

Der Entwurf der EU-Datenschutz-Grundverordnung

Wirkung einer EU-Datenschutz-Grundverordnung

- Europäische Verordnungen sind direkt anwendbares Recht
- Nationales Datenschutzrecht wird ersetzt
- Anwendung zwei Jahre nach Veröffentlichung im Amtsblatt
- Öffnungsklauseln
 - Presse, Kunst, Literatur (Art. 80)
 - Gesundheitswesen (Art. 81)
 - BeschäftigtenDS (Art. 82)
 - Historische, statistische, wissenschaftliche Zwecke (Art. 83)
 - Berufsgeheimnisträger (Art. 84)



Zielsetzung der Reform

Europäischen Kommission:

- Betroffene erhalten mehr Kontrolle über ihre Daten
- Datenschutzregeln passend für den digitalen Binnenmarkt
 - Harmonisiert (EUR 2,3 Milliarden Einsparungen durch Vereinheitlichung unterschiedlicher Datenschutzregeln)
 - Vereinfacht (EUR 130 Millionen Einsparung durch Abschaffung von Meldepflichten)
 - Kein „forum-shopping“ (Datenverarbeitung in Mitgliedsstaat mit weniger strengem Datenschutzrecht)
 - „One-stop-shop“ (eine zuständige Aufsichtsbehörde für Unternehmen in der Europäischen Union)
 - Effiziente Kooperation der Datenschutzaufsichtsbehörden
 - Mehr Konsistenz der Anwendung des Datenschutzrechts
 - Globale Standards für Datenschutz werden gesetzt

Verbleibendes uneinheitliches Datenschutzrecht in der EU

- Nationale Umsetzungen der ePrivacy Richtlinie
- Spezielle Bereiche nationalen Umsetzungsspielraums
 - Betroffenenrechte (Artikel 21) -> auch Ausnahmen
 - Presse (Artikel 80) -> auch Ausnahmen
 - Gesundheit (Artikel 81)
 - Arbeitnehmerdatenschutz (Artikel 82)
 - Forschung (Artikel 83)
 - Berufsgeheimnisse (Artikel 84)
 - Kirchen (Artikel 85)

Begrifflichkeiten

Art 4 (1) „betroffene Person“

bestimmte natürliche Person oder natürliche Person, die direkt oder indirekt **mit Mitteln bestimmt werden kann**, die der für die Verarbeitung Verantwortliche oder jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

Art 4 (2)

„personenbezogene Daten“

alle Informationen, die sich auf eine betroffene Person beziehen;

Neue Regelungsansätze

Artikel	Inhalt
8	Verarbeitung personenbezogener Daten eines Kindes
17	Recht auf Vergessenwerden und Löschung
18	Recht auf Datenübertragung
20	Auf Profiling basierende Maßnahmen
23	Datenschutz durch Technik und datenschutzfreundliche Voreinstellung („privacy by design and by default“)
24	Gemeinsam für die Verarbeitung Verantwortliche
13, 26, 28, 29, 30, 33, 42, 44, 51, 77	Verantwortung und Pflichten des Auftragsdatenverarbeiters
31,32	Meldung von Datenschutzverstößen

Einschränkungen für die Verwendung von Daten

- DS-GVO-E (Artikel 6 Abs. 1 (f) und Abs. 4)
 - Interessenabwägungsklausel erlaubt nicht mehr die Abwägung mit Interessen Dritter (nach § 28 Abs. 2 Nr. 2a und § 29 Abs. 2 Nr. 1 BDSG aber zulässig)
 - Zweckbindung kann nicht durch Interessenabwägungsklausel überwunden werden
 - Verbot kommerziellen Direktmarketings ohne Einwilligung wurde wieder gestrichen. Statt dessen Widerspruchslösung und Pflicht zum Hinweis auf Widerspruchsrecht
- Einschränkungen für Personen unter 18 Jahren (Art. 8 DS-GVO-E). Nach Art. 4 (18) „Kind“.

Erweiterte Transparenzpflichten

Artikel 14 und 15 sowie Erwägungsgründe 46, 48 und 51 DS-GVO-E)

• Information des Betroffenen bei der Datenerhebung über

- Speicherdauer
- Recht auf Auskunft, Berichtigung und Löschung
- Recht auf Beschwerde bei der Datenschutzaufsichtsbehörde und deren Kontaktdaten
- Beabsichtigte Drittländertransfers
- Pflicht zur Datenbereitstellung und Folgen der Verweigerung
- Datenherkunft

Das Recht auf Vergessenwerden

Artikel 17 und Erwägungsgrund 53 DS-GVO-E

•Löschung nach

- Widerspruch, wenn nicht überzeugende überwiegende Gründe dagegen sprechen (Beweislastumkehr)
- Rücknahme der Einwilligung
- Löschung in öffentlich zugänglichen Quellen
- Ausnahmen (insbesondere gesetzliche Speicherpflicht)



Das Recht auf Datenübertragbarkeit

Artikel 18 und Erwägungsgrund 55 DS-GVO-E

- Anspruch auf Übermittlung in elektronischer Form in allgemein genutztem Format
- Recht des Betroffenen, die Daten an Dritte weiterzugeben
- Europäische Kommission kann Formate festlegen

Erweiterte Pflichten

- Zusätzliche Pflichten in der Datenschutz-Grundverordnung
 - Strategien und Maßnahmen (Artikel 22)
 - Detaillierte Dokumentation (Artikel 28)
 - Melde- und Informationspflichten bei Datenschutzverstößen (Artikel 31 und 32)
 - Weitergehende Pflicht zur Folgenabschätzung (Artikel 33)
 - Genehmigung und Zurateziehung (Artikel 34)
 - Erweiterte Rechte der Aufsichtsbehörden (Artikel 46 und 54)



Zulässigkeit der Datenverarbeitung

Anforderungen nach DS-GVO-E:

- Art. 6 Abs. 1 (f):
Interessenabwägungsklausel erlaubt nicht mehr die Abwägung mit Interessen Dritter
- Art. 6 Abs. 4:
Zweckbindung kann nicht durch Interessenabwägungsklausel überwunden werden
- Verbot des Direktmarketings ohne Einwilligung in Vorentwürfen wurde wieder gestrichen.

Verfahrensfestlegungen zur Transparenz

Anforderungen nach Art 12 DS-GVO-E:

- Grds. Bereitstellung von Möglichkeiten für elektronische Eingaben (Authentifizierung?)
- Unverzögliche Informationspflicht, spätestens innerhalb 1 Monat, max. Verlängerung um weiteren Monat
- Unterrichtung schriftlich. Stellt der Betroffene den Antrag elektronisch, ist auf elektronischem Weg zu unterrichten, sofern nichts anderes angegeben.
- Grds. entgeltfrei
- Bei Auskunftsverweigerung ist Begründung und Hinweis auf zust. Aufsichtsbehörde und Rechtsmittel erforderlich

Informationspflichten bei der Datenerhebung (1)

Allgemein zugängliche Datenschutzrichtlinien des Unternehmens bzgl. der Betroffenenrechte

Art 11: Der für die Verarbeitung Verantwortliche verfolgt in Bezug auf die Verarbeitung personenbezogener Daten und die Ausübung der den betroffenen Personen zustehenden Rechte eine **nachvollziehbare und für jedermann leicht zugängliche Strategie**. Der für die Verarbeitung Verantwortliche stellt der betroffenen Person alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten in verständlicher Form unter Verwendung einer klaren, einfachen und adressatengerechten Sprache zur Verfügung, besonders dann, wenn die Information an ein Kind gerichtet ist.

Informationspflichten bei der Datenerhebung (2)

Anforderungen nach Art 14 DS-GVO-E:

- Namen, Kontaktdaten auch des DSB
- Zwecke ... ggf. berechnete Interessen
- Dauer der Speicherung
- Auskunfts-, Berichtigungs-, Lösungs-, Widerspruchsrecht
- Beschwerderecht bei Aufsichtsbehörde und Kontaktdaten
- Empfänger oder Kategorien von Empfängern
- Ggf. Drittlandtransfer
- sonstige Informationen
- Daten obligatorisch oder fakultativ, Folgen der Verweigerung

Ggf. Standardvorlagen der EU-Kommission

Auskunftspflichten

Anforderungen nach Art 15 DS-GVO-E:

- Auskunft an den Betroffenen über BDSG hinaus u.a.
 - Dauer der Speicherung
 - diejenigen personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten,
 - Betroffenenrechte, Hinweis auf Aufsichtsbehörde
 - Tragweite/Auswirkungen der Datenverarbeitung, zumindest bei Profilbildung
- Bei elektronischem Antrag, ist Auskunft auch auf elektronischem Weg zu erteilen, sofern nichts anderes angegeben



Löschpflichten

Anforderungen nach Art 17 (1 u. 2) DS-GVO-E

- Personenbezogene Daten sind zu löschen, wenn:
 - Nicht mehr erforderlich
 - Widerruf der Einwilligung und keine alternative Erlaubnis zur Speicherung
 - Widerspruch gemäß Art. 19 (besondere Situation des Betroffenen, Werbung)
 - Sonstige Unzulässigkeit der Datenverarbeitung
- Right to be forgotten
 - Bei Veröffentlichung von Daten, müssen angemessene, auch technische Maßnahmen, ergriffen werden um dritte Parteien über Löschungswunsch zu informieren



Dokumentations- und Nachweispflichten

Anforderungen nach DS-GVO-E:

- Art. 22: Verpflichtung zum Nachweis von Strategien und Maßnahmen zur Gewährleistung insbesondere von
 - Allgemeinen Dokumentationspflichten, Art. 28
 - Datensicherheit, Art. 30
 - Data Protection Impact Assessments, Art. 33
 - Vorherige Zurateziehung der Aufsichtsbehörde, Art. 34
 - Bestellung eines DSB, Art. 35
- Art. 31 Abs. 4: Dokumentation von Datenverlusten

Dokumentationspflichten

- Art. 28: Mindestangaben zu DV-Verfahren
 - Name/Kontakt verantwortliche Stelle(n)
 - Kontaktdaten DSB
 - Zweck der Datenverarbeitung, einschl. berechtigtes Interesse
 - Kategorien der Betroffenen und Daten
 - Empfänger/-kategorien
 - Geplante Übermittlung in Drittländer
 - Regelfristen für die Löschung
 - Auditverfahren gemäß Art. 22 Abs. 3
- Aufsichtsbehörde kann Vorlage verlangen

Ausnahmen der Dokumentationspflicht

Die genannten Anforderungen gelten nicht für

- a) natürliche Personen, die personenbezogene Daten ohne eigenwirtschaftliches Interesse verarbeiten; oder
- b) Unternehmen oder Organisationen mit **weniger als 250** Beschäftigten, die personenbezogene Daten **nur als Nebentätigkeit** zusätzlich zu ihren Haupttätigkeiten verarbeiten



Datenschutz-Folgeabschätzung

- Art. 33: Eine Folgenabschätzung muss durchgeführt werden, bei (über BDSG hinaus)
 - weiträumiger Überwachung öffentl. Bereiche, insb. Video
 - Daten von Kindern und biometrischen/genetischen Daten
 - Vorabvorlagepflicht Aufsichtsbehörde
- Bewertung muss mindestens enthalten
 - Allg. Beschreibung der DV
 - Bewertung der Risiken für Rechte/Freiheiten Betroffener
 - Sicherheitsmaßnahmen
- Der Verantwortliche holt die Meinung der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein.

Data Breach Notification

- Art. 31: Anzeigepflicht bei Datenverlust
- Erfasst alle personenbezogenen Daten
- Bei jeglichem unberechtigten Zugriff (auch innerhalb der verantw. Stelle?)
- Meldepflicht gegenüber Aufsichtsbehörde grds. innerhalb von 24 Stunden (einschl. Auftragnehmer!)
- Inhalt wie unter BDSG
- Meldepflicht gegenüber Betroffenen, ohne unangemessene Verzögerung nach Unterrichtung der Behörde, es sei denn erfolgreicher Nachweis, dass Verschlüsselung
- Aufsichtsbehörde kann in jedem Fall Benachrichtigung der Betroffenen verlangen

Zusammenarbeit mit Aufsichtsbehörden

- Art. 29: Pflicht zur Informationsbereitstellung und Zugang; Beantwortungsfrist wird durch Aufsichtsbehörde gesetzt
- Art. 34: Genehmigungs- und Anzeigepflichten
 - Genehmigung bei Drittlandtransfers
 - Anzeigepflicht, wenn die Folgenabschätzung ein hohes Risiko ausweist oder nach Anforderung der Aufsichtsbehörde gemäß Abs. 2b
- Zuständigkeit: Art. 51 Abs. 2
 - Aufsichtsbehörde am Hauptsitz des Unternehmens ist zuständig auch für Niederlassungen in anderen Ländern

Sanktionen für Unternehmen

Maximale Strafe in % des globalen Umsatzes	Wenn die verantwortliche Stelle beispielsweise vorsätzlich oder fahrlässig:
0,5 %	<ul style="list-style-type: none">• Auf Anfragen des Betroffenen nicht reagiert• Gebühren für Auskünfte erhebt• Nicht über interne Richtlinien informiert (unklar)
1 %	<ul style="list-style-type: none">• Gegen Transparenz- und Löschungspflichten verstößt• Widersprüche nicht beachtet• Die Dokumentationspflichten nicht einhält
2 %	<ul style="list-style-type: none">• Daten rechtswidrig verarbeitet• Regeln zu internationalen Datenübermittlungen nicht einhält• Keine angemessenen internen Richtlinien hat oder keine Folgenabschätzung durchführt• Keinen Inlandsvertreter benennt



Betrieblicher Datenschutzbeauftragter

Art. 35 – 37 DS-GVO-E

- Art. 35 Abs. 1 lit. (a): Muss bestellt werden, wenn das Unternehmen dauerhaft mehr als 250 Personen beschäftigt
- Art 35 Abs. 1 lit. (b): Muss bestellt werden, wenn die
 - Kerntätigkeit der verantwortlichen Stelle oder des Auftragsverarbeiters
 - besteht in Datenverarbeitungen,
 - die nach ihrem Wesen, Umfang oder ihrem Zweck
 - die regelmäßige und systematische Beobachtung von Betroffenen
 - erforderlich machen
- Abs. 7: Bestellung und Kündigungsschutz für mindestens 2 Jahre



Betrieblicher Datenschutzbeauftragter

- Die verbindliche europaweite Einführung der betrieblichen Selbstkontrolle durch einen DSB trägt den auf deutscher Ebene gemachten guten Erfahrungen Rechnung
- Ein Vergleich hinsichtlich der Aufgaben und Rechtsstellung des DSB nach der DS-GVO-E und dem BDSG zeigt, dass sich die EU-Kommission auch an den Regelungen des deutschen Datenschutzrechts orientiert hat.
- Sinnvollerweise werden dabei Aufgaben, die im BDSG weitgehend durch ein gesetzgeberisch unglücklich formuliertes „Hinwirken“ (§ 4g Abs. 1 Satz 1 BDSG) umschrieben sind, in wesentlichen Teilen konkretisiert. Es fehlt jedoch das gestaltende Element.



Betrieblicher Datenschutzbeauftragter

- Datenschutzaufsicht wird nicht entbürokratisiert. Potenzial einer betriebl. Selbstkontrollinstanz jedoch nicht ausgeschöpft
- Neue Verpflichtungen zur Zusammenarbeit mit bzw. Unterstützung der Aufsichtsbehörde führen zu gradueller Verschiebung: Weg vom DSB als unabhängigem betrieblichen Kontrollorgan hin zum Compliance-Organ mit Verpflichtung zur Unterstützung der staatlichen Fremdkontrolle
- Fehlende Schutzmechanismen (grundlose Befristung, kein Kündigungsschutz, fehlende Regelung zur Verschwiegenheit und zum Benachteiligungsverbot) wirken für eine wirksame Selbstkontrolle kontraproduktiv. Nachbesserungsbedarf!



Vielen Dank für Ihre
Aufmerksamkeit!

