Europäische Grundverordnung zum Datenschutz (DSGVO)

Akteure

Europäische Kommission
EU – Datenschutzreform
Überwachung der Umsetzung der DSGVO

Europäisches Parlament und Europarat
Verhandlung und Beschluss der DSGVO

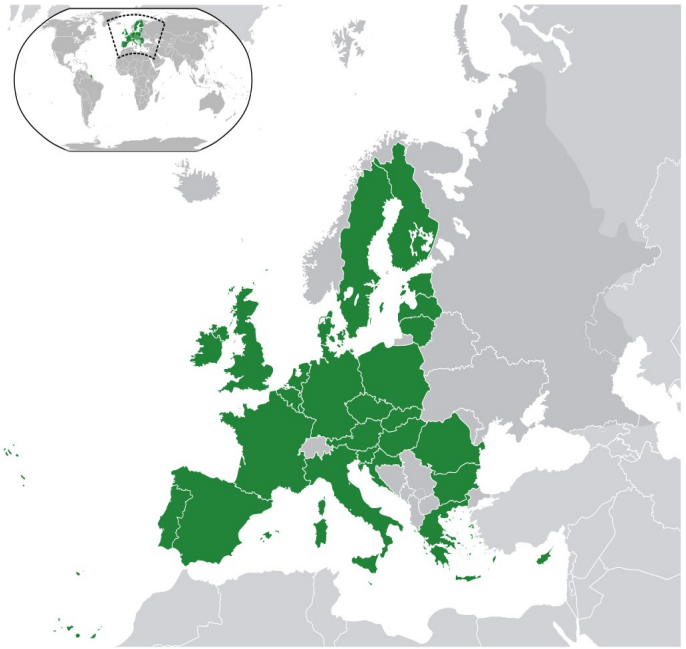
EuGH
Auslegung der DSGVO
Kontrolle der Kommissionsentscheidungen

Datenschutzausschuss
Sicherstellung der einheitlichen Anwendung der DSGVO
Koordination der Zusammenarbeit der Aufsichtsbehörden

Akteure

Mitgliedsstaaten
Ergänzung des Rechtsrahmens
Aufsichtsbehörde
ggf. Benennung der Vertretung im Datenschutzausschuss

Aufsichtsbehörden
Federführende Behörde ist alleiniger Ansprechpartner des Verarbeiters (Hauptniederlassung bzw. Hauptverarbeitung)
Entsenden der Mitglieder des Datenschutzausschuss



Gültigkeit

Regelung mit unmittelbarer innerstaatlicher Geltung

Löst die EU Datenschutzrichtlinie 95/46/EG ab

Ersetzt nationales Datenschutzrecht (BDSG, LDSG's)

Übergangsfrist endet am 25.05.2018

Ziele

EU weite Harmonisierung des Datenschutzes

Modernisierung des Datenschutzrechts
- Zunehmende Digitalisierung
- Globalisierung (Wettbewerb)
- Internet

Sicherung der Betroffenenrechte

Art. 1 DSGVO Gegenstand und Ziele

Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

Art. 4 Begriffsbestimmungen

„**personenbezogene Daten**“

Alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** … beziehen;

Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer … Kennnummer, zu Standortdaten, zu einer Online-Kennung … identifiziert werden kann;

Art. 4 Begriffsbestimmungen

Beispiele für personenbezogene Daten

Name, Anschrift, Titel, Beruf, Familienstand, Religions-, Partei-, Vereinszugehörigkeit, Zahlungsverhalten, Krankheiten, Vorstrafen, Daten des Lebenslaufes, Beurteilungen, ...
Angaben zu Einkommen, Steuern, Vertragskonditionen, Besitzverhältnissen, ...

Beispiele für personenbeziehbare Daten

Pseudonym, Pers.-Nr., FIN, IP-Adresse, Kundennummer, Sozialvers.-Nr., Konto-Nr., Zähler-Nr., Versicherungs-Nr., ...

Art. 4 Begriffsbestimmungen

„**Verarbeitung**“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang ... im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Die wesentlichen Inhalte im Überblick

Verbot mit Erlaubnisvorbehalt
Dieser Kern des Datenschutzrechtes bleibt erhalten. In Artikel 6 DSGVO wird abschließend aufgezählt, unter welchen Bedingungen eine Datenverarbeitung rechtmäßig ist.

Datensicherheit
Die Gewährleistung von Datensicherheit wird als zentrales Prinzip des Datenschutzes verankert.

Zweckbindung
Der Zweckbindungsgrundsatz bleibt mit Einschränkungen. Personenbezogene Daten dürfen stets nur zu einem genau definiertem Zweck verarbeitet werden.

Datensparsamkeit
Das Prinzip der Datensparsamkeit bleibt ebenfalls erhalten. Es dürfen nur die Daten verarbeitet werden, die für den jeweiligen Zweck notwendig sind.

Die wesentlichen Inhalte im Überblick

Erweiterung des territorialen Anwendungsbereiches (Marktortprinzip)
Gilt auch für Unternehmen mit Sitz außerhalb der EU, sofern personenbezogene Daten von Betroffenen aus der EU verarbeitet werden.

Rechenschaftspflicht des Datenverarbeiters
Der Datenverarbeiter ist verantwortlich für die Einhaltung der DSGVO Grundsätze und muss das durch entsprechende **Dokumentation** nachweisen können.

Technische und organisatorische Maßnahmen
Die DSGVO fordert die Einführung von technisch-organisatorischen Maßnahmen (TOMs), die sich nach dem Zweck der Verarbeitung sowie dem Stand der Technik richten. Dabei muss das von den Verfahren ausgehende Risiko zur Beeinträchtigung von Persönlichkeitsrechten berücksichtigt werden.

Die wesentlichen Inhalte im Überblick

Datenschutz Folgeabschätzung
Wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte von Betroffenen birgt, ist vorab eine Risikoabschätzung vorzunehmen und zu dokumentieren.

Das Recht auf Löschung / Vergessen werden
Betroffene können unter Umständen die unverzügliche Löschung ihrer Daten verlangen. Dabei ist auch sicherzustellen, dass bei Dritten gespeicherte Daten gelöscht werden.

Auftragsverarbeitung
Auftragnehmer müssen sicherstellen, dass die Verarbeitung im Einklang mit der DSGVO erfolgt. Sie sind verpflichtet, den Auftraggeber zu unterstützen, haben eine Meldepflicht bei Datenschutzverstößen und können zu Schadensersatz herangezogen werden.

Die wesentlichen Inhalte im Überblick

Einwilligung
Die Rechtslage zur „Einwilligung" bleibt im Großen und Ganzen erhalten. Die Rahmenbedingungen werden aber verschärft. Die Einwilligung muss freiwillig, unmissverständlich, informiert und widerrufbar sein.
Das Vorliegen der Voraussetzungen ist zu dokumentieren.

Transparenz/ Treu und Glauben
Personenbezogene Daten müssen transparent und nach Treu und Glauben verarbeitet werden. Neu ist die Aufnahme des Auffangtatbestandes von **Treu und Glauben** (vgl. § 242 BGB).

Bußgeldvorschriften
- Verstöße gegen die DSGVO können Schadensersatzansprüche von Betroffenen oder Verbänden zur Folge haben (Klagerecht)
- Die Aufsichtsbehörden müssen bei Verstößen Geldbußen verhängen
- Maximal drohen bis 4% des Jahresumsatzes oder bis zu 20 Mio. Euro (der höhere Wert gilt).
- In jedem Fall wirksam, verhältnismäßig und abschreckend
- Berücksichtigung erschwerender oder erleichternder Tatsachen

Die wesentlichen Inhalte im Überblick

Recht auf Datenportabilität
Betroffene haben das Recht, Daten, die sie zur Verarbeitung bereitgestellt haben, in strukturierter, maschinenlesbarer Form, zu erhalten.

Recht auf Auskunft
Die Auskunftsrechte für Betroffene werden erweitert. Auskunft grundsätzlich innerhalb eines Monates (3 Monate mit Begründung). Kopie der verarbeiteten Daten muss zur Verfügung gestellt werden.

Meldung von Datenschutzverstößen
Datenschutzverstöße müssen unverzüglich (72 Stunden nach Bekanntwerden) an die Aufsichtsbehörde und ggf. den Betroffenen gemeldet werden. Ausnahmen wenn kein Risiko für die Betroffenen besteht.

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

- Rechtmäßig und nach Treu und Glauben für den Betroffenen nachvollziehbar (Transparenz)
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherung nur solange es der Zweck erfordert (Speicherbegrenzung)
- Vertraulich und integer (TOMs)

- **!! Rechenschaftspflicht**

Art. 6 Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur verarbeitet werden wenn eine der folgenden Bedingungen vorliegt:

- Einwilligung
- Vertrag oder vorvertragliche Maßnahmen
- Gesetzliche Verpflichtung
- Interessenabwägung

...

Art. 7, Art. 8 Einwilligung / Einwilligung eines Kindes

- Freiwillig, informiert (...so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen...)
- Nachweispflicht
- Bestehende Einwilligungen müssen Anforderungen der DSGVO erfüllen
- Einwilligung eines Kindes (16 Jahre), sonst Zustimmung der Eltern
- Angemessene Maßnahmen um sich von der Zustimmung der Eltern zu vergewissern

Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten

- Rasse / Ethnie
- Politische Meinung
- Religion / Weltanschauung
- Gewerkschaftszugehörigkeit
- Genetische / biometrische Daten
- Gesundheitsdaten
- Sexualleben / sexuelle Orientierung

Art. 15 – Art. 22 Rechte des Betroffenen

- Auskunft (Art. 15)
- Berichtigung (Art. 16)
- Löschung (Art. 17)
- Einschränkung der Verarbeitung (Art. 18)
- Mitteilung über Berichtigung, Löschung, ... an Empfänger (Art. 19)
- Widerspruchsrecht (Art. 21)

Art. 15 – Art. 22 Rechte des Betroffenen

Art. 17 (Abs. 2) Recht auf Löschung ("Recht auf Vergessenwerden")

- Betroffene können Löschung der gespeicherten Daten verlangen
- Bei Veröffentlichung von Daten müssen angemessene, auch technische Maßnahmen ergriffen werden, um Dritte über Löschungswunsch zu informieren.

Art. 20 Recht auf Datenübertragbarkeit (Datenportabilität)

- Betroffener hat Anspruch auf Kopie der verarbeiteten Daten
- Übergabe in gängigem strukturierten Format
- Gilt nur, wenn die Verarbeitung auf Basis einer Einwilligung oder eines Vertrages erfolgt

Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen

Der Verantwortliche muss **geeignete technische und organisatorische Maßnahmen** umsetzen, um sicherzustellen und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Berücksichtigung von Art, Umfangs, Umstände und der Zwecke der Verarbeitung sowie der **Eintrittswahrscheinlichkeit** und **Schwere der Risiken** für die Rechte und Freiheiten natürlicher Personen.

Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfr. Voreinstellungen

Privacy by Design

Unter Berücksichtigung des Stands der Technik …trifft der Verantwortliche... angemessene technische und organisatorische Maßnahmen …, mit denen die wirksame Umsetzung der **Datenschutzgrundsätze** wie etwa Datenminimierung und die Aufnahme der notwendigen Garantien in die Verarbeitung **erreicht werden** sollen, ...

Privacy by Default

Der für die Verarbeitung Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch **Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden; …

Art. 30 Verzeichnis von Verarbeitungstätigkeiten

Jeder Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen.

Jeder Auftragsverarbeiter führt ein Verzeichnis zu allen von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten

Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

Art. 32 Sicherheit der Verarbeitung

Technische Aspekte der Datenverarbeitung bekommen eine höhere Bedeutung.

Technische und organisatorische Maßnahmen unter Berücksichtigung:

- Stand der Technik
- Implementierungskosten
- Art, Umfangs, Umstände und Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeit
- Schwere des Risikos für die Rechte Betroffener

Art. 33 Meldung an die Aufsichtsbehörde

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche den Vorfall unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, an die zuständige Aufsichtsbehörde.

Es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Betroffenen.

Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Art. 35 Datenschutz-Folgenabschätzung

Bei Verarbeitungen mit hohem Risiko für die Rechte und Freiheiten Betroffener, ist vorab eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchzuführen.

- Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist
- Wenn vorhanden, muss der DSB hinzugezogen werden
- Überprüfung bei Änderungen
- Ggf. muss der Standpunkt der Betroffenen eingeholt werden

§ 38 BDSG (neu) Datenschutzbeauftragte nichtöffentlicher Stellen

Verantwortliche und Auftragsverarbeiter benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens **zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Art. 37 DSGVO Benennung eines Datenschutzbeauftragten

Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Zusammenfassung: Dokumentationspflichten

Dokumentationspflichten

Art 26 Abs. 2: Dokumentierte Weisungen, dokumentierte Weisung für Verarbeitung im Drittland
Art 28: Verzeichnis von Verarbeitungstätigkeiten
Art 31: Dokumentation aller Verletzungen des Schutzes pb Daten
Art 44 Abs. 5: Dokumentation von Abwägungen und Garantien bei Drittlandübermittlungen

Nachweispflichten

Art 5: Nachweis der Einhaltung der Verarbeitungsprinzipien
Art 7: Nachweis der Einwilligung
Art 12: Nachweis der Unbegründetheit des Antrags
Art 19: Nachweis für die Erforderlichkeit der Verarbeitung
Art 22: Nachweis für die rechtmäßige Verarbeitung
Art 26: Nachweis im Rahmen der Kontrolle
Art 33: Nachweis zur Einhaltung der DS-GVO

Art. 83 Bußgeldvorschriften

- Beschwerde bei Aufsichtsbehörde
- Gerichtsverfahren gegen Aufsichtsbehörde
- Gerichtsverfahren gegen Verantwortlichen / Auftragsverarbeiter
- Schadensersatzansprüche von Betroffenen oder Verbänden

Die Aufsichtsbehörden müssen bei Verstößen Geldbußen verhängen

- In jedem Fall wirksam, verhältnismäßig und abschreckend
- Berücksichtigung erschwerender oder erleichternder Tatsachen (z. B. Zertifizierung).

Art. 83 Bußgeldvorschriften

Bußgeld	Artikel	Adressat
Bis zu 10.000.000 EUR oder im Fall eines Unternehmens bis zu 2 % seines weltweiten Jahresumsatzes, je nachdem, was höher ist	8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43	Verantwortliche; Auftragsverarbeiter
	42, 43	Zertifizierungsstelle
	41 Abs. 4	Überwachungsstelle
Bis zu 20.000.000 EUR oder im Fall eines Unternehmens bis zu 4 % seines weltweiten Jahresumsatzes, je nachdem, was höher ist	5, 6, 7 und 9, 12-22, 44-49, 58 Abs. 1, 2,	Verantwortliche, Auftragsverarbeiter

Was ist zu tun?

1. Information der Geschäftsleitung

2. Meldung des DSB bei der Aufsichtsbehörde

3. Bestandsaufnahme

- Bestellung, Fachkunde DSB
- Prozesse mit pb Daten
- Rechtsgrundlagen (Vertrag, Einwilligung, ...)
- Dienstleisterbeziehungen
- IT-Sicherheit
- Dokumentationen (Verarbeitungsübersicht)
- Betriebsvereinbarungen
- Produkte (Privacy by Design, Privacy by Default)
- Organisation (Meldepflicht bei Datenschutzpannen)

Was ist zu tun?

4. Umsetzung von Anpassungen

- Anpassung Prozesse / Produkte (Betroffenenrechte, Privacy by Design, Privacy by Default, Informationspflichten bei Pannen)
- Festlegung der Rechtsgrundlagen
- Dokumentationspflichten erfüllen (Verzeichnis der Verarbeitungen, Interessenabwägungen, Risikobewertungen, Datenschutzfolgeabschätzung)
- Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten
- Anpassung von Einwilligungen
- Anpassung von Sicherheitskonzepten (Stand der Technik, Risikobewertung)
- Anpassung von ADV Verträgen
- Anpassungen Betriebsvereinbarungen
- Zertifizierungen erwerben