Datenschutz-Grundverordnung

aus Wikipedia, der freien Enzyklopädie

Basisdaten der Verordnung (EU) 2016/679	
Titel:	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
Kurztitel: (nicht amtlich)	DS-GVO, DSGVO
Kurztitel:	Datenschutz-Grundverordnung
Rechtsnatur:	Verordnung
Geltungsbereich:	EWR (schließt die Europäische Union ein)
Rechtsmaterie:	Datenschutzrecht
Veröffentlichung:	Nicht-amtliche konsolidierte Fassung • Verordnung (EU) 2016/679 (ABl. L 119, S. 1–88). Verordnung berichtigt durch: • Berichtigung der Verordnung (EU) 2016/679 (ABl. L 314 vom 22. November 2016, S. 72) und • Berichtigung der Verordnung (EU) 2016/679 (ABl. L 127 vom 23. Mai 2018, S. 2–8)
Inkrafttreten:	24. Mai 2016
Anzuwenden ab:	25. Mai 2018
Bitte den Hinweis zur geltenden Gesetzesfassung beachten!	

Die **Datenschutz-Grundverordnung** (**DSGVO**; frz. *Règlement général sur la protection des données* RGPD, engl. *General Data Protection Regulation* GDPR) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union

sichergestellt, und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Die Verordnung ersetzt die aus dem Jahr 1995 stammende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Zusammen mit der sogenannten JI-Richtlinie für den Datenschutz in den Bereichen Polizei und Justiz[1] bildet die DSGVO seit dem 25. Mai 2018 den gemeinsamen Datenschutzrahmen in der Europäischen Union.[2]

Inhaltsverzeichnis

Unmittelbare Geltung; nationale Sonderregelungen

Im Gegensatz zur Richtlinie 95/46/EG, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, gilt die Datenschutz-Grundverordnung unmittelbar in allen EU-Mitgliedstaaten ab dem 25. Mai 2018. Die Mitgliedstaaten bringen jedoch durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang (Art. 85 und 86 der Verordnung). Für diese und andere Rechtsvorschriften ist die Datenschutz-Grundverordnung bereits seit ihrem Inkrafttreten am 24. Mai 2016 maßgeblich. Den Mitgliedstaaten ist es sonst grundsätzlich nicht erlaubt, den von der Verordnung festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken. Allerdings enthält die Verordnung verschiedene Öffnungsklauseln, die es den einzelnen Mitgliedstaaten ermöglichen, bestimmte Aspekte des Datenschutzes auch im nationalen Alleingang zu regeln. Daher wird die Datenschutz-Grundverordnung auch als „Hybrid“ zwischen Richtlinie und Verordnung bezeichnet.[3]

Regelungsbedarf gibt es damit sowohl im Hinblick auf die Öffnungsklauseln der Datenschutz-Grundverordnung als auch wegen des Bedarfs der Bereinigung nationalen Datenschutzrechts. Diese Ziele sollen in Deutschland auf Bundesebene mit der Neufassung des Bundesdatenschutzgesetzes und der Änderung weiterer Gesetze erreicht werden.[4] Das Gesetz vom 30. Juni 2017[4] hebt nationales Datenschutzrecht auf oder überführt die bei Inkrafttreten der Datenschutz-Grundverordnung unwirksamen Regelungen des bisherigen Bundesdatenschutzgesetzes in andere Gesetzesbereiche, es passt Regelungen an und schafft teils neue Vorschriften für den Datenschutz. Bereits bei der Diskussion um die diversen Referentenentwürfe des Bundesinnenministeriums, das bei der Gesetzgebung federführend war, haben Datenschützer die unzureichende Berücksichtigung der Erfahrungen der letzten Jahre bemängelt.[5] Juristen bezweifeln die Vereinbarkeit des angepassten Bundesdatenschutzgesetzes mit europäischem Recht.[6]

Inhalt

Die Datenschutz-Grundverordnung ist Teil der EU-Datenschutzreform, welche die Europäische Kommission am 25. Januar 2012 vorgestellt hat.[7][8]

Aufbau der DSGVO

Die DSGVO besteht aus 99 Artikeln in elf Kapiteln:

- Kapitel 1 (Artikel 1 bis 4): Allgemeine Bestimmungen (Gegenstand und Ziele, sachlicher und räumlicher Anwendungsbereich, Begriffsbestimmungen)
- Kapitel 2 (Artikel 5 bis 11): Grundsätze und Rechtmäßigkeit (Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, Bedingungen für die Einwilligung, Verarbeitung besonderer Kategorien personenbezogener Daten)
- Kapitel 3 (Artikel 12 bis 23): Rechte der betroffenen Person (Transparenz und Modalitäten, Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten, Berichtigung und Löschung – das „Recht auf Vergessenwerden“ –, Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall einschließlich Profiling)

- Kapitel 4 (Artikel 24 bis 43): Verantwortlicher und Auftragsverarbeiter (Allgemeine Pflichten, Sicherheit personenbezogener Daten, Datenschutz-Folgenabschätzung und vorherige Konsultation, Datenschutzbeauftragter, Verhaltensregeln und Zertifizierung)
- Kapitel 5 (Artikel 44 bis 50): Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen
- Kapitel 6 (Artikel 51 bis 59): Unabhängige Aufsichtsbehörden
- Kapitel 7 (Artikel 60 bis 76): Zusammenarbeit und Kohärenz, Europäischer Datenschutzausschuss
- Kapitel 8 (Artikel 77 bis 84): Rechtsbehelfe, Haftung und Sanktionen
- Kapitel 9 (Artikel 85 bis 91): Vorschriften für besondere Verarbeitungssituationen (u. a. Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit, Datenverarbeitung am Arbeitsplatz, Zugang der Öffentlichkeit zu amtlichen Dokumenten, Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken, bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften)
- Kapitel 10 (Artikel 92 bis 93): Delegierte Rechtsakte und Durchführungsrechtsakte
- Kapitel 11 (Artikel 94 bis 99): Schlussbestimmungen (u. a. Aufhebung der Richtlinie 95/46/EG und Inkrafttreten der DSGVO)

Vor den 99 Artikeln sind 173 Erwägungsgründe angeführt, die zur Auslegung der Artikel mit herangezogen werden.[9][10]

Bereiche der Neuregelung

Viele Bereiche des Datenschutzes werden durch die DSGVO *nicht* neu geregelt. Insbesondere bleibt der Begriff der „personenbezogenen Daten“ im Artikel 4 weiterhin weit gefasst:

> „personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann; …

Weiterhin gilt ebenfalls, dass die Verarbeitung personenbezogener Daten nur aufgrund eines Erlaubnistatbestands zulässig ist. Diese sind im Artikel 6 aufgeführt:

- Die betroffene Person hat ihre Einwilligung gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich.

Im letzten Fall ist eine Interessensabwägung gegenüber den Interessen der betroffenen Person erforderlich.

Zusammenfassend gilt:

> „Die DSGVO ändert die Konzeption und weitgehend auch die Detailregelungen des geltenden Datenschutzrechts nicht grundlegend. Vielmehr werden vielfach Bestimmungen der EG-Datenschutzrichtlinie 95/46 übernommen, die die Grundlage des BDSG bilden. Andererseits gibt es aber auch zahlreiche neue datenschutzrechtliche Vorgaben, deren Erfüllung allein schon hinsichtlich des immens erhöhten Bußgeldrahmens korrekter Beachtung bedarf.“[11]

Zu folgenden Themenbereichen liefert die DSGVO Neuregelungen oder grundsätzliche Präzisierungen:

Grundsätze der Verarbeitung personenbezogener Daten

Die DSGVO führt im Artikel 5 explizit folgende sechs Grundsätze für die Verarbeitung personenbezogener Daten auf:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung (Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke)
- Datenminimierung („dem Zweck angemessen und erheblich sowie auf das […] notwendige Maß beschränkt“)
- Richtigkeit („es sind alle angemessenen Maßnahmen zu treffen, damit [unrichtige] personenbezogene Daten unverzüglich gelöscht oder berichtigt werden“)
- Speicherbegrenzung (Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es […] erforderlich ist“)
- Integrität und Vertraulichkeit („angemessene Sicherheit der personenbezogenen Daten […], einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“)

Der Verantwortliche muss die Einhaltung dieser Grundsätze nachweisen. Die Nichteinhaltung dieser Grundsätze und der Rechenschaftspflicht kann mit einem angemessenen Bußgeld in Höhe von bis zu 20 Millionen EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes geahndet werden (Artikel 83 Absatz 5 Buchstabe a).

Diese Grundsätze stellen die Programmatik der Verordnung dar.[12] Die Regelung war fast wortlautgleich Teil der Datenschutzrichtlinie (Art. 6 Richtlinie 95/46/EG) und als diese bis 1998 in nationale Gesetzgebung umzusetzen.[13] Sie sind mehr als symbolische Wiederholungen der Art. 16 AEUV, Art. 8 GRCh oder „Transmissionsriemen“ zwischen diesen Bestimmungen und der Verordnung – dies belegt insbesondere die hohe Bußgeldbewehrung der Nichteinhaltung der Bestimmung.[14]

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

→ *Hauptartikel: Rechtmäßigkeit und Treu und Glauben*

Der Dreiklang Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz bedingt einander.[15]

Der **Rechtmäßigkeit**s-Grundsatz lässt sich weit und eng auslegen. Eine enge Auslegung bezieht sich auf die Zulässigkeit der Verarbeitung (Frage nach den „Ob?"), eine weitere Auslegung[16] stellt die Frage nach dem „Wie?". Die herrschende Meinung[17][18][19] legt die Vorschrift eng aus, stellt jedoch fest, dass der ErwGr. 40 in dieser Hinsicht nicht eindeutig ist.

Es ist festzustellen, dass insbesondere der Grundsatz der **Verarbeitung nach Treu und Glauben** noch weiter zu fassen ist, als in der deutschen Rechtsprechung üblich, so sprechen die anderen Sprachversionen beispielsweise von „fairness" (englisch, nicht etwa von „good faith"), „loyauté" (französisch, Anständigkeit, nicht etwa „bonne foi"), italienisch „correttezza" (italienisch, Richtigkeit, nicht etwa „buona fede") und „behoorlijkheid" (niederländisch, Angemessenheit, nicht etwa „goede trouw").[20]

Transparenz stellt hier die Umsetzung der beiden vorgenannten Grundsätze dar: Es muss einerseits retrospektiv nachvollziehbar sein, der Datenverarbeitung Schritt für Schritt zu folgen. Dies hatte bereits 1983 das Bundesverfassungsgericht im Volkszählungsurteil festgestellt.[21] Der Transparenzgedanke der Verordnung geht jedoch über diese reine Rückschau hinaus. Es muss vielmehr vorausblickend möglich sein, nicht nur den Prozess der Verarbeitung zu überblicken und verstehen, sondern auch den Zusammenhang und damit auch bspw. den Grund der Verarbeitung und den Zeitpunkt und Grund der Übermittlung an Dritte. (ErwGr. 39)

Zweckbindung

Zweckgebundene Daten und das Konzept ihrer konformen Verwendung tragen zu Transparenz, Rechtssicherheit und Vorhersehbarkeit bei, die Grundsätze zielen darauf ab, die Betroffenen zu schützen, indem sie Beschränkungen für die Verwendung ihrer Daten durch die dafür Verantwortlichen festlegen und die Angemessenheit der Verarbeitung stärken.[22] Der Grundsatz orientiert sich wie die anderen Grundsätze der Verordnung an höherrangigem Recht. Art. 8 EMRK zielt auf den Schutz des Privatlebens ab und verlangt eine Rechtfertigung für jeden Eingriff in die Privatsphäre. Entsprechend entwickelte der EGMR den „Test zur Bemessung der Erwartung an die Privatheit".[23][24] Das Gericht weitete diesen Schutz und Test, einschließlich des Schutzes personenbezogener Daten, schrittweise von Fällen der Sammlung und Archivierung personenbezogener Daten durch Geheimdienste[25][26] auf die jüngsten Fälle aus, in denen das Gericht diese Garantien auf das Arbeitsumfeld[27] und auf öffentliche Räume[28] noch vor dem Inkrafttreten der Verordnung aus der EMRK ableitete und anwandte. Entsprechend weitreichend ist der Grundsatz der Zweckbindung.

Damit die Zweckbindung überhaupt realisiert werden kann, muss der Zweck festgelegt, eindeutig und legitim sein (Artikel 5 Absatz 1 Buchstabe b). Entsprechend muss der Zweck bereits zum Zeitpunkt der Erhebung feststehen (ErwGr. 39), eine allgemeine Angabe wie „geschäftsmäßige Verarbeitung" oder „Bankgeschäfte" reichen der herrschenden Meinung nach nicht aus.[29][30][31] Vielmehr muss der Zweck „so klar zum Ausdruck gebracht werden, dass Zweifel daran, ob und in welchem Sinne der Verantwortliche der Verarbeitung den Zweck festgelegt hat, ausgeschlossen sind".[31]

Ungehemmter Austausch personenbezogener Daten in der EU

Der Austausch personenbezogener Daten in der EU darf nicht (mehr) mit dem Argument abgelehnt werden, dass der Datenschutz innerhalb der EU verschieden gehandhabt wird. Artikel 1, Absatz (3) formuliert:

> „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden."

Geltungsbereich

Die DSGVO unterscheidet (im Gegensatz etwa zum deutschen BDSG) nicht zwischen der Verarbeitung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen – für alle Verarbeiter gilt dasselbe Recht. Trotzdem fallen bestimmte Arten der Verarbeitung personenbezogener Daten laut Artikel 2 nicht unter die Verordnung. Die Erwägungsgründe (16) und (18) erläutern dies näher:

> „(16) Diese Verordnung gilt nicht für Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Verkehrs personenbezogener Daten im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, wie etwa die nationale Sicherheit betreffende Tätigkeiten."
> „(18) Diese Verordnung gilt nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Als persönliche oder familiäre Tätigkeiten könnte auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten. Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen."

Marktortprinzip

→ *Hauptartikel: Marktortprinzip*

Das europäische Datenschutzrecht gilt auch für außereuropäische Unternehmen, soweit diese ihre Waren oder Dienstleistungen im europäischen Markt anbieten. Dies bedeutet, dass die DSGVO nicht nur Anwendung findet, wenn die Datenverarbeitung im Gebiet der Union oder durch einen im Gebiet der Union ansässigen Anbieter stattfindet, sondern nach Art. 3 DSGVO auch wenn die Datenverarbeitung mit einem Angebot in Zusammenhang steht, das sich an Personen im Unionsgebiet richtet. Die genaue Bestimmung, wann ein solches Ausrichten vorliegt, ist bisher im Datenschutzrecht nicht eindeutig geklärt.

Anforderungen an eine Einwilligung

Prinzipiell sind die Anforderungen an eine wirksame Einwilligung gegenüber dem deutschen BDSG reduziert: Die Schriftform ist nicht mehr die Regel, auch eine stillschweigende Einwilligungserklärung ist nach Erwägungsgrund (32) zulässig, wenn sie eindeutig ist. Da aber andererseits dies vom Verarbeiter nachzuweisen ist, wird die Schriftform doch gängig bleiben. Für besondere personenbezogene Daten ist sie weiterhin vorgeschrieben. In der Praxis werden beispielsweise Consent-Banner verwendet.

Begrenzung der verarbeiteten Daten

Die etwa im deutschen BDSG festgeschriebene allgemeine *Datensparsamkeit* wird durch den Grundsatz der (zweckbezogenen) *Datenminimierung* ersetzt.

Transparenz

Der Erwägungsgrund (39) hebt den Grundsatz der Transparenz jeglicher Datenverarbeitung für die betroffenen Personen hervor. Mehrere Artikel verlangen entsprechende Maßnahmen:

- Nach Artikel 15 hat jede Person das Recht auf Auskunft über alle sie betreffenden Daten.
- Die Informationen darüber sind laut Artikel 12 in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu liefern.
- Nach Artikel 13 und 14 muss jeder betroffenen Person bei einer Datenerhebung in einer Datenschutzerklärung umfangreich Auskunft unter anderem über Zweck, Empfänger und Verantwortliche der Datenverarbeitung, Dauer der Datenspeicherung, Rechte zur Berichtigung, Sperren und Löschen und Verwendung der Daten für Profiling-Zwecke gegeben werden. Wenn sich der Zweck ändert, ist die betroffene Person aktiv zu informieren.
- Nach Artikel 16 hat die betroffene Person ein Recht auf Berichtigung falscher Daten sowie laut Artikel 18 ein Recht auf Einschränkung („Sperrung“) der Datenverarbeitung, wenn Richtigkeit oder Grundlage der Datenverarbeitung bestritten werden.

Die Effektivität all dieser Rechte ist allerdings von der unausgesprochenen Voraussetzung abhängig, dass betroffene Personen selbst verpflichtet sind, sich aktiv darum zu kümmern, von wem und wie ihre Daten verarbeitet werden, und ihre Rechte einzufordern. Dies wird von Kritikern als nicht realistisch angesehen.[32]

Darüber hinaus soll die DSGVO laut Erwägungsgrund (13) auch Transparenz und Rechtssicherheit für die verarbeitenden Unternehmen bewirken, „einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen“.

Recht auf Vergessenwerden

Das Recht auf Vergessenwerden, das in der Überschrift des Artikel 17 ausdrücklich so genannt wird, ist eines der zentralen Rechte der DSGVO. Es umfasst einerseits, dass eine betroffene Person das Recht hat, das Löschen aller sie betreffenden Daten zu fordern, wenn die Gründe für die Datenspeicherung entfallen. Darüber hinaus muss aber auch der Verarbeiter andererseits selbst aktiv die Daten löschen, wenn es keinen Grund mehr für eine Speicherung und Verarbeitung gibt.

Recht auf Datenübertragbarkeit

Als eine eher marktsteuernde Regelung verlangt Artikel 20, dass eine betroffene Person das Recht hat, die Daten, die sie betreffen und die sie selbst dem Verantwortlichen übergeben hat, in einem „strukturierten, gängigen und maschinenlesbaren Format zu erhalten“, auch und insbesondere für den Zweck, sie anderen „ohne Behinderung durch den Verantwortlichen“ zu übermitteln.

Sanktionen

Für die effektive Durchsetzung des Datenschutzrechts sind nun weitaus höhere Bußgelder als bisher möglich. Zudem können die Datenschutzaufsichtsbehörden künftig durchsetzbare Anordnungen und Bußgelder nicht nur gegen private Datenverarbeiter, sondern auch gegenüber Behörden erlassen, wenn das im nationalen Recht vorgesehen ist.

Die Höhe der Bußgelder für Ordnungswidrigkeiten ist nun in bestimmten Fällen nach Artikel 83 Absatz (5) auf bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Jahresumsatzes festgelegt (im Vergleich dazu sah das deutsche BDSG bisher ein maximales Bußgeld von 300.000 Euro vor).

Die Mitgliedsstaaten können darüber hinaus weitere Sanktionsmöglichkeiten vorsehen. Zum Beispiel kann laut Erwägungsgrund 149 vorgesehen werden, Gewinne aufgrund des Verstoßes gegen die DSGVO einzuziehen.

Privacy by Design, Privacy by Default

Nach den Grundsätzen Datenschutz durch Technikgestaltung („privacy by design“, „data protection by design“) und durch datenschutzfreundliche Voreinstellungen („privacy by default“, „data protection by default“) muss die betroffene Person darauf vertrauen können, dass die grundsätzlichen Datenschutzanforderungen von der ersten Nutzung an gewahrt bleiben, und zwar auch dann, wenn die vorgegebenen Werkseinstellungen zunächst nicht geändert werden.[33] Die Konzepte gehören zu den Kernelementen der Verordnung.[34]

Durch den Grundsatz „**privacy by design**“ wird dem Rechnung getragen, dass die Sicherstellung des Datenschutzes nicht allein durch die Einhaltung von Vorschriften gewährleistet werden kann; die Grundsätze des Datenschutzes müssen bereits vor Beginn der technischen Planung in die Konzeptionierung von Verarbeitungsvorgängen integriert werden.[35][36] Daher ergeben sich drei Handlungsfelder für „Datenschutz durch Technikgestaltung“[37][38]:

1. Technik von Verarbeitungsvorgängen, z. B. durch das Softwaredesign: Was technisch verhindert wird oder unterbunden werden kann oder technisch nicht möglich ist, muss nicht mehr verboten und überwacht werden,[39]
2. Geschäftsabläufe, z. B. durch „Funktionstrennung“: Falls Daten lediglich verarbeitet werden, daraus Trends und Zusammenhänge zu erkennen und keine gewonnenen Informationen auf die betreffenden Personen unmittelbar anzuwenden. Vielmehr sollen diese durch technische und organisatorische Maßnahmen frühestmöglich anonymisiert werden,[40]
3. Gestaltung datenschutzfreundlicher Architektur, sowohl physisch (z. B. durch das Vermeiden von personenbezogenen Daten auf Ordnerrücken) als auch elektronisch.[41]

Beim Grundsatz „**privacy by default**“ handelt es sich um eine Spezialisierung des Grundsatzes „privacy by design“.[42][43] Er fußt insbesondere auf dem „Privacy Paradox“,[44][45][46] wonach Benutzer erklären, dass sie sich um ihre Daten und den Datenschutz sorgen, jedoch so handeln, als ob dies nicht der Fall wäre. Die Gründe hierfür sind Gegenstand der Forschung; angenommen werden Faulheit, Unkenntnis oder eine intuitive, irrationale Abwägung der Vor- und Nachteile.[47] Ziel ist, dass Verantwortliche Systeme bereitstellen, deren Werkseinstellungen bereits möglichst datenschutzfreundlich sind.[48] Benutzer eines Systems sollen hierbei jedoch explizit nicht davor geschützt werden,

freiwillig und informiert datenschutzunfreundlichere Einstellungen vorzunehmen, vielmehr sollen betroffene Personen befähigt werden, die Verarbeitung personenbezogener Daten zu überwachen (ErwG 78).

Die Umsetzung der Grundsätze erfolgt durch „geeignete technische und organisatorische Maßnahmen“ (Art. 25 Absatz 1). Unter technischen Maßnahmen sind alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind oder die in Soft- und Hardware umgesetzt werden, unter organisatorischen Maßnahmen solche Schutzversuche, die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden.[49] Hierzu können beispielsweise das physikalische Löschen von Daten[50], die kryptographische Verschlüsselung oder interne IT- und Datenschutz-Regelungen gehören.[51][52]

Verpflichtung zur Bestellung betrieblicher und behördlicher Datenschutzbeauftragter, Vertreter in der Europäischen Union

Die DSGVO sieht nun europaweit die Bestellung von Datenschutzbeauftragten vor, zumindest bei allen öffentlichen Stellen und solchen privaten Unternehmen, bei denen besonders risikoreiche Datenverarbeitungen erfolgen. Damit wird ein Mindeststandard für die Einrichtung dieser Stellen erreicht.

Kleinunternehmer und kleine Unternehmen müssen keinen Datenschutzbeauftragten stellen, es sei denn, einer der nachfolgenden Punkte trifft zu.[53]

- Es sind regelmäßig mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 Satz 1 BDSG(neu)).
- Verantwortlicher ist eine öffentliche Stelle oder Behörde (Art. 37 Abs. 1 lit. a DSGVO).
- Die Kerntätigkeit umfasst die umfangreiche Verarbeitung besonderer Kategorien von Daten oder strafrechtlicher Verurteilungen (Art. 37 Abs. 1 lit. c DSGVO).
- Es ist eine Datenschutz-Folgenabschätzung durchzuführen (§ 38 Abs. 1 Satz 2 BDSG(neu)).
- Die Kerntätigkeit ist die umfangreiche oder systematische Überwachung von betroffenen Personen (Art. 37 Abs. 1 lit. c DSGVO).

Der Begriff der „umfangreichen Verarbeitung“ und die Voraussetzungen für eine Datenschutz-Folgenabschätzung werden im Erwägungsgrund 91 etwas genauer beschrieben, damit bestimmte freie Berufe wie Rechtsanwälte und Ärzte, aber etwa auch Apotheker (als „Angehörige eines Gesundheitsberufes“) in der Regel keinen Datenschutzbeauftragten stellen müssen.

Nicht in der Europäischen Union ansässige Verantwortliche, auf die die Datenschutz-Grundverordnung Anwendung findet, müssen zudem einen Vertreter in der Europäischen Union bestellen.

Öffnungsklauseln

Die DSGVO sieht vor, dass durch nationales Recht an vielen Stellen eine Erweiterung oder detaillierte Festlegung des Datenschutzrechtes erfolgt. Dies erfolgt über so genannte „Öffnungsklauseln“, von denen die DSGVO – je nach Zählweise – 50 bis 60 enthält. Einige verlangen eine Rechtshandlung der Mitgliedsstaaten, die Mehrzahl erlaubt jedoch die Ausnutzung von Spielräumen durch nationale Vorschriften. Der Handlungsspielraum ist

grundsätzlich insofern begrenzt, als dass die Harmonisierung des Datenschutzes durch die DSGVO nicht unterlaufen werden darf.

Ein Beispiel für eine Öffnungsklausel findet sich etwa im Datenschutz von Beschäftigten: Artikel 88 Abs. 1 sieht eine Öffnungsklausel vor, nach der die Mitgliedsstaaten „spezifischere Vorschriften zur Gewährleistung der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext“ vorsehen können. Es ist umstritten, ob diese Formulierung ein Abweichen vom Schutzniveau der allgemeinen Vorschriften zulässt.[54]

Weitere Öffnungsklauseln finden sich u. a.

- in Artikel 9 Abs. 2 und Abs. 4 zur Festlegung besonderer Bedingungen für die Verarbeitung besonderer Arten personenbezogener Daten, wie Gesundheitsdaten oder Daten zu sexuellen Vorlieben;
- in Artikel 10 zur Erlaubnis der Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten;
- in Artikel 28 für rechtliche Grundlagen der Auftragsdatenverarbeitung;
- in Artikel 37 zur Bestellung von Datenschutzbeauftragten, abweichend von den in Artikel 37 festgelegten Voraussetzungen;
- in Artikel 85 zum Ausgleich des Spannungsfelds zwischen Datenschutz und Meinungsfreiheit oder der Regelung eines Presseprivilegs;
- in Artikel 87 für die Regelung der Verarbeitung nationaler Kennziffern oder anderer Kennzeichen von allgemeiner Bedeutung;
- in Artikel 89 für die Regelung von Ausnahmen von Betroffenenrechten bei Verarbeitungen für wissenschaftliche, historische, statistische oder archivarische Zwecke;

Debatte über die DSGVO

Seit dem Vorschlag des Gesetzgebungsentwurfs der Europäischen Kommission hatte es umfassende Debatten im Rahmen des Gesetzgebungsverfahrens gegeben. Insbesondere das Europäische Parlament hatte durch zahlreiche öffentliche Anhörungen viele der geäußerten Kritikpunkte aufgegriffen und im Rahmen des von Jan Philipp Albrecht als Berichterstatter verhandelten Kompromisses einfließen lassen. Auch im Ministerrat waren unterschiedlichste Standpunkte eingeflossen. Aus beiden Vorlagen wurde im Rahmen der Trilogverhandlungen am 15. Dezember 2015 ein finaler Verordnungstext erarbeitet, der am Ende nahezu einstimmig vom Plenum des Europäischen Parlaments sowie den Innen- und Justizministern der EU-Mitgliedstaaten angenommen wurde und zum 25. Mai 2016 formal in Kraft trat. Die während der mehr als vier Jahre dauernden Verhandlungen aufgeworfenen Kritikpunkte unterschiedlicher Seiten der Debatte werden nachstehend ausschnittsweise zusammengefasst:

Debatte über Entwürfe

Zwischenzeitliche Entwürfe sahen vor, dass ein interner Datenschutzbeauftragter und interne Dokumentationspflichten nur für Unternehmen mit mehr als 250 Mitarbeitern verpflichtend sind. Dies – so Kritiker – hätte den Datenschutz in Deutschland und Österreich geschwächt.[55] Die endgültige Fassung sieht eine verpflichtende Benennung des internen Datenschutzbeauftragten bei Behörden und bei Verantwortlichen vor, deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen oder in der umfangreichen Verarbeitung sensibler Daten besteht (Art. 37 Abs. 1). Die Mitgliedstaaten sind aber befugt, strengere

Regelungen zu erlassen (Art. 37 Abs. 4). Die internen Dokumentationspflichten gelten nicht für Unternehmen mit weniger als 250 Mitarbeitern, sofern die Datenverarbeitung kein Risiko für die Betroffenen birgt, nur gelegentlich erfolgt und nicht die Verarbeitung sensibler Daten einschließt (Art. 30 Abs. 5).

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) erwartet, dass die Abschaffung des internen Datenschutzbeauftragten zu Kostensteigerungen aufgrund wachsender Bürokratie führe. Unternehmen müssten intern eine Stelle für die Behördenkommunikation einrichten und bei der Einführung neuer Software mit Verzögerungen rechnen, weil die Landesämter für Datenschutz personell nicht gut genug ausgestattet seien. 66 unabhängige Verbraucher- und Datenschutzorganisationen forderten Jean-Claude Juncker im April 2015 auf, den „*Goldstandard* des europäischen Datenschutzes“ zu erhalten.[56]

Der BvD bemängelte ferner fehlende klare Regeln für den Datentransfer aus der EU in Drittstaaten (z. B. USA) und forderte eine EU-weite Bestellung betrieblicher Datenschutzbeauftragter.[57]

Andererseits wird die Weitergabe von Verbraucherdaten an Konkurrenten (Datenportabilität) nicht nur Anbieter wie Facebook betreffen, sondern auch für kleinere Unternehmen gelten.[55]

Der deutsche Bundesrat erhob am 30. März 2012 Subsidiaritätsrüge gegen den Verordnungsvorschlag. Die Länderkammer war der Auffassung, dass der Vorschlag mit dem Subsidiaritätsprinzip nicht im Einklang stehe und deshalb gegen Art. 5 Abs. 3 EUV verstoße.[58] Nach dieser Vorschrift darf die Europäische Union in den Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, nur tätig werden, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern wegen ihres Umfangs oder ihrer Wirkungen auf EU-Ebene besser zu implementieren sind.

Von vielen Seiten wurde die oft vage und unklare Formulierung des Entwurfs kritisiert. Danach sollten auch viele elementare Regelungen erst gar nicht in die Grundverordnung eingefügt, sondern diesen erst durch gesonderte Rechtsakte der EU-Kommission Geltung verschafft werden.

Im Verhandlungsbeschluss des Europäischen Parlaments waren die Kritikpunkte bereits weitgehend ausgeräumt.[59] Nachdem aber die ursprünglich angenommenen Datenschutzaspekte der Verordnung nach einem Pressebericht vom März 2015 von der zuständigen Arbeitsgruppe der EU in großen Teilen aufgeweicht wurden, kam es zu erneuter Kritik. So wird in einem Positionspapier der Arbeitsgruppe der Industrie das Sammeln von personenbezogenen Daten ohne festgelegte Zwecke erlaubt, ebenso wie die Weitergabe dieser Daten an Dritte.[60]

Kritik am endgültigen Verordnungstext

Auch nach Verabschiedung der Datenschutz-Grundverordnung wird grundlegende Kritik, insbesondere von Seiten der Rechtswissenschaft geübt:

So bezeichnete der Leiter des Instituts für Informations-, Telekommunikations- und Medienrecht an der Universität Münster, Thomas Hoeren, die Datenschutz-Grundverordnung als „eines der schlechtesten Gesetze des 21. Jahrhunderts“.[61]

Der Leiter des Fachgebiets Öffentliches Recht mit Schwerpunkt Recht der Technik der Universität Kassel, Alexander Roßnagel, meinte, die Datenschutz-Grundverordnung ignoriere „alle modernen Herausforderungen für den Datenschutz wie Soziale Netzwerke, Big Data (Datenflut und deren Beherrschung), Suchmaschinen, Cloud Computing, Ubiquitous computing (Durchdringung des Alltags und von Dingen durch Computer) und andere Technikanwendungen“.[62] In einer Studie wird der deutsche Gesetzgeber aufgefordert, die unübersichtliche Gemengelage aus neuen europäischen Regelungen und weitergeltendem deutschem Recht aufzulösen.[63]

Auch der Deutsche Anwaltverein (DAV) sieht bei der DSGVO insoweit Änderungsbedarf, als der nationale Gesetzgeber zum Schutz der berufsspezifischen Rechte und Pflichten der Rechtsanwälte (z. B.: Unabhängigkeit vor staatlichen Einflüssen, Anwaltsgeheimnis, absolute Treuepflicht des Rechtsanwalts gegenüber seinem Mandanten) in der Verordnung ermöglichte Öffnungsklauseln nutzen muss, um all dies überhaupt weiter gewährleisten zu können.[64] Der DAV zog das Fazit einer „Ausdünnung des deutschen Datenschutzrechts“.[65]

Die Forderung des DAV an den nationalen Gesetzgeber geht in drei Richtungen:

- Keine Zugangsbefugnisse der Datenschutz-Aufsichtsbehörden ohne ausdrückliche vorherige Zustimmung der Anwaltskammer.[66]
- Generelle und umfassende Erlaubnisklausel für anwaltliche Datenverarbeitung von personenbezogenen Daten im Rahmen der Mandate.[67]
- Einschränkung der Auskunftspflichten und Auskunftsrechte.[68]

Richard David Precht nannte die Verordnung im Zusammenhang mit Datenschutz einen „sperrigen Versuch, mal so'n Lattenzaun zu bauen“ [69]

Lobbyarbeit

Rund um die Verhandlungen der Datenschutz-Grundverordnung kritisierten EU-Abgeordnete massives Lobbying von Seiten der US-Regierung und von US-amerikanischen IT-Unternehmen. Technologie-Unternehmen aus den USA fürchten demnach den negativen Einfluss der Verordnung auf ihre Niederlassungen in Europa und übten entsprechenden Druck auf die Regierung von US-Präsident Obama aus. So forderte der amerikanische EU-Botschafter William E. Kennard in einer Rede in Brüssel am 4. Dezember 2012, dass die zentralen Forderungen der Verordnung gestrichen werden müssen: das Löschen sämtlicher Daten einer Person aus den Unternehmensdatenbanken auf Wunsch und die ausdrückliche Einverständniserklärung einer Person, bevor ihre Daten überhaupt gesammelt werden dürfen.[70]

Von amerikanischen Unternehmen wird ein *California-Effekt* durch die EU-Gesetzgebung befürchtet. Ähnlich wie strengere Umweltgesetze in Kalifornien den Mindeststandard in den USA schleichend anheben, wird erwartet, dass die höheren Standards in der EU das Datenschutzniveau für alle weltweit operierenden Unternehmen anheben würden. Während bisher in den USA lediglich Finanz- und Gesundheitsdaten einem gewissen Datenschutz unterliegen,[70] ist die Erfassung und das Zusammenführen sämtlicher anderer gesammelter Daten und deren unbegrenzte Aufbewahrung durch Privatunternehmen erlaubt. Amerikanische Bürgerrechtsorganisationen erhofften sich andererseits eine Steigerung des Datenschutzstandards in den USA und unterstützten daher die Pläne in der EU.

Die Plattform LobbyPlag.eu zeigt, dass viele Abänderungsanträge von Abgeordneten im EU-Parlament wortgleich aus Lobbypapieren von Unternehmen wie Amazon, eBay, der Lobbygruppe „Digitaleurope“[70] mit den Mitgliedern Apple, Microsoft, Cisco, Intel, IBM, Oracle, Texas Instruments und Dell oder von der US-amerikanischen Handelskammer übernommen wurden. Unter anderem waren dies die Abgeordneten Malcolm Harbour (ECR), Andreas Schwab (CDU/EPP), Klaus-Heiner Lehne (EPP) oder Marielle Gallo (EPP). Andererseits weist die Plattform auch auf wortgleiche Übernahmen aus den Unterlagen von Datenschutzorganisationen wie Bits of Freedom und EDRi durch Abgeordnete wie Amelia Andersdotter (PPEU/Piraten) oder Eva Lichtenberger (EFA/Die Grünen) hin.[71]

Im zuständigen LIBE-Ausschuss des EU-Parlaments wurden schlussendlich über 3.100 Abänderungsanträge gegenüber dem Entwurf der EU-Kommission eingebracht. Generell setzten sich die meisten sozialdemokratischen und grünen Abgeordneten für eine Verstärkung oder Präzisierung des Entwurfs ein, während sich die meisten konservativen und liberalen Abgeordneten für eine Lockerung im Sinne der IT-Wirtschaft stark machten.

LobbyPlag erarbeitete eine Liste der Abgeordneten, die, gemessen an den von ihnen eingebrachten Änderungsanträgen, am nachdrücklichsten für weniger bzw. für mehr Datenschutz eintraten. Bis Anfang Juni 2013 brachte sich für die Aufweichung des Datenschutzes demnach Axel Voss (EPP/CDU) am stärksten ein, bei der Stärkung des Datenschutzes sah man Jan Philipp Albrecht (EFA/Die Grünen) an erster Stelle. Beide hatten in der Summe je 147 Änderungsanträge zugunsten der Abschwächung beziehungsweise Stärkung des Datenschutzes eingebracht.[72]

Unter Druck durch Teile der deutschen Wirtschaft, die fürchtete, im globalen Wettbewerb Nachteile durch die Grundverordnung zu erleiden, argumentierten auch Vertreter des Deutschen Innenministeriums, dass das Recht auf informationelle Selbstbestimmung einem harmonisierten Wettbewerb entgegenstünde.[73]

Verfahren

Nach langen Verhandlungen scheiterte ein Entwurf der irischen Ratspräsidentschaft im Juni 2013 im EU-Ministerrat. Unter anderem meldeten die Vertreter Deutschlands, Großbritanniens und Frankreichs zahlreiche Bedenken an. Die anvisierte Positionierung vor der Sommerpause konnten damit sowohl Rat als auch Parlament nicht leisten. Am 21. Oktober 2013 nahm das Europäische Parlament im Innen- und Justizausschuss seine durch den Grünen-Europaabgeordneten Jan Philipp Albrecht als EP-Berichterstatter ausgearbeitete Verhandlungsposition mit überwältigender Mehrheit an[74] und bestätigte sie am 12. März 2014 durch das Plenum.[75]

Nachdem im Rat entscheidende Teile der Verordnung unter Ausschluss der Öffentlichkeit zu Gunsten eines schwächeren Datenschutzes verändert worden waren, sollten am 12. und 13. März 2015 die Justizminister der Mitgliedstaaten eine Einigung zum zweiten Kapitel der Verordnung erzielen, bevor die übrigen Kapitel verhandelt wurden.[60] Erst im Juni 2015 einigten sich die EU-Justizminister auf einen Entwurf der EU-Datenschutz-Grundverordnung.[76]

Am 24. Juni begannen die Abstimmungsverhandlungen zwischen Rat, Europäischem Parlament und Europäischer Kommission (sogenannter Trilog). Eine am 15. Dezember 2015 zwischen Parlament und Rat informell erzielte Einigung[77] wurde am 17. Dezember vom Innen- und Rechtsausschuss des Parlaments mit großer Mehrheit angenommen. Am 8. April

2016 beschloss der EU-Ministerrat die vorliegende Fassung[78][79]; das EU-Parlament nahm die Regelungen am 14. April ebenfalls an.[80]

Die Veröffentlichung im Amtsblatt der Europäischen Union erfolgte am 4. Mai 2016,[81] weshalb sie gemäß Art. 99 Abs. 1 DSGVO am 24. Mai 2016 in Kraft trat und gemäß Art. 99 Abs. 2 ab dem 25. Mai 2018 anzuwenden ist. Ein Corrigendum (d. h. ein Beschluss zur Korrektur inhaltlicher Fehler) erging – beschränkt auf einige Sprachfassungen der DS-GVO (DE, ET, IT, HU) – am 27. Oktober 2016.[82]

Befürchtung der Schwächung durch das TiSA-Abkommen

Unterlagen aus den Geheimverhandlungen zum Trade in Services Agreement (TiSA), die im November 2016 Greenpeace zugespielt wurden, belegen nach Aussage von Greenpeace, dass Lobbyisten versuchen, neben Netzneutralität und Bankenregulierung auch den Datenschutz nachhaltig zu schwächen und die Datenschutz-Grundverordnung faktisch unwirksam zu machen. Unternehmen sollen Kunden- und Nutzerdaten ins außereuropäische Ausland transferieren und dort ohne Zweckbindung weiterverarbeiten können.[83]

Anpassung des Datenschutzrechts der EU-Mitgliedsstaaten

Angaben gemäß DSGVO an einer Überwachungskamera im öffentlichen Raum in Hamburg

Deutschland

Mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU vom 30. Juni 2017 wurde unter anderem das Bundesdatenschutzgesetz neu gefasst.[4]

Umsetzung und weltweite Folgeerscheinungen

Die Umsetzung der umfassenden Änderungen durch die Datenschutzgrundverordnung dauert bis heute noch immer an, obwohl die DS-GVO bereits seit 25. Mai 2018 gilt.[88][89][90] Für

2020 ist von der EU Kommission auch die Evaluierung der DS-GVO geplant (Art. 97 Abs. 1 DS-GVO).

Einige große US-Medienverlage wie die der Chicago Tribune oder die Los Angeles Times, so wurde bekannt, haben ihre Internetpräsenzen teilweise für viele europäische Nutzer gesperrt. Zu groß war offenbar die Befürchtung, für mögliche Datenschutzverstöße sanktioniert zu werden.[91][92] In Österreich hat die Immobilienverwaltung der Stadt Wien, Stadt Wien – Wiener Wohnen, angekündigt, rund 200.000 Namensschilder an Klingeln zu entfernen, da sie befürchtet, gegen die DSGVO zu verstoßen.[93] Diese Ankündigung wurde im November 2018 wieder zurückgezogen.

In Deutschland wurden bis Ende 2018 in 41 Fällen Bußgeldbescheide aufgrund von Datenschutzverstößen erlassen, davon alleine 33 in Nordrhein-Westfalen. Die Bußgelder bewegen sich in niedriger Höhe, in Nordrhein-Westfalen waren es insgesamt 15.000 Euro, in Baden-Württemberg allerdings bei einer Einzelstrafe 80.000 Euro.[94]

Di französische Datenschutzbehörde CNIL verhängte im Januar 2019 nach Beschwerden der Nichtregierungsorganisationen La Quadrature du Net aus Frankreich und NOYB aus Öseterreich ein Bußgeld über 50 Millionen Euro gegen Google LLC wegen mangelnder Transparenz bei den Informationen zur Verwendung der erhobenen Daten[95] und zum Speicherzeitraum[96] und weil die von Google eingeholte Einwilligung zur Anzeige personalisierter Werbung ungültig sei.[97]

Einzelnachweise

1. ↑ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates. In: ABL. L 119/89 vom 4. Mai 2016.
2. ↑ *Umsetzung der JI-Richtlinie in Deutschland* Website des Bundesdatenschutzbeauftragten, abgerufen am 10. Juni 2018
3. ↑ Jürgen Kühling, Mario Martini et al.: Die Datenschutz-Grundverordnung und das nationale Recht – Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster 2016, S. 1.
4. ↑ Hochspringen nach: a b c Vorgangsablauf im DIP und Text des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU – DSAnpUG-EU (BGBl. 2017 I S. 2097)
5. ↑ Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI): *Stellungnahme zum Entwurf eines Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU – DSAnpUG-EU.* netzpolitik.org, 31. August 2016, abgerufen am 1. Februar 2017 (PDF).
6. ↑ Bundesministerium des Innern: *Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU).* netzpolitik.org, 31. August 2016, abgerufen am 1. Februar 2017 (PDF).
7. ↑ *Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern.* In: *europa.eu.* Europöische Kommission, 25. Januar 2012, abgerufen am 2. Januar 2019 (deutsch, englisch, französisch, dänisch, spanisch, niederländisch,

italienisch, schwedisch, portugiesisch, finnisch, griechisch, tschechisch, estnisch, ungarisch, litauisch, lettisch, maltesisch, polnisch, slowakisch, slowenisch, bulgarisch, rumänisch).

8. ↑ Falk Lüke: *Reding stellt EU-Datenschutzreform vor.* In: *heise online*. Heise Medien GmbH & Co. KG, 25. Januar 2012, abgerufen am 2. Januar 2019.
9. ↑ *Was muss ich wissen zur EU-Datenschutz Grundverordnung?* Bitkom, 2016, S. 5, abgerufen am 2. Dezember 2017 (PDF; 234 kB).
10. ↑ Wissenschaftliche Dienste des Deutschen Bundestages - Fachbereich: PE 6: Fachbereich Europa: *Vorgaben der Verordnung (EU) Nr. 995/2010 - Auslegungsgrundsätze des EuGH*. Hrsg.: Deutschen Bundestag. PE 6 - 3000 - 83/16, 15. Juni 2016, S. 4, Abschnitt 2.1. Erwägungsgründe und Bestimmungen eines Rechtsakts (Satz 2) (bundestag.de [PDF; abgerufen am 2. Januar 2019]): „Der EuGH vertritt in ständiger Rechtsprechung die Ansicht, dass „[…] die Begründungserwägungen eines Gemeinschaftsrechtsakts rechtlich nicht verbindlich sind und weder herangezogen werden können, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen, noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht.““
11. ↑ Peter Gola, Andreas Jaspers et al.: *Datenschutzgrundverordnung im Überblick.* DATAKONTEXT: München 2016. ISBN 978-3-89577-774-5, S. 22.
12. ↑ Information Commissioner's Office: *The principles.* In: *Guide to the General Data Protection Regulation.* Abgerufen am 26. Juni 2018 (englisch): „The principles lie at the heart of the GDPR. They are set out right at the start of the legislation, and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime – and as such there are very limited exceptions.“
13. ↑ EuGH: *Urteil in der Rechtssache C-131/12.* (ECLI:EU:C:2014:317). 13. Mai 2014, abgerufen am 26. Juni 2018 (Rn. 71): „Jede Verarbeitung personenbezogener Daten muss – vorbehaltlich der in Art. 13 der Richtlinie 95/46 zugelassenen Ausnahmen – den in Art. 6 der Richtlinie aufgestellten Grundsätzen in Bezug auf die Qualität der Daten und einem der in Art. 7 der Richtlinie aufgeführten Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten genügen (vgl. Urteile Österreichischer Rundfunk u. a., EU:C:2003:294, Rn. 65; ASNEF und FECEMD, C-468/10 und C-469/10, EU:C:2011:777, Rn. 26, und Worten, C-342/12, EU:C:2013:355, Rn. 33).“
14. ↑ Eike Michael Frenzel: *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. Kommentar. Hrsg.: Boris Paal, Daniel Pauly. 2. Auflage. C.H. Beck, München 2018, ISBN 978-3-406-71838-0, Art 5 Rn. 2.
15. ↑ EuGH: *Urteil in der Rechtssache C-201/14.* (ECLI:EU:C:2015:638). 1. Oktober 2015, abgerufen am 26. Juni 2018 (Rn. 34): „Folglich verpflichtet das in Art. 6 der Richtlinie 95/46 vorgesehene Erfordernis der Verarbeitung personenbezogener Daten nach Treu und Glauben eine Verwaltungsbehörde, die betroffenen Personen davon zu unterrichten, dass die personenbezogenen Daten an eine andere Verwaltungsbehörde weitergeleitet werden, um von dieser in ihrer Eigenschaft als deren Empfänger verarbeitet zu werden.“
16. ↑ Philipp Reimer: *Europäische Datenschutzgrundverordnung*. Handkommentar. Hrsg.: Gernot Sydow. Nomos, Baden-Baden 2017, ISBN 978-3-8487-1782-8, Art. 5 Rn. 1.
17. ↑ Eike Michael Frenzel: *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. Kommentar. Hrsg.: Boris Paal, Daniel Pauly. 2. Auflage. C.H. Beck, München 2018, ISBN 978-3-406-71838-0, Art 5 Rn. 16.

18. ↑ Tobias Herbst: *Datenschutz-Grundverordnung/BDSG*. Kommentar. Hrsg.: Jürgen Kühling, Benedikt Buchner. C.H. Beck, München 2018, ISBN 978-3-406-71932-5, Art. 5 Rn. 10f.
19. ↑ Information Commissioner's Office: *Lawful basis for processing.* In: *Guide to the General Data Protection Regulation.* Abgerufen am 26. Juni 2018 (englisch): „The first principle requires that you process all personal data lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful basis under Article 6. And to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful basis applies."
20. ↑ Übersetzungszentrum für die Einrichtungen der Europäischen Union: *Grundsatz von Treu und Glauben.* IATE ID: 1087248. Abgerufen am 2. Januar 2019 (englisch, französisch, italienisch, niederländisch).
21. ↑ Bundesverfassungsgericht: *Urteil vom 15. Dezember 1983.* Az. 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 484/83. S. 46, archiviert vom Original am 7. März 2010; abgerufen am 26. Juni 2018 (pdf): „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."
22. ↑ Artikel-29-Datenschutzgruppe: *Opinion 03/2013 on purpose limitation.* Workingpaper 203. Europäischen Kommission, 2. April 2013, abgerufen am 26. Juni 2018 (pdf, englisch): „Purpose specification and the concept of compatible use contribute to transparency, legal certainty and predictability; they aim to protect the data subject by setting limits on how controllers are able to use their data and reinforce the fairness of the processing."
23. ↑ EGMR: *Urteil in der Beschwerdesache 12433/86.* Lüdi ./. Schweiz. In: *Human Rights Documentation*. Europarat, 15. Juni 1992, abgerufen am 26. Juni 2018 (englisch, französisch, bulgarisch, russisch, slowenisch, spanisch).
24. ↑ EGMR: *Urteil in der Beschwerdesache 20605/92.* Halford ./. Vereinigtes Königreich. In: *Human Rights Documentation*. Europarat, 4. Mai 2000, abgerufen am 26. Juni 2018 (englisch, französisch, armenisch, lettisch, slowakisch, slowenisch, spanisch).
25. ↑ EGMR: *Urteil in der Beschwerdesache 27798/95.* Amann ./. Schweiz. In: *Human Rights Documentation*. Europarat, 16. Februar 2000, abgerufen am 26. Juni 2018 (englisch, französisch, spanisch).
26. ↑ EGMR: *Urteil in der Beschwerdesache 28341/95.* Rotaru ./. Rumänien. In: *Human Rights Documentation*. Europarat, 25. Juni 1997, abgerufen am 26. Juni 2018 (englisch, französisch, aserbaidschanisch, mazedonisch, rumänisch, serbisch, spanisch).
27. ↑ EGMR: *Urteil in der Beschwerdesache 62617/00.* Copland ./. Vereinigtes Königreich. In: *Human Rights Documentation*. Europarat, 3. April 2007, abgerufen am 26. Juni 2018 (englisch, französisch, albanisch, armenisch, aserbaidschanisch, bosnisch, bulgarisch, georgisch, isländisch, mazedonisch, rumänisch, russisch, spanisch, türkisch, ukrainisch).
28. ↑ EGMR: *Urteil in der Beschwerdesache 4158/05.* Gillan und Quinton ./. Vereinigtes Königreich. In: *Human Rights Documentation*. Europarat, 12. Januar 2010, abgerufen am 26. Juni 2018 (englisch, französisch, deutsch, albanisch, armenisch, aserbaidschanisch, bosnisch, bulgarisch, kroatisch, georgisch, isländisch, mazedonisch, rumänisch, russisch, spanisch, türkisch, ukrainisch).
29. ↑ Ulf Brühann: *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. In: Eberhard Grabitz, Meinhard Hilf, Martin Nettesheim (Hrsg.): *Das Recht der Europäischen*

Union. Kommentar. 40. Auflage. Beck, München 2010, ISBN 978-3-406-60907-7, Abschnitt A 30, Art. 6 Rn 9.
30. ↑ Eike Michael Frenzel: *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. Kommentar. Hrsg.: Boris Paal, Daniel Pauly. 2. Auflage. C.H. Beck, München 2018, ISBN 978-3-406-71838-0, Art 5 Rn. 27.
31. ↑ Hochspringen nach: a b Ulrich Dammann, Spiros Simitis: *EG-Datenschutzrichtlinie*. Kommentar. Nomos, Baden-Baden 1997, ISBN 978-3-7890-4517-2, Artikel 6 Rn. 6.
32. ↑ Peter Gola, Andreas Jaspers et al.: *Datenschutzgrundverordnung im Überblick.* DATAKONTEXT: München 2016. ISBN 978-3-89577-774-5, S. 18: „Da Betroffene – wie durch Meinungsumfragen umfassend belegt – derartige Datenschutzklauseln überwiegend nicht lesen und diese Leseabneigung mit steigendem Umfang des Texts nicht nachlassen wird, …“
33. ↑ Dennis-Kenji Kipker: *Privacy by Default und Privacy by Design*. Band 39, Nr. 6, Mai 2015, S. 410, doi:10.1007/s11623-015-0438-0.
34. ↑ Mario Martini: *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. Kommentar. Hrsg.: Boris Paal, Daniel Pauly. 2. Auflage. C.H. Beck, München 2018, ISBN 978-3-406-71838-0, Art 25 Rn. 8.
35. ↑ Ann Cavoukian: *Privacy Design Principles for an Integrated Justice System.* Working Paper. Information and Privacy Commissioner of Ontario, 5. April 2000, archiviert vom Original am 25. Februar 2008; abgerufen am 24. Juni 2018 (pdf, englisch): „Privacy design principles need to be built into the technology architecture at the outset of the technology initiative. For privacy design principles to be useful, beyond general discussion and agreement in the planning stage, however, they need additional specificity.“
36. ↑ Konferenz der Datenschutzbeauftragten des Bundes und der Länder: *Ein modernes Datenschutzrecht für das 21. Jahrhundert.* Eckpunkte. Landesbeauftragter für den Datenschutz Baden-Württemberg, 18. März 2010, S. 7, abgerufen am 24. Juni 2018 (pdf): „Die technische Integration des Datenschutzes in Produkte und Verfahren, z. B. im Hinblick auf Datenvermeidung oder Datensparsamkeit sowie einfachen und wirkungsvollen Selbstdatenschutz der Nutzerinnen und Nutzer, würde dagegen spätere Datenschutzprobleme vermeiden helfen.“
37. ↑ Ann Cavoukian: *Privacy by Design.* Information and Privacy Commissioner of Ontario, Januar 2009, archiviert vom Original am 6. Februar 2009; abgerufen am 24. Juni 2018 (pdf, englisch): „In brief, Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. […] This approach originally had technology as its primary area of application, but I have since expanded its scope to two other areas. In total, the three areas of application are: (1) technology; (2) business practices; and (3) physical design.“
38. ↑ Ann Cavoukian: *Privacy by Design.* The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Information and Privacy Commissioner of Ontario, Mai 2010, archiviert vom Original am 27. Mai 2010; abgerufen am 24. Juni 2018 (pdf, englisch).
39. ↑ Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka: *Modernisierung des Datenschutzrechts*. Gutachten. Hrsg.: Bundesministerium des Innern. Berlin September 2001, DNB 963524534, S. 35 unten (semanticscholar.org [PDF; abgerufen am 24. Juni 2018]).
40. ↑ Giovanni Buttarelli: *Bewältigung der Herausforderungen in Verbindung mit Big Data: Ein Ruf nach Transparenz, Benutzerkontrolle, eingebautem Datenschutz und Rechenschaftspflicht.* Stellungnahme 7/2015. Europäischer Datenschutzbeauftragter, 19. November 2015, S. 17f, abgerufen am 24. Juni 2018.

41. ↑ Wilhelm Steinmüller, Leonhard Ermer, Wolfgang Schimmel: *Datenschutz bei riskanten Systemen: Eine Konzeption entwickelt am Beispiel eines medizinischen Informationssystems* (= *Informatik-Fachberichte*. Band 13). Springer-Verlag, Berlin / Heidelberg 1978, ISBN 978-3-540-08684-0, doi:10.1007/978-3-642-48218-2.
42. ↑ Marit Hansen: *Data Protection by Default in Identity-Related Applications*. In: Simone Fischer-Hübner, Elisabeth de Leeuw, Chris Mitchell (Hrsg.): *Policies and Research in Identity Management*. Third IFIP WG 11.6 Working Conference (= *IFIP Advances in Information and Communication Technology*. Band 396). Springer, Heidelberg / Berlin 2013, ISBN 978-3-642-37281-0, doi:10.1007/978-3-642-37282-7_2 (englisch, inria.fr [PDF]).
43. ↑ Artikel-29-Datenschutzgruppe – Arbeitsgruppe Polizei und Justiz: *Die Zukunft des Datenschutzes: Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten.* Workingpaper 168. Europäischen Kommission, 1. Dezember 2009, S. 15f, abgerufen am 24. Juni 2018 (pdf): „Die Anwendung eines solchen Grundsatzes [“Privacy by Design”] würde die Notwendigkeit für den Einsatz von Technologien zum Schutz der Privatsphäre (PET), von “Privacy by Default”-Voreinstellungen und der erforderlichen Tools unterstreichen, die die Nutzer dazu befähigen, ihre personenbezogenen Daten besser zu schützen (z. B. Zugangskontrollen, Verschlüsselung).“
44. ↑ John Schwartz: *'Opting In': A Privacy Paradox.* In: *The Washington Post.* Nash Holdings LLC, 3. September 2000, abgerufen am 24. Juni 2018.
45. ↑ Susan Athey, Christian Catalini, Catherine E. Tucker: *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*. In: *MIT Sloan Research Paper*. Nr. 5196-17. Stanford Graduate School of Business, Stanford 17. April 2018, doi:10.2139/ssrn.2916489 (englisch).
46. ↑ Tobias Dienlin, Sabine Trepte: *Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors*. In: *European Journal of Social Psychology*. Band 45, Nr. 3. John Wiley & Sons, 14. Juli 2014, ISSN 1099-0992, doi:10.1002/ejsp.2049 (englisch).
47. ↑ Monika Taddicken: *The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*. In: *Journal of Computer-Mediated Communication*. Band 21, Nr. 2, 1. Januar 2014, S. 248–273, doi:10.1111/jcc4.12052 (englisch).
48. ↑ Digitalcourage: *Privacy by Default: Datenschutz darf keine Ausnahme bleiben.* 9. Mai 2014, archiviert vom Original am 24. April 2017; abgerufen am 24. Juni 2018.
49. ↑ Datenschutz-Wiki-Bearbeiter: *Technische und organisatorische Maßnahmen.* In: *Datenschutz-Wiki.* Ruhr-Universität Bochum, BvD, 29. April 2016, abgerufen am 24. Juni 2018.
50. ↑ *M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung.* In: *IT-Grundschutz-Katalog.* Bundesamt für Sicherheit in der Informationstechnik, 2013, abgerufen am 24. Juni 2018.
51. ↑ *M 2.1 Festlegung von Verantwortlichkeiten und Regelungen.* In: *IT-Grundschutz-Katalog.* Bundesamt für Sicherheit in der Informationstechnik, 2013, abgerufen am 24. Juni 2018.
52. ↑ *M 2.505 Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten.* In: *IT-Grundschutz-Katalog.* Bundesamt für Sicherheit in der Informationstechnik, 2013, abgerufen am 24. Juni 2018.

53. ↑ David Engemann: *Braucht ein Kleinunternehmer einen Datenschutzbeauftragten?* Landesbeauftragte für Datenschutz und Informationsfreiheit NRW sowie der Händlerbund auf die Frage nach der Bestellung eines Datenschutzbeauftragten für Kleinunternehmer. 6. Februar 2018, abgerufen am 26. Februar 2018.
54. ↑ dazu *Riesenhuber*, in: BeckOK Datenschutzrecht, Stand 1. Februar 2018, Art. 88, Rn. 67 ff. mwN.
55. ↑ Hochspringen nach: a b Christoph Weiss: *Die Neuordnung des Datenschutzes in Europa.* In: *fm4.orf.at.* FM4, 28. Februar 2012, abgerufen am 2. Januar 2019.
56. ↑ Berufsverband der Datenschutzbeauftragten Deutschlands: *EU-Pläne zum Datenschutz belasten Wirtschaft.* (Memento des Originals vom 18. Mai 2015 im *Internet Archive*) **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe den Link gemäß Anleitung und entferne dann diesen Hinweis.@1@2Vorlage:Webachiv/IABot/www.bvdnet.de In: BvDnet.de vom 10. Mai 2015.
57. ↑ BvD: *Datenschützer mahnen klare Regeln für den Datentransfer aus der EU in Drittstaaten an. BvD veröffentlicht Positionspapier zur EU-Datenschutzgrundverordnung.* (Memento des Originals vom 15. Juli 2015 im *Internet Archive*) **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe den Link gemäß Anleitung und entferne dann diesen Hinweis.@1@2Vorlage:Webachiv/IABot/www.bvdnet.de vom 13. Juli 2015.
58. ↑ *Pressemitteilung: Subsidiaritätsrüge zur europäischen Datenschutz-Grundverordnung.* Bundesrat, 30. März 2012, abgerufen am 24. Februar 2015.
59. ↑ Verhandlungsposition des Europäischen Parlamentes vom 21. Oktober 2013
60. ↑ Hochspringen nach: a b Svenja Bergt: *Weichspüler für den Datenschutz.* In: *TAZ.* 4. März 2015, abgerufen am 4. März 2015.
61. ↑ Heise-Online: Rechtsexperte: Datenschutz-Grundverordnung als „größte Katastrophe des 21. Jahrhunderts“
62. ↑ *Neue Datenschutz-Grundverordnung der EU laut Experten ohne Wirkung.* In: *Heise.de.* Abgerufen am 5. Oktober 2016.
63. ↑ *Studie: EU-Datenschutz-Grundverordnung verfehlt alle Ziele – Kasseler Juristen entwirren Rechtslage.* In: *uni-kassel.de.* Universität Kassel, 29. September 2016, archiviert vom Original am 15. Dezember 2017; abgerufen am 2. Januar 2019.
64. ↑ SN 39/16: Zur Öffnungsklausel der Datenschutz-Grundverordnung, Stellungnahme Nr.: 39/2016 des Deutschen Anwaltvereins durch den Ausschuss Berufsrecht zu den Öffnungsklauseln der Datenschutz-Grundverordnung (EU) 2016/679 vom 27. April 2016, Berlin, August 2016.
65. ↑ Stellungnahme Nr.: 39/2016, S. 3.
66. ↑ Inanspruchnahme der Öffnungsklauseln in Artikel 90 DSGVO iVm Artikel 58 Absatz 1 Buchstaben e und f DSGVO, „um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung von mandatsbezogenen Informationen in Einklang zu bringen“ (Stellungnahme Nr.: 39/2016, S. 3).
67. ↑ Inanspruchnahme der Öffnungsklauseln in Artikel 6 Abs. 1 Satz 1 lit. e DSGVO, da die Verarbeitung personenbezogener Daten im öffentlichen Interesse gemäß Artikel 6 Abs. 1 Satz 1 Buchstabe e DSGVO liegt, wenn sie der anwaltlichen Berufsausübung dient (Stellungnahme Nr.: 39/2016, S. 5 ff).
68. ↑ In Artikel 15 DSGVO sind Auskunftsrechte geregelt. Ein Auskunftsrecht soll nicht bestehen, „wenn und soweit die personenbezogenen Daten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen“ (Stellungnahme Nr.: 39/2016, S. 7).

69. ↑ SRF Kultur: Sternstunde Philosophie: *Der Philosophische Stammtisch: Schöne neue digitale Welt?* (ab 0:12:45) 15. September 2018 auf YouTube, abgerufen am 25. Januar 2018.
70. ↑ Hochspringen nach: a b c Kevin J. O'Brien: *Silicon Valley Companies Lobbying Against Europe's Privacy Proposals.* In: *New York Times.* 25. Januar 2013, abgerufen am 30. März 2013.
71. ↑ Übersicht auf der Internetpräsenz von LobbyPlag.eu
72. ↑ *Amendments/Overview.* In: *Lobbyplag.* Abgerufen am 11. Juni 2013.
73. ↑ Uwe Ebbinghaus, Stefan Schulz, Thomas Thiel: *Machtprobe mit Silicon Valley.* 11. März 2014, abgerufen am 16. März 2014.
74. ↑ Volker Briegleb, Stefan Krempl: *EU-Parlament gibt grünes Licht für Datenschutzreform.* In: *heise.de.* 21. Oktober 2013, abgerufen am 22. Oktober 2013.
75. ↑ Markus Beckedahl: *EU-Datenschutzgrundverordnung passiert erste Lesung im EU-Parlament.* In: *netzpolitik.org*, 12. März 2014.
76. ↑ *EU-Datenschutzgrundverordnung: EU-Minister einigen sich auf Datenschutzreform*. In: *Die Zeit*. 15. Juni 2015 (zeit.de [abgerufen am 16. Juni 2015]).
77. ↑ Pressemitteilung der Europäischen Kommission vom 15. Dezember 2015.
78. ↑ Rat der Europäischen Union: Standpunkt des Rates in erster Lesung im Hinblick auf den Erlass der VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
79. ↑ Rat der Europäischen Union: Data protection reform: Council adopts position at first reading (Pressemitteilung vom 8. April 2016).
80. ↑ Europäisches Parlament: Parlament verabschiedet EU-Datenschutzreform – EU fit fürs digitale Zeitalter (Pressemitteilung vom 14. April 2016).
81. ↑ Amtsblatt der Europäischen Union vom 4. Mai 2016: Abl. EU 2016 L 119/1.
82. ↑ Rat der Europäischen Union: Corrigendum zu 2012/0011 (COD), Nr. 12399/16 vom 27. Oktober 2016 (PDF).
83. ↑ *Andreas Albert und Nicolai Kwasniewski: „Wie ein Abkommen den Datenschutz durchlöchert".* In: *Spiegel Online*. 25. November 2016.
84. ↑ Bundesgesetzblatt für die Republik Österreich: *Datenschutz-Anpassungsgesetz 2018.* 31. Juli 2017, abgerufen am 17. November 2017 (PDF).
85. ↑ Wirtschaftskammer Österreich: *EU-Datenschutz-Grundverordnung (DSGVO): Das Datenschutz-Anpassungsgesetz 2018.* Wirtschaftskammer Österreich, 26. September 2017, abgerufen am 22. November 2017.
86. ↑ *Österreich spült sich EU-Regeln weich.* In: *orf.at.* 25. April 2018, abgerufen am 26. April 2018.
87. ↑ *Keine Strafen: Österreich zieht neuem Datenschutz die Zähne.* In: *heise.de.* 24. April 2018, abgerufen am 26. April 2018.
88. ↑ *Unternehmen kommen bei DSGVO-Umsetzung kaum voran.* In: *wiwo.de.* 27. September 2018, abgerufen am 8. Januar 2019.
89. ↑ *Kaum Fortschritte - Umsetzung der Datenschutz-Grundverordnung.* In: *industrie.de.* Konradin Mediengruppe, 4. Oktober 2018, abgerufen am 8. Januar 2019.
90. ↑ Rüdiger Franz: *Zweifel an Nutzen - EU-Datenschutz macht Bonner Wirtschaft viel Arbeit.* In: *general-anzeiger-bonn.de.* 8. Januar 2019, abgerufen am 9. Januar 2019.
91. ↑ Dietmar Neuerer: *Unternehmen drohen Bußgelder in „erheblichem Umfang".* In: *handelsblatt.de.* 30. Oktober 2018, abgerufen am 8. Januar 2019.
92. ↑ David Zajonz: *Drei Monate DSGVO - Die große Abmahnwelle ist ausgeblieben.* In: *tagesschau.de.* 25. August 2018, abgerufen am 8. Januar 2019.

93. ↑ Beschriftung der Gegensprechanlagen, Webseite von *Stadt Wien - Wiener Wohnen*, abgerufen 31. Oktober 2018
94. ↑ Heike Anger, Dietmar Neuerer: *Behörden verhängen erste Bußgelder wegen Verstößen gegen DSGVO.* In: *handelsblatt.de.* 19. Januar 2019, abgerufen am 25. Januar 2019: „Die meisten Bußgelder verhängte Nordrhein-Westfalen (33), gefolgt von Hamburg (3) und Baden-Württemberg und Berlin (jeweils 2) und dem Saarland (1). Allein beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA), das die Einhaltung des Datenschutzrechts in privaten Wirtschaftsunternehmen, bei Freiberuflern, in Vereinen und Verbänden sowie im Internet überwacht, laufen derzeit 85 Bußgeldverfahren nach der DSGVO. Mit Blick auf die Höhe der Bußgelder besteht derzeit offenbar noch Schonfrist. So verhängte der Landesdatenschutzbeauftragte von Baden-Württemberg mit 80.000 Euro bislang die höchste Einzelstrafe. Im konkreten Fall landeten aufgrund unzureichender interner Kontrollmechanismen Gesundheitsdaten im Internet. Hamburg verhängte insgesamt Bußgelder in Höhe von 25.000 Euro, Nordrhein-Westfalen von knapp 15.000 Euro.“
95. ↑ CNIL: *Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.* In: *Légifrance.* 19. Januar 2019, abgerufen am 25. Januar 2019 (französisch, « [C]omme cela a également été relevé au titre du manquement aux obligations de transparence, l'information fournie n'est pas suffisamment claire et compréhensible en ce qu'il est difficile pour un utilisateur d'avoir une appréhension globale des traitements dont il peut faire l'objet et de leur portée. » (deutsch: „Wie auch im Zusammenhang mit der Verletzung der Transparenzanforderungen festgestellt wurde, sind die bereitgestellten Informationen nicht ausreichend klar und verständlich, sodass es für einen Benutzer nicht nachvollziehbar ist, welche Verarbeitungen mit seinen Daten durchgeführt werden.“)).
96. ↑ CNIL: *Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.* In: *Légifrance.* 19. Januar 2019, abgerufen am 25. Januar 2019 (französisch, « Elle constate néanmoins que s'agissant de la dernière catégorie [‹ Informations conservées pendant de longues périodes pour des raisons précises. ›], seules des explications très générales sur la finalité de cette conservation sont fournies et aucune durée précise ni les critères utilisés pour déterminer cette durée ne sont indiqués. Or cette information figure parmi celles devant être obligatoirement délivrées aux personnes en application du a) du °2 de l'article 13 du Règlement. » (deutsch: „Es wird festgestellt, dass in der letztgenannten Kategorie [‚Informationen, die aus bestimmten Gründen über einen längeren Zeitraum aufbewahrt werden.‘] nur sehr allgemeine Erläuterungen Speicherzweck gegeben werden und keine genaue Dauer oder die Kriterien zur Bestimmung dieser Dauer angegeben werden. Diese Informationen sind jedoch obligatorischen Informatione, gemäß Artikel 13 Absatz 2 Buchstabe a) der Verordnung zur Verfügung zu stellen sind.“)).
97. ↑ Simon Rebiger, Ingo Dachwitz: *Die DSGVO zeigt erste Zähne: 50-Millionen-Strafe gegen Google verhängt.* In: *netzpolitik.org.* 21. Januar 2019, abgerufen am 25. Januar 2018.