Überblick zur EU-Datenschutz-Grundverordnung

Autoren: Arbeitskreis Datenschutz
Stand: März 2022

1. Hintergrund zur DSGVO

- Die DSGVO ist am 25. Mai 2016 in Kraft getreten und gilt seit dem **25. Mai 2018 verbindlich** in allen EU-Mitgliedstaaten. Zu beachten ist, dass die DSGVO sog. **Öffnungsklauseln** enthält. Diese bieten dem nationalen Gesetzgeber einen Umsetzungsspielraum in bestimmten Bereichen. In Deutschland ist insoweit insbesondere das BDSG zu berücksichtigen.
- Unternehmen drohen bereits für das Nichtvorhalten datenschutzkonformer Prozesse Bußgelder von bis zu vier Prozent des weltweit erzielten Vorjahresumsatzes.
- Bei der Verarbeitung von personenbezogenen Daten sind die Datenschutzgrundsätze Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit nachweisbar einzuhalten.
- Als Ausdruck der Compliance-Verantwortlichkeit des Datenverarbeiters sieht die DSGVO eine Rechenschaftspflicht (Accountability) vor. Daraus folgt eine deutliche Ausweitung der Dokumentationspflichten.
- Die DSGVO legt einen starken **Fokus auf Formalisierung, Dokumentation, Risikoanalyse und Transparenz** und zielt im Ergebnis auf die Einrichtung eines stark formalisierten **Datenschutz- Management-Systems** ab.

DICO
Deutsches Institut für Compliance

2. Die DSGVO im Überblick

1	**Territorialer Anwendungsbereich**	• Neben Datenverarbeitern in der EU können auch Datenverarbeiter außerhalb der EU in bestimmten Fällen in den Anwendungsbereich der DSGVO fallen, z. B. bei dem Angebot von Waren oder Dienstleistungen für den europäischen Markt.
2	**Sanktionsmöglichkeiten**	• Bereits für das Nichtvorhalten datenschutzkonformer Prozesse drohen Bußgelder von bis zu vier Prozent des weltweit erzielten Vorjahresumsatzes.
3	**Compliance-Verantwortlichkeit und Haftung**	• Der Verantwortliche muss die Einhaltung der Grundsätze für die Verarbeitung durch entsprechende Dokumentation nachweisen („Rechenschaftspflicht"). Dies führt faktisch zu einer Beweislastumkehr
4	**Anforderungen an das Verarbeitungsverzeichnis**	• Das Nichtvorhalten des Verarbeitungsverzeichnisses ist bußgeldbewehrt. • Auch Auftragsverarbeiter müssen ein Verarbeitungsverzeichnis führen.
5	**Datenschutz-Folgenabschätzung**	• Die Datenschutz-Folgenabschätzung stellt eine besondere Form der Risikoanalyse für Hochrisikoverarbeitungen dar und kann dazu führen, die Aufsicht zu konsultieren.
6	**Gemeinsam für die Verarbeitung Verantwortliche („Joint Controllership")**	• Konstrukt der Zusammenarbeit mit der Anforderung, die Rechte und Pflichten der verschiedenen verantwortlichen Stellen vertraglich in transparenter Form niederzulegen.
7	**Anforderungen an die Auftragsverarbeitung**	• Unterstützungspflicht des Auftragnehmers zugunsten des Auftraggebers bei Erfüllung seiner Pflichten bspw. zur Datensicherheit, der Meldepflicht bei Datenschutzverletzungen sowie der Datenschutz-Folgenabschätzung.
8	**Privacy by Design/ Privacy by Default**	• Die DSGVO erfordert die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Die Umsetzung angemessener technischer und organisatorischer Maßnahmen ist erforderlich.
9	**Löschen von Daten und das Recht auf Vergessenwerden**	• Die betroffene Person kann u. U. die Löschung ihrer Daten vom Verantwortlichen verlangen. Dies umfasst auch die Sicherstellung der Löschung der Daten bei Dritten. Beachte ergänzend § 35 BDSG: Einschränkung der Verarbeitung statt Löschung.
10	**Informationspflichten und Betroffenenrechte**	• Die betroffene Person ist hinsichtlich der Verarbeitung ihrer personenbezogenen Daten zu informieren. Darüber hinaus stehen der betroffenen Person weitrechende Betroffenenrechte zu (z. B. Recht auf Auskunft).
11	**Aufgabenbereich des Datenschutzbeauftragten**	• Unterrichtung und Beratung des Verantwortlichen und Auftragsverarbeiters, Überwachung der Einhaltung der Datenschutzvorschriften, Beratung des Verantwortlichen bei Datenschutz-Folgenabschätzung, Zusammenarbeit mit Datenschutzaufsichtsbehörde.
12	**Verarbeitung von Beschäftigtendaten**	• Die Verarbeitung von Beschäftigtendaten richtet sich nach § 26 BDSG. • Geregelt sind u. a. Anforderungen an die Einwilligung des Beschäftigten in die Datenverarbeitung.
13	**Fristgebundene Notifikationspflichten bei Datenschutzverstößen**	• Grdsl.: 72-Stunden-Frist zur Meldung an die Aufsichtsbehörde. • Die Meldepflicht ist nicht an bestimmte Datenkategorien oder Arten von Verstößen geknüpft – jeder Datenschutzverstoß kann potenziell relevant sein. • Benachrichtigung der Betroffenen bei voraussichtlich hohem Risiko.