

Datenschutzgrundverordnung (DSGVO)

Markus Pieper, MdEP

(Sachstand: 25. Mai 2018)

Worum geht es?

Die Datenschutzgrundverordnung (kurz DSGVO) ist ein Gesetz, das Regeln für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten beinhaltet. Ziel der DSGVO ist es, Datensicherheit im 21. Jahrhundert zu gewährleisten und durch ein erstmals einheitliches Datenschutzsystem in der Europäischen Union (EU) Bürokratie abzubauen. Das Gesetz wurde 2016 beschlossen. In Deutschland tritt daher eine Neufassung des Bundesdatenschutzgesetzes (BDSG) am 25. Mai 2018 in Kraft.

- Unter personenbezogenen Daten werden alle Daten, die in irgendeiner Form einer Person zugeordnet werden können, verstanden: *Name, Geburtsdatum, Lokalisierung, Online-Kennung, Gesundheitsdaten, Einkommen und sonstige persönliche Profile.*

Warum wurde das Datenschutzrecht überhaupt geändert?

Das Deutsche Bundesdatenschutzgesetz zählte lange zu einem der schärfsten Datenschutzrechte in der EU, was zu einem erheblichen Wettbewerbsnachteil für deutsche Unternehmen führte. Daher diente das Bundesdatenschutzgesetz der DSGVO auf EU-Ebene auch als Vorlage. Darüber hinaus führten die unterschiedlichen datenschutzrechtlichen Anforderungen für Unternehmen, die grenzüberschreitend in der EU tätig sind, zu enormen Kosten. In einer globalisierten Welt Datenschutz kann sich nicht nach dem Standort des Unternehmens richten, sondern nach dem des Bürgers. Daher gelten die neuen Datenschutzanforderungen für alle, die mit Daten europäischer Bürger arbeiten, also auch für Facebook, Google und Unternehmen wie Cambridge Analytica.

Was wird sich ändern?

Die wesentlichen Datenschutz-Prinzipien, die Dokumentation der Verarbeitungstätigkeiten (Verfahrensverzeichnis) sowie die Bestellung eines Datenschutzbeauftragten **sind weitestgehend gleich geblieben**. Das liegt vor allem daran, dass sich die DSGVO stark am aktuellen bzw. bald alten Bundesdatenschutzgesetz orientiert. **Neuerungen** umfassen:

- ausgebauten **Anforderungen an die Einwilligung** für sensible Daten wie auch die Einwilligung von Kindern und Jugendlichen;
- **Neue Rechte für Betroffene:** Lösch-, Widerspruchs- und Informationsrechte; Prominentestes Beispiel darunter ist das Recht, vergessen zu werden;
- **Datensicherheit:** Es muss zukünftig eine Datenschutz-Folgenabschätzung bei risikobelasteter Verarbeitung durchgeführt werden. Das ist beispielsweise bei groß angelegten Überwachungen öffentlicher Räume oder der Verarbeitung biometrischer Daten der Fall. Dagegen entfällt in Deutschland die Pflicht zur Meldung der Verfahren bei der Aufsichtsbehörde (sog. Vorab-Kontrolle);

- Ferner werden externe Datenverarbeiter gegenüber Auftraggebern bei Datenpannen stärker in die Verantwortung genommen.

Wer ist von den Änderungen betroffen?

- Neben öffentlichen Stellen sind in erster Linie **Unternehmen** aber **auch (gemeinnützige) Vereine und Organisationen**, die Daten **sammeln, speichern und verwenden**, betroffen. Das heißt, auch Unternehmen, die Kundendateien führen oder Lieferantendaten speichern, fallen unter die Verordnung.
- Sofern Privatpersonen aus persönlichen oder familiären Gründen Daten verarbeiten, findet die Datenschutzgrundverordnung keine Anwendung.

Verhältnismäßigkeit: Selbstverständlich gelten manche Anforderungen nur für gewisse sensible Daten oder Unternehmen einer bestimmten Betriebsgröße:

- **Kleine und mittelständische Unternehmen** sind nicht verpflichtet, ein Verzeichnis ihrer Datenverarbeitungstätigkeiten zu führen, erfolgt die Verarbeitung gelegentlich und beinhaltet unter anderem keine sensiblen Daten.¹

Was passiert, wenn ich gegen die Datenschutzgrundverordnung verstoße?

Wie bisher hängt die Auswirkung von den **Umständen des einzelnen Verstoßes** sowie von der Bewertung der **jeweiligen Datenschutzbehörde** ab (Hinweis: hier besteht Spielraum für die Mitgliedstaaten!). So können die Datenschutzbehörden:

- Verantwortliche oder Auftragsverarbeiter verwarnen;
- die Verarbeitung zum Teil oder gänzlich beschränken;
- die Zertifizierung, die die Einhaltung der DSGVO bescheinigt, entziehen.
- Zusätzlich oder anstelle der oben genannten Maßnahmen Geldbußen verhängen. Diese können - je nach Art, Schwere, Dauer sowie Vorsätzlichkeit oder Fährlässigkeit des Verstoßes - auch über den aktuell in Deutschland geltenden Bußgeldern von maximal 300.000 Euro liegen.

Wie ist die DSGVO entstanden?

Als Gesetzgeber arbeiten das Europäische Parlament und der Rat, in dem für Deutschland die jeweiligen Bundesministerien vertreten sind, zusammen. Im Europäischen Parlament war der ehemalige Abgeordnete der Grünen Jan-Philipp Albrecht, im Rat das Innen- sowie das Justizministerium federführend verantwortlich. Darüber hinaus beinhaltet die DSGVO insbesondere im Beschäftigungsbereich eine Vielzahl von **Öffnungsklauseln bzw. Ausgestaltungsmöglichkeiten** für den nationalen Gesetzgeber.

Der Bundesgesetzgeber hat diese Anpassungen mit der Novellierung des Bundesdatenschutzgesetzes vor ca. einem Jahr vorgenommen. Beispielsweise sieht die DSGVO einen verpflichtenden Datenschutzbeauftragten für nicht-öffentliche Stellen vor, wenn das Kerngeschäft auf der Verarbeitung von personenbezogener Daten liegt (z.B. ein App-Hersteller) oder wenn die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten beruht, z.B. in der Personalverwaltung. Der deutsche Gesetzgeber hat diese Öffnungsklausel genutzt, um festzulegen, dass ein Datenschutzbeauftragter dann einzustellen ist, wenn mindestens zehn Personen mit der ständigen automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (Art. 38 BDSG-neu).

Das heißt, Gesetzgebung ist nie ausschließlich „europäisch“, sondern zieht immer noch weitere nationale oder sogar regionale Prozesse nach sich. Für die Kontrolle der Einhaltung der Datenschutzgesetze sind beispielsweise die jeweiligen Landesdatenschutzbehörden zuständig.

¹ Für die Definition von kleinen und mittleren Unternehmen (KMU):
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:de:PDF>

Welche Forderungen konnte die CDU/CSU-Gruppe im Europäischen Parlament (nicht) durchsetzen?

Beim Thema Datenschutz bilden die Linken im Europäischen Parlament stets Mehrheiten mit den Liberalen. So sieht die DSGVO die von den Grünen geforderten Geldbußen vor, gegen die sich die CDU/CSU stellte. Dagegen konnte die CDU/CSU die Pflicht zur Datenschutz-Folgenabschätzung und -Beauftragten auf Unternehmen, die als Kerntätigkeit Daten verarbeiten oder mit risikoreichen Daten arbeiten, einschränken.

Wie kann ich mich als Unternehmen etc. am besten auf die anstehenden Änderungen vorbereiten?

Nicht in Panik verfallen. Sollten Sie sich an das alte Bundesdatenschutzgesetz in Deutschland gehalten haben, ist grundsätzlich wenig zu befürchten. Ein strukturierter Abgleich des aktuellen Zustandes mit dem zukünftigen Soll-Zustand kann als Ausgangspunkt für mögliche Anpassungen dienen. Insbesondere sollten bereits geltende Verträge mit Auftragsdatenverarbeitern analysiert und gegebenenfalls angepasst werden, damit gewährleistet ist, dass die Vertragspartner ebenfalls gemäß der DSGVO handeln. Für die weitere Beratung sind folgende Ansprechpartner sowie deren Angebote hilfreich:

- Digitalverband Bitkom: Für Musterverträge und Leitfäden;²
- Kammern oder externen Dienstleister: Für weitere Fachkenntnisse.

Wie geht es weiter?

Die neuen Datenschutzregelungen gelten ab dem **25. Mai 2018**. In der Europäischen Union haben weniger als die Hälfte der Mitgliedstaaten ihre nationalen Bestimmungen angepasst. In Österreich wird anders als in Deutschland von Geldbußen bei Verstoß im Erstfall abgesehen. Das Bundesdatenschutzgesetz sieht die Möglichkeit einer Verwarnung ohne Verwarnungsgeld ausdrücklich nicht vor. Laut EU-Kommissarin für Justiz und Verbraucherschutz Vera Jourova ist es Aufgabe der nationalen Datenschutzbehörden festzulegen, wann die Verordnung spätestens umgesetzt sein muss. Damit stellte sie den europäischen Unternehmen Nachsicht in Aussicht.

Es gilt daher,

- (1) diese Spielräume auf nationaler Ebene verhältnismäßig und KMU-freundlich zu gestalten.
- (2) die Anwendung der DSGVO unbedingt - europäisch sowie national - einheitlich vorzunehmen, statt sie in den unterschiedlichen Bundesländern verschärft anzuwenden.
- (3) für die beratende Tätigkeit der Landesdatenschutzbeauftragten zu werben, statt eine Abmahnkultur heraufzubeschwören.

Unternehmen sollten positiv zur Umsetzung ermutigt werden, denn die DSGVO kann den Vertrauensverlust der Kunden, der durch die jüngsten Datenskandale entstanden ist, wieder herstellen und bietet den Unternehmen langfristig Einsparpotentiale.

² <https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html>