DATENSCHUTZ – D04

Stand: Januar 2018

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

Dokumentationspflichten nach der DSGVO

Die Datenschutz-Grundverordnung (DSGVO) betont die Verantwortlichkeit, die Unternehmen (auch „verantwortliche Stellen“ oder „Verantwortliche“ genannt) für die Einhaltung des Datenschutzes haben. Sie müssen **nachweisen** können, dass ihre Datenverarbeitung datenschutzkonform ist. Das gilt unabhängig von der Unternehmensgröße oder Branche. Dies gelingt nur über eine umfassende Dokumentation.

Die DSGVO zählt an verschiedenen Stellen Dokumentationspflichten auf, die wir nachfolgend darstellen:

1. Rechenschaftspflicht, Art. 5 Abs. 2, 24 Abs. 1 DSGVO

Wer personenbezogene Daten verarbeitet, ist verantwortlich für die **Einhaltung** der Grundsätze des DSGVO und muss deren Einhaltung nachweisen können („Rechenschaftspflicht“). Die **Datenschutzgrundsätze** sind:

- die Rechtmäßigkeit der Verarbeitung,
- die Verarbeitung nach Treu und Glauben,
- Transparenz,
- Zweckmäßigkeit,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und Vertraulichkeit.

Jedes Unternehmen hat geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen und den Nachweis erbringen zu können, dass es bei seiner Datenverarbeitung vollumfänglich die Regelungen der DSGVO beachten. Die ergriffenen Maßnahmen sind regelmäßig zu überprüfen und zu aktualisieren.

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

Wichtig: *Diese Vorgabe kann das Unternehmen nur erfüllen, wenn es ein Datenschutz-Management-System aufbaut. Das ist von allen Mitarbeitern umzusetzen. So kann im Rahmen eines Vertragsmanagements etwa eine Liste erstellt werden, in die alle Verträge eingetragen werden, nach Prüfung der erhobenen personenbezogenen Daten, ist zu überprüfen, ob eine Auftragsdatenverarbeitung vorliegt usw. Die entsprechenden Dokumentationen sind aufzustellen und permanent zu pflegen. Ist ein betrieblicher Datenschutzbeauftragter bestellt, sollte eine solche Dokumentation über die datenschutzrechtlich relevanten Sachverhalte mit ihm abgesprochen werden.*

Wichtig: *Datenschutz ist und bleibt Chefsache, der Unternehmer muss das Datenschutzmanagementsystem aufbauen und überwachen.*

2. Dokumentation von erteilten Einwilligungen, Art. 6 Abs. 1 lit. a, Art. 7 ff. DSGVO

Wird eine Datenverarbeitung auf eine Einwilligung gestützt, so muss das Unternehmen nachweisen können, dass diese wirksam erteilt und rechtmäßig gestaltet wurde. Bisher rechtmäßig (!) eingeholte Einwilligungen sind weiterhin wirksam. Liegen keine Einwilligungen vor oder sind diese nicht rechtswirksam eingeholt worden, sollten Unternehmen dies nachholen. Das verantwortliche Unternehmen muss die Einholung nachweisen können. Dies gelingt nur über eine **schriftliche** oder **elektronische** Einwilligung.

Der Betroffene hat das Recht, die Einwilligung **jederzeit** für **die Zukunft zu widerrufen**. Der Betroffene ist bei der Erhebung der Einwilligung über sein Widerrufsrecht zu informieren. Auch dies ist zu dokumentieren.

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

3. Dokumentation bei Datenerhebung zur Wahrung der berechtigten Interessen, Art. 6 Abs. 1 lit. f, Abs. 4 DSGVO

Wer eine Datenverarbeitung auf die Rechtsgrundlage „**Wahrung der berechtigten Interessen des Verantwortlichen oder Dritten**“ stützt, muss den hiervon betroffenen Personen die Gründe mitteilen, die er oder ein Dritter in Abwägung zu den Interessen der Betroffenen als überwiegend ansieht. Die **Gründe** sind zu **dokumentieren**.

Ausdrücklich als eine dem berechtigten Interesse dienende Verarbeitung ist die Verarbeitung personenbezogener Daten zum Zwecke der **Direktwerbung**. Bei der Abwägung sind die „vernünftigen Erwartungen“ der betroffenen Person zu berücksichtigen und zu dokumentieren. Ein anderer Fall ist das **Kontaktformular in Onlineshops**, über das der potenzielle Kunde Produktinformationen erfragen kann.

Ferner hat das Unternehmen den Betroffenen vorab umfassend über sein **Widerrufsrecht** und eine Zweckänderung zu **informieren**.

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

4. Dokumentation der Einhaltung der Informationspflichten bei Datenerhebungen nach Art. 13, 14 DSGVO

Jedes Unternehmen muss nachweisen, dass es die erweiterten Informationspflichten nach der DSGVO erfüllt. Den Informationspflichten kann am besten durch eine Datenschutzerklärung nachgekommen werden. Es empfiehlt sich auch alte Datenschutzerklärungen aufzubewahren sowie den Zeitpunkt der Übermittlung zu dokumentieren.

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

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

5. Dokumentation der Information über die Betroffenenrechte, Art. 15 ff. DSGVO

Dem Betroffenen stehen verschiedene Rechte gegen die verantwortliche Stelle zu, über die der Betroffene informiert werden muss (z.B. das Auskunfts- oder Berichtigungsrecht).

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

Der Umgang mit den Betroffenenrechten sollte dokumentiert werden (z.B. in einen Datenschutz-Management-System). Prüft die Aufsichtsbehörde den Vorgang, dient die Dokumentation als **Nachweis**, dass den datenschutzrechtlichen Bestimmungen nachgekommen wurde.

Wurde z.B. ein Widerspruch gegen die Datenverarbeitung abgelehnt, müssen die Gründe festgehalten werden, warum der Antrag abgelehnt wurde, Art. 21 DSGVO.

6. Dokumentation der technisch-organisatorischen Maßnahmen, Art. 24, 32 DSGVO

Der Verantwortliche ist verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten einzusetzen, um sicherzustellen und nachweisen zu können, dass sie die Vorgaben der DSGVO einhalten und ein **angemessenes technisches Schutzniveau** für personenbezogene Daten gewährleisten. Der Nachweis erfolgt über eine entsprechende Beschreibung dieser Maßnahmen (z.B. in einem Auftragsdatenverarbeitungsvertrag und/oder im sog. **Verzeichnis für Verarbeitungstätigkeiten**). Beim Nachweis kann auch auf genehmigte Verhaltensregeln oder auf genehmigte Zertifizierungen zurückgreifen werden.

Zu den technisch-organisatorischen Maßnahmen gehören bspw. die Pseudonymisierung und Verschlüsselung personenbezogener Daten oder Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Backup).

Bei der Festlegung der technisch-organisatorischen Maßnahmen sollte der Stand der Technik, Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für von der Datenverarbeitung Betroffene berücksichtigt und dokumentiert werden.

7. Auftragsverarbeitung-Vertrag (ADV), Art. 28 DSGVO

Wird ein Dienstleister beauftragt, personenbezogene Daten nach Weisung und nur zum Zwecke der Vertragserfüllung zu verarbeiten, muss ein **schriftlicher Auftragsdatenvertrag** abgeschlossen werden. Art. 28 DSGVO schreibt vor, welche Anforderungen an einem solchen Vertag bestehen.

Alte Verträge sollten überprüft werden und ggf. entsprechend angepasst werden. Auch dies ist zu dokumentieren

8. Verpflichtung zur Vertraulichkeit

Die DSGVO regelt, dass Beschäftigte personenbezogene Daten nur auf Anweisung des Verantwortlichen verarbeiten dürfen. Diese sind verpflichtet, ihre Mitarbeiter entsprechend anzuhalten und zu schulen. Insoweit sollten Verantwortliche notwendige **interne Datenschutzregelungen** (Betriebsvereinbarungen, Dienstanweisungen) erstellen und die Mitarbeiter in diesen Fragen entsprechend **informieren und schulen**. Interne Datenschutzregelungen sowie sonstige Anweisungen zum Datenschutz sollten dokumentiert und regelmäßig auf Änderungsbedarf geprüft werden.

Daneben sollten die Mitarbeiter auf das Datengeheimnis und zur Vertraulichkeit **schriftlich verpflichtet** werden. Diese Verpflichtung sollte Eingang in die Personalakte finden.

9. Meldung von Datenpannen, Art. 33 DSGVO

Der Verantwortliche hat jede Datenverletzung **binnen 72 Stunden** der zuständigen Datenschutzaufsichtsbehörde zu melden. Für saarländische Unternehmen ist dies:

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/

Eine Meldepflicht **entfällt**, **wenn die Datenverletzung voraussichtlich nicht zu einem Risiko für Betroffene führt** (z.B. weil die Daten auf dem als verloren gemeldeten iPad nach dem Stand der Technik sicher verschlüsselt sind).

Die DSGVO verpflichtet Verantwortliche, **jede Datenverletzung zu dokumentieren** und hierbei alle Fakten, Auswirkungen und ergriffene Abhilfemaßnahmen festzuhalten. Dies dient auch als Nachweis gegenüber der Aufsichtsbehörde.

Falls die Datenpanne ein hohes Risiko für den Betroffenen zur Folge hätte, treffen den Verantwortlichen zudem Mitteilungspflichten.

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

10. Datenschutz-Folgenabschätzung, Art. 35 DSGVO

Für jede Verarbeitung personenbezogener Daten ist zu ermitteln, welches Risiko für die Rechte Betroffener damit verbunden ist (**Risikobewertung**). Das Ergebnis der Bewertung ist zu dokumentieren. Stellt ein Verantwortlicher fest, dass die beabsichtigte Datenverarbeitung ein **hohes Risiko** für die betroffenen Personen zur Folge hätte und kann dieses hohe Risiko nicht minimiert werden, so hat ein Verantwortlicher eine sog. **„Datenschutz-Folgenabschätzung“** durchzuführen. Kann das als Ergebnis festgestellte hohe Risiko nicht durch technische und/oder organisatorische Maßnahmen zum Schutz der Daten minimiert werden, ist dies zu dokumentieren und die Aufsichtsbehörde vorab, d. h. vor einem Einsatz, zu konsultieren. Dies hat ferner zu erfolgen bei all den Verarbeitungen, die Datenschutzaufsichtsbehörden als hoch risikoreich einstufen und deshalb in einer sog. „Blacklist“ veröffentlichen, die die Datenschutzaufsichtsbehörden demnächst veröffentlichen werden.

11. Benennung eines betrieblichen Datenschutzbeauftragten, Art. 37

Sowohl im Falle einer Bestellpflicht als auch bei einer freiwilligen Bestellung eines Datenschutzbeauftragten sollte die Bestellung **schriftlich** erfolgen. In der Bestellurkunde sollte festgehalten werden, welche Aufgaben auf den Datenschutzbeauftragten übertragen werden (wie z.B. die Führung eines Verzeichnisses für Verarbeitungstätigkeiten). Ein Muster für die Bestellung eines betrieblichen Datenschutzbeauftragten finden Sie in unserem Infoblatt ➔**D06** „Betrieblicher Datenschutzbeauftragter“, **Kennzahl 2158.**