 4 DSGVO ist eine Zweckänderung nur möglich, wenn die **Weiterverarbeitung** der Daten **mit dem ursprünglichen Zweck vereinbar** ist. Die DSGVO nennt verschiedene Kriterien, nach denen die Vereinbarkeit geprüft werden kann. Ist der neue Zweck **nicht** mit dem ursprünglichen **vereinbar,** dürfen die Daten nur mit **ausdrücklicher Einwilligung** weiterverarbeitet werden.

Wird der Zweck der Verarbeitung geändert, muss der Betroffene zudem vorab darüber informiert werden, Art. 13, 14 DSGVO.

➔**D05** „Informationspflichten nach der DSGVO“, **Kennzahl 2158**

Praxistipp: *Bei der Festlegung der Zwecke sollten Sie bereits jetzt an mögliche künftige legitime Zwecke denken. Fassen Sie die Erhebungszwecke möglichst weit, um sich einen Spielraum offen zu lassen.*

c) Einwilligung
Die Anforderungen an eine wirksame Einwilligung haben sich erhöht. Die Einwilligung setzt eine **freiwillige, informierte und eindeutige Handlung** voraus. Einwilligungserklärungen sind unwirksam, wenn sie sich auf Daten erstrecken, die zur Erfüllung des Vertrages nicht erforderlich sind (sog. **Kopplungsverbot**).

Ebenfalls unwirksam sind Erklärungen, die bei einem „klaren Ungleichgewicht“ zwischen Verantwortlichen und Betroffenen getroffen werden. Dieses Kriterium ist völlig neu. Es muss abgewartet werden, wie die Rechtsprechung dieses Kriterium anwenden wird. Neu geregelt wird, dass **Minderjährige** unter 16 Jahren keine wirksamen Einwilligungserklärungen abgeben können. Es bedarf vielmehr der Einwilligung der Erziehungsberechtigten.

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 2158**

d) Informationspflichten
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 2158**

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

➔**D07** „Die Datenschutzerklärung nach der DSGVO“, **Kennzahl 2158**

e) Verzeichnis von Verarbeitungstätigkeiten
Das aus dem BDSG bekannte Verfahrensverzeichnis wird durch das Verzeichnis von Verarbeitungstätigkeiten abgelöst. In diesem Verzeichnis müssen alle Verarbeitungsprozesse personenbezogener Daten erfasst werden. Eine Pflicht zur Erstellung besteht, wenn das Unternehmen mehr als 250 Mitarbeiter beschäftigt, die Verarbeitungen ein Risiko für die Rechte und Freiheiten der Betroffenen darstellen oder - was in den allermeisten Fällen der Fall sein sollte - wenn die Verarbeitung von personenbezogenen Daten nicht nur gelegentlich erfolgt. Werden z.B. regelmäßig Kunden- oder Beschäftigtendaten verarbeitet, ist ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen.

➔**D11** „Verzeichnis von Verarbeitungstätigkeiten“, **Kennzahl 2158**

f) Dokumentationspflichten
Die DSGVO betont die Verantwortlichkeit, die Unternehmen für die Einhaltung des Datenschutzes haben. Sie müssen nachweisen können, dass ihre Datenverarbeitung datenschutzkonform ist (sog. **Rechenschaftspflicht**, Art. 5 Abs. 2 DSGVO). Dies gelingt nur über eine umfassende Dokumentation.

➔**D04** „Dokumentationspflichten nach der DSGVO“, **Kennzahl 2158**

g) Auftragsverarbeitung (ADV)
Nicht nur der Begriff der Auftragsdatenverarbeitung hat sich geändert. Daneben wird auch der Auftragsverarbeiter stärker in die Pflicht genommen. Er hat eigene Dokumentationspflichten (insbesondere das Bereithalten von Verfahrensverzeichnissen) und haftet gegebenenfalls selbst gegenüber dem Betroffenen.

Praxistipp: *Die Anforderungen an ADV-Verträge sind in Art. 28 DSGVO festgehalten. Altverträge sind zu überprüfen und an die DSGVO anzupassen.*

➔**D12** „Auftragsverarbeitung nach der DSGVO“, **Kennzahl 2158**

h) Recht auf Datenübertragung
Der Betroffene hat nach Art. 20 DSGVO das Recht, die von ihm bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Auf Wunsch können diese Daten auch an einen Dritten übermittelt werden. Neben dem Recht auf Datenübertragung existieren auch weitere Betroffenenrechte, auf die der Verantwortliche entsprechend reagieren muss.

➔**D05** „Informationspflichten nach der DSGVO“, **Kennzahl 2158**

Praxistipp: *Unternehmen müssen ab dem 25. Mai 2018 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.*

i) Datenschutz-Folgenabschätzung
Vor Einführung eines neuen Verfahrens im Unternehmen muss eine **Risikobewertung** vorgenommen werden. Stellt sich bei der Risikobewertung heraus, dass durch die geplante Datenverarbeitungen ein **hohes Risiko für die Rechte und Freiheiten** des Betroffenen bestehen, muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Die Datenschutz-Folgenabschätzung löst die bisherige Vorabkontrolle nach § 4d Abs. 5 BDSG ab.

Ein hohes Risiko besteht insbesondere, wenn sensible Daten verarbeitet werden. Liegt ein hohes Risiko vor, muss zudem die **Aufsichtsbehörde konsultiert** werden. Die Aufsichtsbehörden in Deutschland haben angekündigt, dass sie eine Liste mit Verarbeitungstätigkeiten veröffentlichen werden, die eine Datenschutz-Folgenabschätzung zwingend benötigen.

j) Meldepflichten
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.

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.*

k) Geldbußen
Die Geldbußen für Verstöße wurden drastisch erhöht. Die Höchstgrenze von bisher 300.000 € wurde auf bis zu 20 Mio. € und auf bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs pro Verstoß erhöht.

5. Was ist weitestgehend gleich geblieben?

Die Grundsätze des Datenschutzrechtes haben sich kaum geändert. Die Verarbeitung von Daten ist weiterhin verboten, solange sie nicht durch einen Erlaubnistatbestand gerechtfertigt ist oder eine Einwilligung vorliegt. (**Verbot mit Erlaubnisvorbehalt**). Art. 6 Abs. 1 DSGVO zählt die verschiedenen Erlaubnistatbestände auf. Die Datenverarbeitung ist insbesondere zulässig, wenn sie zur Erfüllung eines Vertrags, oder zur Durchführung vorvertraglicher Maßnahmen oder zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist.

Weitere Prinzipien der DSGVO sind:

- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Datenverarbeitung
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Die Verarbeitung sensibler Daten ist, wie bisher auch, nur mit ausdrücklicher Einwilligung möglich, Art. 9 DSGVO.

➔**D02** „Einwilligung nach der DSGVO“, **Kennzahl 2158**

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

➔ **D06** „Betrieblicher Datenschutzbeauftragter nach der DSGVO und dem BDSG (neu)“, **Kennzahl 2158**

6. Welche Dokumente und Prozesse muss ich in meinem Unternehmen überprüfen/anpassen/implementieren?

- Datenschutzerklärungen müssen überarbeitet bzw. die Informationspflichten erfüllt werden;
- Einwilligungen müssen gegebenenfalls überarbeitet oder neu eingeholt werden. Bereits rechtskonforme eingeholte Einwilligungen bleiben weiterhin wirksam;
- Verfahrensverzeichnisse sind zu erstellen;
- Risikobewertungen und gegebenenfalls eine Datenschutz-Folgenabschätzung müssen vornegenommen werden;
- ADV-Verträge sind abzuschließen oder gegebenenfalls anzupassen;
- Betriebsvereinbarungen müssen überarbeitet werden;
- Verfahren zur Erfassung und Bearbeitung von Betroffenenanfragen wie z.B. Löschungs- oder Auskunftsanfragen sind zu implementieren;
- Verfahren bei Datenpannen muss geregelt werden;
- Schulung der Mitarbeiter;
- technisch-organisatorische Maßnahmen sind festzulegen;
- die Prozesse müssen evaluiert werden.

Beachte: Diese Liste ist nicht abschließend. Unternehmen müssen prüfen, welche Prozesse im eigenen Betrieb angepasst und umgesetzt werden müssen.

7. Welche Abteilungen sollten über die Änderungen informiert werden?

Folgende Stellen innerhalb des Unternehmens sollten informiert und sensibilisiert werden:

- der Datenschutzbeauftragte;
- die Geschäftsleitung;
- die Rechtsabteilung zwecks Anpassung der Rechtstexte;
- die EDV-Abteilung, insbesondere zur Festlegung der technisch-organisatorischen Maßnahmen im Unternehmen;
- die Qualitätsmanagement-Abteilung;
- die Finanzabteilung;
- die Personalabteilung und der Betriebsrat und
- ggf. Projektabteilung/Produktentwicklungsabteilung.