

DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG - EIN ÜBERBLICK -

1

© 2016 DATAKONTEXT GmbH

Ziele der Datenschutz-Grundverordnung (DS-GVO)

- Betroffene erhalten **mehr Kontrolle** über ihre Daten
- **Globale Standards** für Datenschutz werden gesetzt
- 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

3

© 2016 DATAKONTEXT GmbH

Die EU Datenschutz-Grundverordnung

Grundsätzliches zur Datenschutzgrundverordnung

Überblick über wesentliche Inhalte

Überblick zur Datenschutzorganisation

2

© 2016 DATAKONTEXT GmbH

Wirkungen der DS-GVO

Art. 91:

„... Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat.“

- Die DS-GVO ist eine allgemeine Regelung mit unmittelbarer innerstaatlicher Geltung
-> „**Durchgriffswirkung**“
- Grundsätzliche Vollharmonisierung im nicht-öffentlichen Bereich
- Ersetzt nationales Datenschutzrecht, führt grds. zur Unanwendbarkeit entgegenstehender nationaler Regelungen
- Öffnungsklauseln für nationalen Gesetzgeber in bestimmten Bereichen – Richtlinien-Charakter im öffentlichen Bereich
- Zweijährige Anpassungsphase für Rechtsbereinigung und Folgeänderungen



4

© 2016 DATAKONTEXT GmbH

Öffnungsklauseln

Verpflichtung der Mitgliedstaaten zum Tätigwerden

DS-GVO

Befugnis der Mitgliedstaaten für spezifische und/oder abweichende Regelungen

Ca. 50 – 60 Öffnungsklauseln:

- bei Rechtsgrundlagen der Datenverarbeitung
- für spezifischere nationale Regelungen
- für Ausnahmen von Betroffenenrechten
- für andere Fälle

GDD

DATAKONTEXT

5

Anpassung in Deutschland

Anpassung in Deutschland

Insbesondere BDSG z. B.:

- DSB (§ 4f)
- Beschäftigten-datenschutz (§ 32)
- Aufsicht (§ 38)
- Sanktionen (§ 44)
- Zertifizierung
- ...

Weitere gesetzliche Regelungen zum Datenschutz, insbesondere:

- Landesdatenschutzgesetze
- SGB X
- Kirchliche DSG
- ...
- Auch z. B. Datenschutzkodex der Presse

GDD

DATAKONTEXT

© 2016 DATAKONTEXT GmbH

Auswirkung auf bestehende Regelungen

<div style="display: flex; align-items: center; justify-content: center;"> <div style="width: 15px; height: 10px; background-color: black; margin-right: 5px;"></div> National </div>	<div style="display: flex; align-items: center; justify-content: center;"> <div style="width: 15px; height: 10px; background-color: #0056b3; margin-right: 5px;"></div> Europa </div>
<p>•öffentlicher Bereich: Fortbestand der wesentlichen allgemeinen und der bereichsspezifischen Regelungen</p> <p>•nicht-öffentlicher Bereich: weitgehende Ersetzung durch DS-GVO</p> <ul style="list-style-type: none"> •Rechtsbereinigungsaufgaben im <ul style="list-style-type: none"> – BDSG – LDSG´s – bereichsspezifischen Datenschutzrecht wie Melderecht, Sozialrecht usw. •Nicht betroffen sind z. B. (zunächst) <ul style="list-style-type: none"> – TMG ? – TKG – BetrVG – UWG 	<ul style="list-style-type: none"> •EU-DS-Rili (RL 95/46/EG) wird aufgehoben •E-Privacy-RL 2002/58 bleibt bestehen, aber Reformpflicht •Reformpflicht der VO 45/2001 •Fortbestand (bis auf Widerruf) der <ul style="list-style-type: none"> – Angemessenheitsbeschlüsse für Drittländer – BCR-Anerkennungen – Standardvertragsklauseln – Bestehenden Einwilligungen <ul style="list-style-type: none"> •Aufbau des Europäischen Datenschutzausschusses

GDD

DATAKONTEXT

6

Ausgestaltung / Überwachung

Kommission

- Überwachung der Umsetzung der DS-GVO
- Erlass delegierter Rechtsakte

EuGH

- Auslegung der DS-GVO
- Kontrolle der Kommissionsentscheidungen

DS-GVO

Europäischer Datenschutzausschuss

- Interpretation der DS-GVO
- Koordination der Zusammenarbeit

Nationale Gerichte

- Auslegung der DS-GVO und nationaler Datenschutzvorschriften

Mitgliedsstaaten

- Ergänzen und modifizieren den Rechtsrahmen

Aufsichtsbehörden

- Überwachung der Umsetzung des Datenschutzes (Zusammenarbeit)

GDD

DATAKONTEXT

8

Interpretation/Auslegung der Gesetze

GDD
DATAKONTEXT

■ DS-GVO

Keine gefestigte Interpretations- bzw. Auslegungshilfen:

- EuGH-Rechtsprechung bezieht sich auf Richtlinie 95/46/EG
- Stellungnahmen/Orientierungshilfen des Europäischen Datenschutzausschusses müssen erst noch formuliert werden
- Kommentierungen aus der Literatur existieren noch nicht

➢ Unternehmen werden sich anfangs einer großen Rechtsunsicherheit bei der Auslegung der EU-DS-GVO stellen müssen.

➢ Eine unterschiedliche Auslegungspraxis in den Mitgliedstaaten muss durch den Europäischen Datenschutzausschuss und den EuGH nivelliert werden.

9 © 2016 DATAKONTEXT GmbH

GDD
DATAKONTEXT

Die EU Datenschutz-Grundverordnung

Grundsätzliches zur Datenschutzgrundverordnung

Überblick über wesentliche Inhalte

Überblick zur Datenschutzorganisation

11 © 2016 DATAKONTEXT GmbH

Zeitliche Auswirkungen

GDD
DATAKONTEXT

Einigung im Trilog: 17./18.12.2015

Verkündung: 04. Mai

Annahme d. Rat und EP: April

Inkrafttreten / Beginn der Umsetzungsfrist: 25. Mai

Geltung / Ende der Umsetzungsfrist: 25. Mai

- **BDSG gilt weiter**
 - **Beginn der Umsetzungsfrist** (...Verarbeitungen, die zum Zeitpunkt des Inkrafttretens dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. ... (EG 134))
 - Ermächtigung der Kommission zum Erlass **delegierter Rechtsakte** (Art. 86 Abs. 2)
- **BDSG ist nicht mehr anwendbar**
 - **Aufhebung** der EU-DS-RiII (RL 95/46/EG) (Art 88)
 - **Verarbeitungen** müssen im Einklang mit der GVO sein
 - **Ablauf** diverser Melde-/ Erklärungspflichten der Mitgliedsstaaten bezüglich nationaler Regelungen

10 © 2016 DATAKONTEXT GmbH

Gliederung der DS-GVO

GDD
DATAKONTEXT

- Kapitel I: Allgemeine Bestimmungen Grundsätze
- Kapitel II: Rechte der betroffenen Person
- Kapitel III: Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter
- Kapitel IV: Übermittlung personenbezogener Daten an Drittländer o. an internationale Organisationen
- Kapitel V: Unabhängigkeit der Aufsichtsbehörden Zusammenarbeit und Kohärenz Rechtsbehelfe, Haftung und Sanktionen
- Kapitel VI: Vorschriften für besondere Datenverarbeitungssituationen
- Kapitel VII: Delegierte Rechtsakte und Durchführungsrechtsakte
- Kapitel VIII: Schlussbestimmungen

12

Reduzierte Verarbeitungstatbestände

**Art. 6
Rechtmäßigkeit
der Verarbeitung**

Nationales Recht

Art. 7 Einwilligung

Art. 8 Einwilligung eines Kindes

Art. 9 Besondere Datenkategorien

Art. 10 Verurteilungen und Straftaten

Art. 11 Verarbeitung ohne Bestimmung der Betroffenen

**KAPITEL II
GRUNDSÄTZE**

Artikel 5 Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten
(Prinzipien zur Datenverarbeitung)

13 © 2016 DATAKONTEXT GmbH

Prinzipien zur Datenverarbeitung – Art. 5

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	• Verarbeitung auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für den Betroffenen nachvollziehbaren Weise
Zweckbindung	• Erhebung für festgelegte, eindeutige und rechtmäßige Zwecke und Verbot der Weiterverarbeitung in einer mit diesen Zwecken nicht zu vereinbarenden Weise
Datenminimierung	• Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß
Richtigkeit	• sachlich richtige und ggf. aktuellste Daten, Vorsehen von Maßnahmen zur unverzüglichen Löschung oder Berichtigung von unzutreffenden Daten
Speicherbegrenzung	• Speicherung mit Personenbezug höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist;
Integrität und Vertraulichkeit	• geeignete TOM zum angemessenen Schutz der Daten insbes. vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung

Rechenschaftspflicht (Accountability):

- Verantwortung und
- Nachweispflicht für die Einhaltung der Prinzipien

15 © 2016 DATAKONTEXT GmbH

Rechtmäßigkeit der Datenverarbeitung

Für die Verarbeitung personenbezogener Daten normiert Art. 6 DSGVO als allgemeinen Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt.

Die Verarbeitung von Daten ist demnach nur zulässig, wenn eine Einwilligung oder eine andere in dieser Vorschrift normierte Ausnahme vorliegt. Dies ist der Fall, wenn

- die Verarbeitung für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen;
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt;
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- wenn sie im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich ist oder
- sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Dieser Rechtfertigungsgrund gilt nicht für Behörden.

16 © 2016 DATAKONTEXT GmbH

Datenportabilität

Art. 20


- Erweiterung des Auskunftsrechts: Recht auf Erhalt einer Kopie seiner Daten
- Erweiterung durch Portierbarkeit der Daten zu einem Wettbewerbsdienst
- Eine Kopie kann vom Betroffenen herausverlangt werden als strukturiertes, gängiges und maschinenlesbares Format
 - „Strukturiert“ bedeutet Datenbankformat (XML); komma-separierte Liste, SQLite usw.)
- hinderungsfreie Übermittlung an andere Stelle, ggf. Direktübermittlung (Abs. 2a)
- Gilt nur bei Verarbeitung aufgrund Einwilligung oder Vertrag.
- **AUSNAHME:** Die Portierung beeinträchtigt Rechte und Freiheiten anderer Personen
- **ACHTUNG:** Im Text keine Beschränkung auf Internetdienste!

Schnittstellen für die Datenportabilität müssen vorhanden sein

16 © 2016 DATAKONTEXT GmbH

GD

„Recht auf Vergessenwerden“

Art. 17 Abs. 2 

- Vom Verantwortlichen veröffentlichte Daten sind nach den Vorgaben des Art. 17 Abs. 1 zu löschen (vorbehaltlich der Ausnahmen nach Art. 17 Abs. 3).
- Zudem:** Information anderer für die Datenverarbeitung Verantwortlicher über das Verlangen des Betroffenen zur Löschung
 - aller Links zu diesen personenbezogenen Daten oder
 - von Kopien oder Replikationen dieser Daten
- Berücksichtigung der verfügbaren Technologie und der Implementierungskosten
- Vergleichbar § 35 VII

DATAKONTEXT

17

GDD

Schutzkonzept

Überwachung durch den Datenschutzbeauftragten
(Art. 37 – 39 DS-GVO)

Standards und Zertifizierung
(Art. 42 – 43 DS-GVO)

Dokumentation und Nachweise
(Verfahrenswissen der DS-GVO)

Organisatorische Absicherung
(Art. 24 – 31, 33 – 36 DS-GVO)

Technische Absicherung
(Art. 25, 32 DS-GVO)

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

GDD

Die EU Datenschutz-Grundverordnung

Grundsätzliches zur Datenschutzgrundverordnung

Überblick über wesentliche Inhalte

Überblick zur Datenschutzorganisation


DATAKONTEXT

17


© 2016 DATAKONTEXT GmbH

GDD


DSB: Evolution der Aufgabenstellung



Sicherstellungsauftrag
(§ 29 Abs. 1 BDSG 1977 / § 37 Abs. 1 BDSG 1990)



Hinwirkungsauftrag
(§ 4g Abs. 1 BDSG 2001)



Überwachungsauftrag
(Art 39 Abs. 1 DS-GVO 2016)

DATAKONTEXT

20

© 2016 DATAKONTEXT GmbH

Datenschutzbeauftragter – Bestellpflicht – Art. 37

GDD

DATAKONTEXT

Verpflichtend

- Öffentliche Stellen
- Unternehmen
- > *Kerntätigkeit besteht aus Verarbeitungsvorgängen, welche auf Grund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung [monitoring] von betroffenen Personen erforderlich machen*
- > *Datenverarbeiter, deren Kerntätigkeit aus der Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 und 9a der DS-GVO in großem Umfang besteht*
- Nationale Öffnungsklausel: Nachfolgeregelung zu § 4f

Freiwillig

- Alle übrigen für die Verarbeitung Verantwortlichen

21

© 2016 DATAKONTEXT GmbH

Privacy by design / Privacy by default

GDD

DATAKONTEXT

Privacy by design

Unter Berücksichtigung des Stands der Technik ... 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; ...**

Nachweis durch Zertifizierung nach Art 42 möglich

Möglichkeiten müssen in der Software implementiert sein Produkt-Zertifizierung ist möglich

23

© 2016 DATAKONTEXT GmbH

Verarbeitungen / Prozesse

GDD

DATAKONTEXT

Art. 5 Abs. 2: Prinzip „Rechenschaftspflicht“ (Accountability):
„Der für die Verarbeitung Verantwortliche ist für die Einhaltung des Absatzes 1 [Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten] verantwortlich und muss dessen Einhaltung nachweisen können.“

22

© 2016 DATAKONTEXT GmbH

Datenschutz-Folgenabschätzung

GDD

DATAKONTEXT

Art. 35

3. Die Folgenabschätzung enthält zumindest Folgendes:

- (a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen;
- (b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- (c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1;
- (d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Ausreichende Dokumentationen hierzu müssen vorhanden sein

24

© 2016 DATAKONTEXT GmbH

Sicherheit der Verarbeitung – Art. 32

GDD

DATAKONTEXT

- Angemessen, unter Beachtung insbes. des „Stands der Technik“, Risikoadäquat
- Fokussierung auf die IT-Sicherheitsziele:
 - Vertraulichkeit
 - Integrität
 - Verfügbarkeit
- Sicherheitsmanagement

Als Dienstleister müssen ausreichende Nachweise zur Verfügung gestellt werden können

25

© 2016 DATAKONTEXT GmbH

Dokumentations- und Nachweispflichten

GDD

DATAKONTEXT

Dokumentationspflichten z. B.

- Art 30 Abs. 2 (a)
 - Dokumentierte Weisungen
 - Dokumentierte Weisung für Verarbeitung im Drittland
- Art 30: Verzeichnis von Verarbeitungstätigkeiten
- Art 33: Dokumentation aller Verletzungen des Schutzes personenbezogener Daten
- Art 46 Abs. 5: Dokumentation von Abwägungen und Garantien bei Drittlandübermittlungen

Nachweispflichten z. B.

- Art 5 Abs. 2: Nachweis der Einhaltung der Verarbeitungsprinzipien
 - Art 7: Nachweis der Einwilligung
 - Art 12: Nachweis der Unbegründetheit des Antrags
 - Art 22: Nachweis für die Erforderlichkeit der Verarbeitung
 - Art 24: Nachweis für die rechtmäßige Verarbeitung
 - Art 26: Nachweis im Rahmen der Kontrolle
 - Art 35: Nachweis zur Einhaltung der DS-GVO

Viele Dokumentationen und Nachweise müssen erbracht werden können

27

© 2016 DATAKONTEXT GmbH

Verzeichnis von Verarbeitungstätigkeiten - Art. 30

GDD

DATAKONTEXT

- Verantwortlicher: „Verzeichnis aller Verarbeitungstätigkeiten“
- Auftragsverarbeiter: Kundenbezogene Aufzeichnung der „durchgeführten Tätigkeiten ...“
- Nicht öffentlich / Einsicht für Aufsichtsbehörden
- Dokumentation ähnlich Verfahrnsverzeichnis
- Zusätzlich aufzunehmen: Beurteilung und Garantien bei Drittlandsübermittlungen gemäß Art. 49 Abs. 1 (g)
- Ausnahmen für Unternehmen unter 250 MA – häufig nicht einschlägig
- **Achtung:** Daneben bestehen weitere Dokumentationspflichten

26

© 2016 DATAKONTEXT GmbH

Nachweis der IT-Sicherheit

GDD

DATAKONTEXT

Art. 32 DS-GVO / Garantien

↓

Konkretisierung

Verhaltensregeln

Einhalten von Verhaltensregeln

- EU-Mitgliedsstaaten
- EU-Kommission
- EU-Datenschutzausschuss
- Aufsichtsbehörden
- Verbände

Zertifizierung

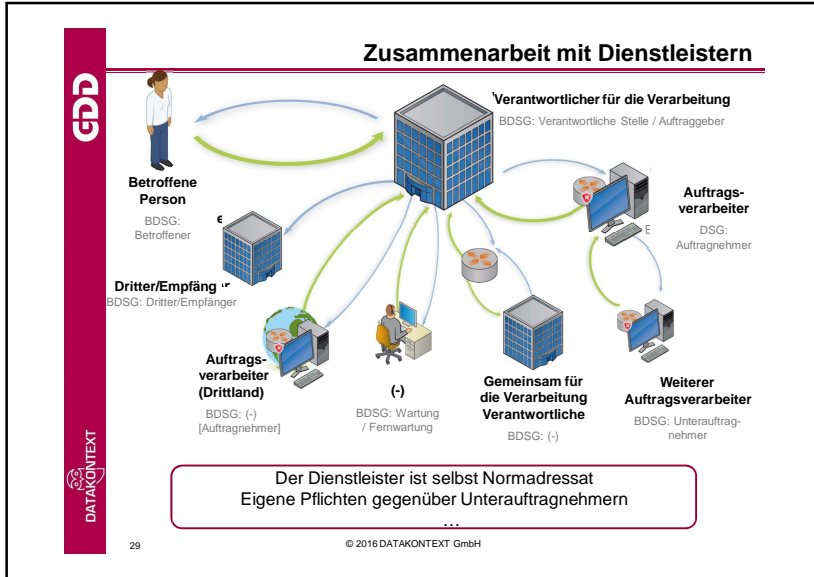
- EU-Kommission (delegierte Rechtsakte)
- EU-Mitgliedsstaaten
- EU-Datenschutzausschuss
- Aufsichtsbehörden

Viele Nachweise können über Zertifizierung erbracht werden
ISO- Zertifikate etc. entsprechen dem (bisher) nicht

28

© 2016 DATAKONTEXT GmbH

7



Verschärfung der Bußgeldvorschriften, Art. 83 Abs. 4, 5, 6

<ul style="list-style-type: none"> o Bis zu 10.000.000 EUR oder im Fall eines Unternehmens bis zu 2 % seines weltweiten Jahresumsatzes, je nach dem, was höher ist o Bis zu 20.000.000 EUR oder im Fall eines Unternehmens bis zu 4 % seines weltweiten Jahresumsatzes, je nach dem, was höher ist 	Pflichten gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43; 42, 43 41 Abs. 4 Verstöße gegen die folgenden Bestimmungen: Artikel 5, 6, 7 und 9, 12-22, 44-49, 58 Abs. 1, 2,	Verantwortliche; Auftragsverarbeiter Zertifizierungsstelle Überwachungsstelle Verantwortliche, Auftragsverarbeiter
--	--	---

Berücksichtigung erschwerender und erleichternder (z. B. Zertifizierung) Tatsachen aber:
In jedem Fall
“wirksam, verhältnismäßig und abschreckend”

© 2016 DATAKONTEXT GmbH

Sanktionen - Systematik

Rechtswege:

- Beschwerde bei Aufsichtsbehörde
- Gerichtsverfahren gegen Aufsichtsbehörde
- Gerichtsverfahren gegen Verantwortlichen für die Verarbeitung / Auftragsverarbeiter

Vertretung:

- Vertretung des Betroffenen durch einen Verband
- Verbandsklagerecht

(nach nationalem Recht)

Sanktionen:

- Schadensersatz
- Bußgeld
- Strafe (nach nationalem Recht)

© 2016 DATAKONTEXT GmbH

Vielen Dank für Ihre Aufmerksamkeit!

© 2016 DATAKONTEXT GmbH