Überblick zur EU-Datenschutz-Grundverordnung

Autoren: Arbeitskreis Datenschutz
Stand: Mai 2018

1. Hintergrund zur DSGVO

- Die DSGVO ist am 25. Mai 2016 in Kraft getreten und gilt ab dem **25. Mai 2018 verbindlich** in allen EU Mitgliedstaaten. Am gleichen Tag tritt das neue BDSG in Kraft.
- Die DSGVO löst in Deutschland vor allem das alte BDSG ab und ersetzt die EU-Datenschutzrichtlinie 95/46/EG.
- Viele Anforderungen der DSGVO klingen zwar ähnlich denen des BDSG; im Detail unterscheiden sie sich jedoch bisweilen deutlich. Faktisch bleibt **kaum ein Regelungsbereich unverändert**.
- Die Grundsätze des Verbots mit Erlaubnisvorbehalt, der Datenvermeidung und Datensparsamkeit, der Zweckbindung wie auch verschiedene Anforderungen an technische Sicherheit einerseits und Information der Betroffenen andererseits sind auch heute schon im BDSG angelegt.
- Die DSGVO legt aber einen sehr viel stärkeren **Fokus auf Formalisierung, Dokumentation, Risikoanalyse und Transparenz**.
- Im Ergebnis zielt die DSGVO auf die Einrichtung eines stark formalisierten **Datenschutzmanagementsystems** ab, das umfangreiche Neuerungen und Adjustierungen von Organisation, Prozessen und Maßnahmen mit sich bringt.
- Zu beachten ist, dass die DSGVO sog. **Öffnungsklauseln** enthält. Diese bieten dem nationalen Gesetzgeber einen Umsetzungsspielraum in bestimmten Bereichen. In Deutschland ist insoweit z. B. das neue BDSG zu beachten.

DICO
Deutsches Institut für Compliance

2. Wesentliche Änderungen durch die DSGVO

1	Ausweitung des territorialen Anwendungsbereichs	• Auch Datenverarbeiter außerhalb der EU sind in bestimmten Fällen vom Anwendungsbereich der DSGVO erfasst, z. B. bei dem Angebot von Waren oder Dienstleistungen für den europäischen Markt, sog. „Marktortprinzip“.
2	Neue, massiv erweiterte Sanktionsmöglichkeiten	• Der Bußgeldrahmen wird auf bis zu EUR 20 Mio. oder 4 % des weltweiten Vorjahresumsatzes erhöht.
3	Verschärfung der Compliance-Verantwortlichkeit und Haftung	• Verantwortlichkeit des Datenverarbeiters im Fokus. Er muss die Einhaltung der Grundsätze für die Verarbeitung durch entsprechende Dokumentation nachweisen („Rechenschaftspflicht“). Dies führt zu einer Beweislastumkehr und vermehrten Haftungsrisiken.
4	Neue Anforderungen an das Verarbeitungsverzeichnis	• Wird zum Basis-Dokumentationstool. • Nichtvorhalten ist bußgeldbewehrt. • Auch Auftragsverarbeiter müssen ein Verarbeitungsverzeichnis führen.
5	Datenschutz-Folgenabschätzung	• Besondere Form der Risikoanalyse für Hochrisikoverarbeitungen. • Kann zu Konsultation der Aufsichtsbehörde führen.
6	Gemeinsam für die Verarbeitung Verantwortliche („Joint Controllership“)	• Neues Konstrukt der Zusammenarbeit mit der Anforderung, die Rechte und Pflichten der verschiedenen verantwortlichen Stellen vertraglich in transparenter Form niederzulegen.
7	Neue Anforderungen an die Auftragsverarbeitung	• Unterstützungspflicht des Auftragnehmers zugunsten des Auftraggebers bei Erfüllung seiner Pflichten zur Datensicherheit, der Meldepflicht bei Datenschutzverstößen sowie der Datenschutz-Folgenabschätzung.
8	Privacy by Design/ Privacy by Default	• Erfordert ein Assessment der bisher implementierten Maßnahmen und technischen Voreinstellungen sowie ggf. Neuausrichtung von Prozessen, Maßnahmen und IT, z. B. Berechtigungskonzepte, Pseudonymisierung, Speicherfristen, Lösch- und Sperrkonzepte usw..
9	Löschen von Daten und das Recht auf Vergessenwerden	• Der Betroffene kann u. U. die Löschung seiner Daten vom Verantwortlichen verlangen. Das Recht auf Vergessenwerden adressiert auch die Frage der Sicherstellung der Löschung der Daten bei Dritten. • Beachte ergänzend § 35 BDSG-neu: Einschränkung der Verarbeitung statt Löschung.
10	Neue fristgebundene Informations- und Transparenzpflichten	• Betroffenenrechte wurden erweitert. • Erfordern neue Prozesse und Musterformulare. • Nichteinhaltung bußgeldbewehrt.
11	Erweiterter Aufgabenbereich des Datenschutzbeauftragten	• Unterrichtung und Beratung des Verantwortlichen und Auftragsverarbeiters, Überwachung der Einhaltung der Datenschutzvorschriften, Beratung des Verantwortlichen bei Datenschutz-Folgenabschätzung, Zusammenarbeit mit Aufsichtsbehörde.
12	Neue Regelungen zur Verarbeitung von Beschäftigtendaten	• § 26 BDSG-neu greift wesentliche Regelungen des bisherigen § 32 BDSG auf und ergänzt ihn u. a. um Ausführungen zur Einwilligung des Beschäftigten in die Datenverarbeitung.
13	Verschärfte, fristgebundene Notifikationspflichten bei Datenschutzverstößen	• Grdsl.: 72-Stunden-Frist zur Meldung an die Aufsichtsbehörde. • Die Meldepflicht ist nicht mehr an bestimmte Datenkategorien oder Arten von Verstößen geknüpft – jeder Datenschutzverstoß kann potentiell relevant sein. • Benachrichtigung der Betroffenen bei voraussichtlich hohem Risiko.