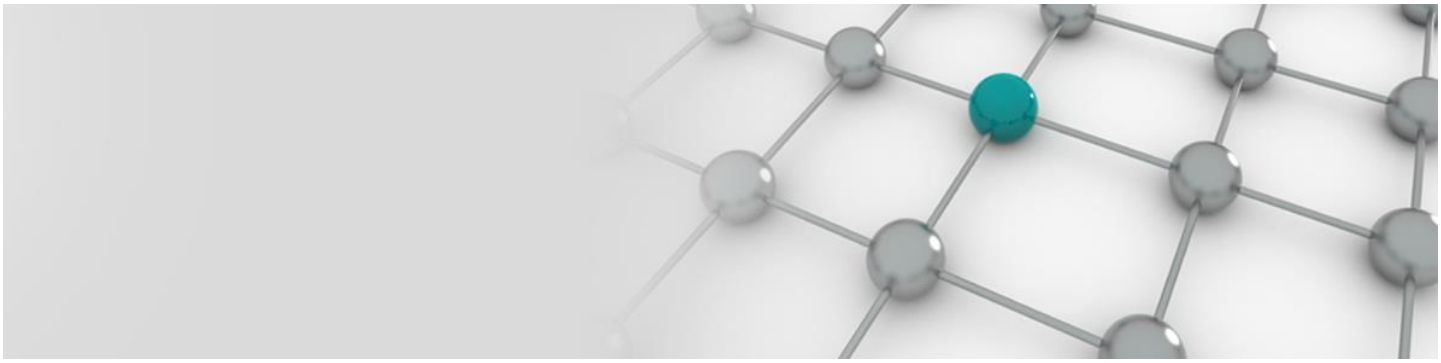

EU-DATENSCHUTZ GRUNDVERORDNUNG

Whitepaper

Was ändert sich mit dem neuen Recht?
Was sollten Unternehmen jetzt tun?

AdOrga Solutions

Regina Mühlich
consulting@adorgasolutions.de

Inhalt

1 Einleitung 2
2 Allgemeiner Überblick 2
3 Wirkung und Reichweite 3
3.1 Nationale Öffnungsklauseln 3
4 Was ändert sich mit dem neuen Recht? 4
4.1 Bußgelder in Abhängigkeit des weltweiten Umsatzes 4
4.2 Der betriebliche Datenschutzbeauftragte 4
4.3 Nachweispflichten und Unterrichtung 5
4.4 Die Datenschutz-Folgeabschätzung 5
4.5 Funktionsübertragung adé 6
4.6 Weltweite Geltung 6
5 Neue Rechte für betroffene Personen 6
5.1 Das Recht auf Vergessen werden 6
5.2 Die Datenportabilität 6
5.3 Koppelungsverbot 6
5.4 Arbeitnehmerdatenschutz 6
6 Fazit: Was sollten Unternehmen jetzt tun? 7

* Hinweis: Der Übersichtlichkeit wegen werden im Folgenden nur die männlichen Formen verwendet.

1 Einleitung

Am 15. Dezember 2015, nach fast vier Jahren Debatten, stieg „weißer Rauch“ in Brüssel auf: Die Vertreter der EU-Kommission und des EU-Parlaments beschlossen den Entwurf der EU-Datenschutzgrund-verordnung (EU-DSGVO).

Jetzt im April 2016 erfolgte die Zustimmung seitens EU-Rat und EU-Parlaments Der Kompromiss wurde im schriftlichen Umlaufverfahren, ohne Änderungen und Anpassungen zum Entwurf, verabschiedet.

Es war dringend an der Zeit: Die bisherigen Regeln stammten aus dem Jahr 1995, waren veraltet und wurden in einzelnen EU-Ländern unterschiedlich umgesetzt. Wie geht es aber nun weiter? Was bleibt, was verändert sich? Welche Besserungen oder Herausforderungen bringt die EU-DSGVO mit sich?

2 Allgemeiner Überblick

Die Verordnung wird 20 Tage nach der Veröffentlichung im EU-Amtsblatt in Kraft treten und zwei Jahre nach der Veröffentlichung wirksam sein. Ab Mai 2018 gelten für fast alle EU-Länder die gleichen (hohen?) Standards. Durch die Ausnahmen, die Dänemark und Großbritannien im Bereich Justiz und Inneres ausgehandelt haben, werden die Bestimmung der Richtlinie dort nur eingeschränkt gelten.

Ein einführender allgemeiner Überblick:

- Nutzer erhalten das Recht, Informationen leichter wieder löschen zu lassen („Recht auf Vergessenwerden“) und Daten von einem Anbieter zum nächsten mitzunehmen („Portabilität“).
- Zugleich wird das Alter, ab dem man sich bei Online-Netzwerken wie Facebook oder WhatsApp anmelden darf, in einigen europäischen Ländern von 13 auf 16 Jahre steigen.
- Internet-Konzerne wie Google, Facebook & Co müssen sich die Zustimmung zur Datennutzung ausdrücklich einholen und ihre Produkte datenschutzfreundlich voreinstellen („Privacy by Design“). Daran sind nicht nur europäische Unternehmen gebunden, sondern beispielsweise auch US-Firmen.
- Außerdem können gegen Unternehmen bei Verstoß gegen die Datenschutzregeln Strafen von bis zu vier Prozent der weltweiten Jahresumsätze verhängt werden.
- Aufbau der EU-DSGVO:

  Kapitel I: Allgemeine Bestimmungen
  Kapitel II: Grundsätze
  Kapitel III: Rechte der betroffenen Person
  Kapitel IV: Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter
  Kapitel V: Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen
  Kapitel VI: Unabhängige Aufsichtsbehörden
  Kapitel VII: Zusammenarbeit und Kohärenz
  Kapitel VIII: Rechtsbehelfe, Haftung und Sanktionen

Kapitel IX: Vorschriften für besondere Datenverarbeitungssituationen
Kapitel X: Delegierte Rechtsakte und Durchführungsbestimmungen
Kapitel XI: Schlussbestimmungen

- Neue Begrifflichkeiten:
  Das BDSG spricht von der „verantwortlichen Stelle“, die EU-DSGVO von der „Verarbeitung Verantwortlicher“. Aus dem „Auftragsdatenverarbeiter“ wird der „Auftragsverarbeiter“, aus dem Betroffenen die „betroffene Person“. Dritte und Empfänger werden zum „Empfänger“.

3 Wirkung und Reichweite

Die Verordnung soll Datenverarbeitungen künftig in der gesamten Union einheitlich regeln und den bisherigen Flickenteppich nationaler Gesetze zum Umgang mit personenbezogenen Daten ablösen. Die Wirkungen der EU-Datenschutzgrundverordnung erstreckt sich gemäß Art. 91 GVO: „….Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat.“ Des Weiteren besagt Art. 88 GVO: „1. Die Richtlinie 95/46/EG wird aufgehoben…“. Die GVO ist somit eine allgemeine Regelung mit unmittelbarer innerstaatlicher Geltung („Durchgriffswirkung“) und bedeutet eine grundsätzliche Vollharmonisierung, da sie nationales Datenschutzrecht ersetzt.

3.1 Nationale Öffnungsklauseln

In bestimmten Bereichen wird es Öffnungsklauseln für nationale Gesetzgeber geben, die es vor Inkrafttreten der EU-Datenschutzgrundverordnung zu regeln gilt. Diese sind:

- Spezifischere Anforderungen an die Verarbeitungen zur Erfüllung rechtlicher Verpflichtungen oder öffentlicher Aufgaben (Art. 6 Abs. 2a)
- Datenschutzbeauftragter (Art. 35)
- Betroffenenrechte im öffentlichen Interesse (Art. 21)
- Presse, Kunst, Literatur (Art. 80)
- Zugang zu amtlichen Dokumenten (Art. 80a)
- Informationen des öffentlichen Sektors (Art. 88 aa)
- Nationale Kennzeichen von allgemeiner Bedeutung (Art. 80 b)
- Gesundheit (Art. 81)
- Arbeitnehmerdatenschutz (Art. 82)
- Forschung (Art. 83)
- Berufsgeheimnisse (Art. 84)
- Kirchen (Art. 85)
- Bedeutung des zukünftigen EU-Datenschutzrechts für Unternehmen und Betriebe im Detail, sprich für den für die Verarbeitung Verantwortlichen (bisher verantwortliche Stelle)

(die Zitate aus dem Rechtstext sind der deutschen Übersetzung der Arbeitsfassung 5455/16 vom 28. Januar 2016 entnommen: https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/bvd-allgemein/EU-DSGVO/280116GRV-politische_Einigung_pdf.pdf).

4 Was ändert sich mit dem neuen Recht?

Ob das EU-Datenschutzgesetz wirklich strenger als das bisherige deutsche Recht ist, wird derzeit kontrovers diskutiert und beurteilt. Wie so oft kommt es auf den Blickwinkel des einzelnen Unternehmens an – Brüssel schraubt an vielen Stellen:

4.1 Bußgelder in Abhängigkeit des weltweiten Umsatzes

Bußgelder waren bis dato bei Unternehmen und Betrieben kein häufiges Thema, sondern eher selten. Gemäß § 43 Bundesdatenschutzgesetz (BDSG) werden Ordnungswidrigkeiten mit einer Geldbuße bis zu 50.000 Euro geahndet. Ein Verstoß gegen die Ordnungswidrigkeitentatbestände des § 43 Abs. 2 BDSG zieht ein Bußgeld von bis zu 300.000 Euro nach sich. § 43 Abs. 2 BDSG stellt insbesondere Pflichten beim Umgang mit personenbezogenen Daten unter Strafe.

Das ändert sich nun gründlich: Brüssel macht Ernst bei den Sanktionen. In der Verordnung heißt es, diese sollen „wirksam und abschreckend“ sein. Wenn sich Unternehmen, Betrieb oder ein Verein nicht an die neuen Vorgaben halten, drohen Geldbußen. Dabei wird zwischen zwei Bußgeldrahmen unterschieden:

Bei weniger schweren Fehlern (d. h. Verstöße gegen Organisationsregeln) bis zu zwei Prozent des Umsatzes oder 10 Mio. Euro – je nachdem, welche Summe höher ist.

Bei Verstößen gegen Zulässigkeit und Rechte der Betroffenen sollen zukünftig Bußgelder bis 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes (je nachdem, welche Summe höher ist) verhängt werden.

Der Bußgeldkatalog ist bindend. Das bedeutet, die Aufsichtsbehörden haben keinen Ermessensspielraum (mehr), ob und in welcher Höhe sie ein Bußgeld verhängen.

Die EU-Mitgliedsstaaten legen gemäß Art. 79 b Sanktionen für Verstöße, die keiner Geldbuße unterliegen, fest. Diese Sanktionen müssen allerdings wirksam, verhältnismäßig und abschreckend sein.

4.2 Der betriebliche Datenschutzbeauftragte

In Kapitel 4, Abschnitt 4, Artikel 35 zur Benennung eines Datenschutzbeauftragten heißt es:

„Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

(a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die in ihrer gerichtlichen Eigenschaft handeln, oder

(b) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen, oder

(c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 9a besteht.

Es gibt also fortan eine Bestellpflicht. Des Weiteren exisitiert eine nationale Öffnungsklausel (Art. 35 Abs. 4). Es ist davon auszugehen, dass Deutschland die Regelung gemäß § 4f BDSG übernehmen wird. Die Stellung und Aufgaben (Art. 73) des (deutschen) Datenschutzbeauftragten bleiben weitestgehend unverändert: Er hat einen **Sicherstellungsauftrag** (§ 29 (1), § 37 (1) BDSG) und **Hinwirkungsauftrag** (§ 4g Abs. 1 BDSG) sowie zukünftig, als Aufgabenerweiterung, einen **Überwachungsauftrag** (Art 36 Abs. 1 EU-DSGVO 2016).

Der Datenschutzbeauftragte musste bislang gemäß § 4g BDSG auf die Einhaltung des BDSG und anderer Vorschriften zum Datenschutz hinwirken. Hinwirken deshalb, weil er die Umsetzung der datenschutzrechtlichen Vorschriften nicht selbst vornehmen kann. Die EU-DSGVO verlangt zukünftig, dass überwacht werden muss, dass auch alle Vorgaben und Regeln eingehalten werden. In Konsequenz haften Datenschutzbeauftragte und Unternehmer nunmehr auch persönlich (**Haftung**).

4.3 Nachweispflichten und Unterrichtung

Die Unternehmen und Betriebe müssen, wie bisher auch, wirksame Datenschutzrichtlinien einführen und ihre Mitarbeiter schulen. Die Einhaltung der definierten Vorschriften muss bewiesen werden können. Ein effektives Datenschutzmanagementsystem inklusive Risikoanalysen, Strukturen, Prozessen, Kontrollen und Change Management wird notwendig. Des Weiteren müssen Unternehmen betroffene Personen über deren Datenverarbeitung künftig umfassender und auch früher informieren. Hier drohen bei Nichtbeachtung hohe Bußgelder.

4.4 Die Datenschutz-Folgeabschätzung

Ein neues Werkzeug für Aufsichtsbehörden und verantwortliche Stellen ist die Datenschutz-Folgeabschätzung (Art. 33). Wobei, so ganz neu ist das Thema nicht. § 4d BDSG regelt dies bereits mit der Vorabkontrolle: „Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung…“

Mit der Folgeabschätzung sollen Risiken erkannt und bewertet werden, die für die betroffene Person entstehen, wenn ein Unternehmen eine neue Technik oder ein neues System zur Datenverarbeitung einsetzt. Angesichts der unterschiedlichen Interessen und Rollen der Beteiligten sollen auf diese Weise Grundrechtsverletzungen verhindert werden. Die Experten schlagen vor, sich an **sechs Schutzzielen** zu orientieren: Aus dem Bereich IT-Sicherheit sind dies Verfügbarkeit, Integrität und Vertraulichkeit sowie aus den Datenschutzzielen die Nichtverkettbarkeit, Transparenz und Intervenierbarkeit.

Bei der Datenschutz-Folgeabschätzung werden die Schutzziele nicht nur aus der Unternehmensperspektive betrachtet, welche die Geschäftsprozesse sichern soll. Vielmehr geht es hierbei um die Organisation selbst, die Daten verarbeitet und als Risiko betrachtet wird. Das bedeutet, wenn eine Datenverarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten betroffener Personen zur Folge hat, muss das Unternehmen eine umfassende Vorprüfung vornehmen, dokumentieren und gegebenenfalls später mit der Datenschutzbehörde abstimmen.

4.5 Funktionsübertragung adé

Die sogenannte Funktionsübertragung wurde lange diskutiert. Es ging um die Abgrenzungsfrage, wann die Tätigkeit eines Dienstleisters aus seiner technischen Unterstützung in die eigenverantwortliche Verarbeitung im Sinne des § 3 Abs. 7 BDSG übergeht. Art. 26 DS-GVO regelt die Auftragsverarbeitung in Verbindung mit Art. 24 „Gemeinsam für die Verarbeitung Verantwortliche“. Der für die Verarbeitung Verantwortliche hat grundsätzlich die Zwecke der Verarbeitung vorzugeben, dem Auftragsverarbeiter bleibt jedoch die Entscheidung über die Mittel. Dadurch werden die bisherigen Funktionsübertragungen in Zukunft regelmäßig unter die Auftragsverarbeitung fallen.

4.6 Weltweite Geltung

Die Datenschutzgrundverordnung soll nicht nur für die Europäische Union gelten, sondern weltweit. Auch Unternehmen im Ausland müssen den europäischen Datenschutz einhalten, wenn sie Daten von Personen in der EU verarbeiten, diesen Personen Waren und Dienstleistungen anbieten.

5 Neue Rechte für betroffene Personen

Auch für die Betroffenen, welche fortan „betroffene Personen“ tituliert werden, gibt es neue Rechte.

5.1 Das Recht auf Vergessen werden

Bei der Veröffentlichung von Daten müssen angemessene, auch technische, Maßnahmen ergriffen werden, um dritte Parteien über einen Löschungswunsch informieren zu können. Mit Art. 17. Abs. 2, dem „Right to be forgotten“ haben Nutzer zukünftig das Recht, Informationen leichter wieder löschen zu lassen. Der Empfänger, an den ein Unternehmen Daten weitergegeben hat, muss demnach ebenfalls über die Löschung informiert werden.

5.2 Die Datenportabilität

Die Datenportabilität (Art. 18) umfasst ein weiteres neues Recht für die betroffene Person. Damit hat ein Betroffener den Anspruch auf Kopie der verarbeiteten Daten, wobei die Übergabe in gängigem, strukturiertem Format erfolgen muss. Für die Unternehmen wird diese Regelung sicherlich teuer und aufwändig werden. Die Datenportabilität gilt auch, wenn beispielsweise ein Arbeitsverhältnis endet.

5.3 Koppelungsverbot

Vertragliche Zusatzleistungen dürfen nicht mehr daran geknüpft werden, dass die betroffene Person in die Verarbeitung der Daten einwilligt. Dies betrifft vor allem „Dienst gegen Daten“ (Koppelungsverbot bei Einwilligungen).

5.4 Arbeitnehmerdatenschutz

Für den Arbeitnehmerdatenschutz (Art. 82) gibt es eine nationale Öffnungsklausel. Viele der neuen Regeln haben die IT-Wirtschaft im Blick und passen nicht so richtig zum Datenschutz am Arbeitsplatz. Betriebsvereinbarungen sind weiterhin eine Alternative, setzen jedoch eine gute Zusammenarbeit mit dem Betriebsrat voraus. Es bleibt abzuwarten, wie die Bundesregierung mit der Öffnungsklausel hinsichtlich des Arbeitnehmerdatenschutzes umgeht. Es ist aber auch hier davon auszugehen, dass § 32 BDSG

„Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“ weitestgehend unverändert bleibt.

Firmen müssen ihre IT-Systeme so gestalten, dass diese den Anforderungen entsprechen, z. B. von vornherein so wenig wie möglich personenbezogene Daten zu sammeln und zu verarbeiten, wie es zur Erreichung des Zweckes konkret notwendig ist (Erforderlichkeit und Zweckbindung). Wenn immer möglich, sind diese Daten zu pseudonymisieren. Insbesondere dem Grundsatz des Datenschutzes durch Technik (**data protection by design**) und durch datenschutzfreundliche Voreinstellungen (**data protection by default**) ist hier Genüge zu tun. Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten sind herzustellen, um es der betroffenen Person zu ermöglichen, die Datenverarbeitung zu überwachen sowie den für die Verarbeitung Verantwortlichen in die Lage zu versetzen, Sicherheitsfunktionen zu schaffen und zu verbessern (Standpunkt des Europäischen Parlaments vom 14. März 2014, Grund 61).

6 Fazit: Was sollten Unternehmen jetzt tun?

- Prüfen Sie bereits jetzt, welche Systeme von der neuen Gesetzgebung betroffen sind.
- Prüfen Sie Ihr bestehendes Datenschutzmanagement-System auf Gesetzeskonformität. Damit wird die Umsetzung der zukünftigen Regelungen zwar nicht einfacher, aber leichter.
- Wo steht Ihr Unternehmen jetzt und was ist zu tun, um künftig den Anforderungen der EU-Datenschutzgrundverordnung gerecht zu werden?
- Führen Sie eine Risko-Analyse durch. Welche Risiken und Gefährdungen drohen Ihrem Unternehmen?
- Planen Sie Ihre Ressourcen – sowohl im Hinblick auf Mitarbeiter als auch auf das Budget. Es gibt viele Veränderungen und gegebenenfalls wird vieles anzupassen sein.
- Erstellen Sie einen Plan. In größeren Unternehmen wird die Transformation auf die Datenschutzgrundverordnung eine große Herausforderung. Beginnen Sie rechtzeitig – einige Arbeitsschritte können schon jetzt umgesetzt werden.
- Die EU-DSGVO sieht vor (Artikel 35), dass die meisten Unternehmen einen Datenschutzbeauftragten bestellen müssen. Unabhängig davon, wie der deutsche Gesetzgeber mit der Öffnungsklausel umgeht: Jetzt ist der beste Zeitpunkt, die interne Situation zu prüfen und sich gegebenenfalls auch rechtzeitig externe Unterstützung zu holen.
- Das neue Datenschutzgesetz sieht umfassende Rechenschafts- und Dokumentationspflichten vor. Überlegen Sie sich rechtzeitig, wie und mit welchen Mitteln Sie dies zukünftig gewährleisten können.
- Dies alles verursacht (hohe) Umsetzungskosten. Planen Sie diese auch in Ihr zukünftiges Budget ein.