



2. CEMA Online IT.special: EU-Datenschutz-Grundverordnung

Rechtliche Betrachtung der DSGVO

Kai Bodensiek
Rechtsanwalt

Rechtsgrundlagen im Datenschutz

Datenschutzgrundverordnung (DSGVO)

- Wird am 25.5.2018 geltendes Recht
- Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat
- Grundsätzlicher Vorrang der DSGVO vor anderen Rechtsvorschriften
- Vereinheitlichung des Schutzniveaus in der gesamten EU
- Stärkung des Binnenmarkts (Unternehmen können die Datenverarbeitung in allen Mitgliedstaaten gleich regeln)
- Öffnungsklauseln (Mitgliedstaaten können in bestimmten Bereichen nationale Spezialgesetze schaffen)

Rechtsgrundlagen im Datenschutz

Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU)

- Anpassung des deutschen Datenschutzrechts an das geänderte Datenschutzrecht der EU
- Neustrukturierung des Bundesdatenschutzgesetz
- Ergänzung der DSGVO
- Fraglich, ob die im Entwurf vorgesehenen Konkretisierungsregelungen durch entsprechende Öffnungsklauseln in der DSGVO abgedeckt sind (Beschäftigtendatenschutz und Betroffenenrechte)

Gegenstand und Ziele der DSGVO

Art. 1 Abs. 1 DSGVO: „Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.“

- **Personenbezogene Daten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
- **Verarbeitung:** Jeder Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

Anwendungsbereich der DSGVO

Sachlicher Anwendungsbereich

Art. 2 Abs. 1 DSGVO: *„Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“*

- **Automatisierte Verarbeitung** umfasst letztlich jede Form von Datenverarbeitungsanlage
- **teilweise automatisierte Verarbeitung** liegt etwa vor, wenn ein Mensch die zu verarbeitenden Daten in ein System eingibt.
- **Nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen** umfasst Sammlungen personenbezogener Daten, die gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können.

Ausnahme, Art. 2 Abs. 2 lit. c) DSGVO: *„Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.“*

Anwendungsbereich der DSGVO

Räumlicher Anwendungsbereich

Art. 3 Abs. 1 DSGVO: *„Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.“*

Art. 3 Abs. 2 DSGVO: *„Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht*

- a) *betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;*
- b) *das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.“*

Die DSGVO gilt damit nicht nur für in der EU niedergelassene Unternehmen, sondern auch für außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind.

Grundsätze der DSGVO

- Grundsätze sind in Art. 5 DSGVO normiert (zentrale Norm)
- Diese Grundsätze sind bei Auslegung und Anwendung der gesamten Verordnung heranzuziehen
- Grundsätze sind kein Novum (§ 3a BDSG), Verletzungen waren aber bisher nicht an Rechtsfolgen geknüpft
- **Neu ist:** Bei fehlender oder mangelhafter Umsetzung der in Art. 5 normierten Grundsätze drohen Bußgelder von bis zu 20 Mio. oder von bis zu vier Prozent des globalen Umsatzes des Konzerns bzw. des Unternehmens, Art. 83 Abs. 5 lit. a) DSGVO.

Umsetzung der in Art. 5 DSGVO normierten Grundsätze ist aus Compliance-Sicht unbedingt erforderlich!

Grundsätze der DSGVO

Rechtmäßigkeit der Verarbeitung, Art. 5 Abs. 1 lit. a) DSGVO

- Verarbeitung personenbezogener Daten muss rechtmäßig sein
- Verarbeitung ist verboten, wenn nicht ein Erlaubnistatbestand vorliegt
- Art. 6 und Art. 9 enthalten eine Reihe von Erlaubnistatbeständen

Verarbeitung nach Treu und Glauben (Verhältnismäßigkeit), Art. 5 Abs. 1 lit. a) DSGVO

- Verarbeitung muss zur Verwirklichung eines legitimen Zwecks geeignet sein
- Verarbeitung muss das mildeste aller gleich effektiven Mittel zur Verwirklichung dieses Zwecks darstellen
- Verarbeitung muss auf der Basis einer angemessenen Interessenabwägung zwischen dem verfolgten Zweck und den mit der Verarbeitung verbundenen Folgen für die betroffene Person stehen

Grundsätze der DSGVO

Transparenz, Art. 5 Abs. 1 lit. a) DSGVO

- Für die betroffene Person sollte erkennbar sein, dass die betreffenden personenbezogenen Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden sowie in welchem Umfang die Daten verarbeitet werden und künftig noch verarbeitet werden sollen
- DSGVO sieht umfassende Informationspflichten bei der Erhebung personenbezogener Daten vor (Art. 13, 14)

Informationspflichten Verantwortlicher und Auskunftsrechte Betroffener gehen über die bisherigen Vorgaben des Bundesdatenschutzgesetzes hinaus. Prozesse und Verantwortlichkeiten sollten rechtzeitig so aufgesetzt werden, dass sie die Pflichten der DSGVO erfüllen.

Grundsätze der DSGVO

Zweckbindung, Art. 5 Abs. 1 lit. b) DSGVO

- Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden
- Personenbezogene Daten dürfen grundsätzlich nur für diejenigen Zwecke verwendet werden, für die sie erhoben wurden
- Eine Zweckänderung ist nur unter engen Voraussetzungen zulässig, Art. 6 Abs. 4 DSGVO

Datenminimierung, Art. 5 Abs. 1 lit. c) DSGVO

- „Personenbezogene Daten müssen dem Zweck **angemessen** und **erheblich** sowie auf das für die Zwecke der Verarbeitung **notwendige Maß** beschränkt sein.“

Grundsätze der DSGVO

Richtigkeit, Art. 5 Abs. 1 lit. d) DSGVO

- Personenbezogene Daten müssen **sachlich richtig** und erforderlichenfalls auf dem neuesten Stand sein
- Falls Daten unrichtig oder veraltet sind, muss der Verantwortliche alle angemessenen Maßnahmen ergreifen, um diese Daten **unverzüglich** zu korrigieren bzw. zu aktualisieren oder zu löschen

Speicherbegrenzung, Art. 5 Abs. 1 lit. e) DSGVO

- Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist
- Dieser Grundsatz wird durch die in Art. 17 festgelegten Löschpflichten konkretisiert

Verantwortliche sollten unbedingt Prozesse und Fristen für die regelmäßige Überprüfung oder Löschung von Daten implementieren bzw. vorsehen!

Grundsätze der DSGVO

Integrität und Vertraulichkeit, Art. 5 Abs. 1 lit. f) DSGVO

- Personenbezogene Daten müssen so verarbeitet werden, dass eine angemessene Sicherheit der Daten gewährleistet ist
- Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust und unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen
- Grundsatz wird in Art. 32 (Datensicherheit) und Art. 33, 34 (Melde- und Benachrichtigungspflichten) konkretisiert

Grundsätze der DSGVO

Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO

- Der für die Verarbeitung Verantwortliche ist für die Einhaltung der Grundsätze aus Art. 5 Abs. 1 verantwortlich und muss deren Einhaltung nachweisen können
- Dies ist eine wesentliche Änderung gegenüber der bisherigen Rechtslage
- Wird durch Art. 24 Abs. 1 Satz 1 ergänzt (Verantwortlicher muss auch den Nachweis dafür bringen können, dass er personenbezogene Daten in Übereinstimmung mit der Verordnung verarbeitet)

Unternehmen müssen nicht nur sicherstellen, die einzelnen Anforderungen der DSGVO zu erfüllen, sondern dies auch nachweisen können. Dies führt zu erheblichen Dokumentations- und Nachweispflichten, welche bei der Planung von Prozessen und Strukturen unbedingt zu beachten sind.

Erlaubnistatbestände der DSGVO

Einwilligung der betroffenen Person, Art. 6 Abs. 1 lit. a) DSGVO

- Anforderungen an eine wirksame Einwilligung sind in Art. 7 und Art. 8 geregelt
- Verantwortlicher muss nach Art. 7 Abs. 1 nachweisen können, dass die betroffene Person wirksam eingewilligt hat

Erlaubnistatbestände der DSGVO

Erfüllung eines Vertrages mit der betroffenen Person, Art. 6 Abs. 1 lit. b) DSGVO

- Verarbeitung zum Zweck der Erfüllung eines Vertrages
- Verarbeitung zum Zweck der Durchführung vorvertraglicher Maßnahmen auf Antrag der betroffenen Person
- Grundsätze aus Art. 5 müssen beachtet werden:
 - Zweckfestlegung (Erfüllung eines Vertrages)
 - Transparenz (Betroffener muss erkennen, für welche vertraglichen Zwecke und in welcher Weise)
 - Verhältnismäßigkeit (Interessenabwägung mit Grundrechten der betroffenen Person)
 - Datenminimierung (auf das für den Zweck notwendige Maß beschränkt)
 - Richtigkeit (Daten müssen richtig und auf dem neusten Stand sein)
 - Speicherbegrenzung (Daten dürfen nur solange gespeichert werden, wie dies für die Verwirklichung der vertraglichen Zwecke, für die sie verarbeitet werden, erforderlich ist)
 - Dokumentation (Überlegungen und Maßnahmen sollten vom Verantwortlichen dokumentiert werden)

Erlaubnistatbestände der DSGVO

Wahrung berechtigter Interessen, Art. 6 Abs. 1 lit. f) DSGVO

- Abwägung zwischen Interessen des Verantwortlichen und Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person
- Umfassende Abwägung der Umstände, die jeweils für oder gegen eine Datenverarbeitung sprechen
- Bei der Abwägung sind „die vernünftigen Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, zu berücksichtigen“
- Kann die betroffene Person absehen, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird?

Betroffene Personen sollten deshalb umfassend über die geplanten Datenverarbeitungen informiert werden. Je transparenter die Information gegenüber dem Betroffenen, desto eher wird eine Interessenabwägung zu Gunsten der Datenverarbeitung ausgehen.

Hinweis: Erwägungsgrund (47) - *„Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“*

Pflichten aus der DSGVO

Informationspflichten bei Datenerhebung, Art. 13, 14 DSGVO

- Informationspflichten sind deutlich umfassender als bisher
- Betroffener muss „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache“ unterrichtet werden, Art. 12 Abs. 1
- Für Datenerhebung beim Betroffenen selbst ergeben sich die Informationspflichten aus Art. 13
- Für Datenerhebung bei Dritten ergeben sich die Informationspflichten aus Art. 14

Die ordnungsgemäße Erfüllung der Informationspflichten sollte unbedingt sichergestellt werden, da dies für die Aufsichtsbehörden ohne großen Aufwand überprüft werden kann. Auch hier drohen hohe Bußgelder!

Pflichten aus der DSGVO

Datenerhebung beim Betroffenen, Art. 13 DSGVO

- Die folgenden Informationen muss der Verantwortliche der betroffenen Person **zum Zeitpunkt der Erhebung der Daten** mitteilen:
 - **Kontaktdaten**
 - **Zwecke und Rechtsgrundlage**
 - **Berechtigte Interessen**
 - **Empfänger**
 - **Übermittlung in Drittländer**
 - **Dauer der Speicherung**
 - **Betroffenenrechte**
 - **Hintergründe der Bereitstellung**
 - **Automatisierte Entscheidungsfindung**

Pflicht entfällt, wenn und soweit die betroffene Person bereits über die Informationen verfügt!

Pflichten aus der DSGVO

Datenerhebung bei Dritten, Art. 14 DSGVO

- Die folgenden Informationen muss der Verantwortliche der betroffenen Person mitteilen:
 - **Kontaktdaten**
 - **Zwecke und Rechtsgrundlage**
 - **Kategorien personenbezogener Daten**
 - **Empfänger**
 - **Übermittlung in Drittländer**
 - **Dauer der Speicherung**
 - **Berechtigte Interessen**
 - **Betroffenenrechte**
 - **Herkunft der Daten**
 - **Automatisierte Entscheidungsfindung**
 - **Zweckänderung**

Pflicht entfällt, wenn und soweit die betroffene Person bereits über die Informationen verfügt!

Pflichten aus der DSGVO

Datenerhebung bei Dritten, Art. 14 DSGVO

- Zeitpunkt der Erteilung der Informationen:
 - Innerhalb einer der Verarbeitung angemessenen Frist, längstens jedoch innerhalb eines Monats
 - Für den Fall, dass die personenbezogenen Daten zur **Kommunikation mit der betroffenen Person** verwendet werden sollen, müssen die Informationen spätestens mit der ersten Mitteilung an die Person erfolgen
 - Ist eine **Offenlegung an einen anderen Empfänger** beabsichtigt, müssen die Informationen spätestens zum Zeitpunkt der ersten Offenlegung erteilt sein

BREHM & v.MOERS

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Kai Bodensiek
Rechtsanwalt

Brehm & v. Moers Rechtsanwälte PartG mbB
Anna-Louisa-Karsch-Str. 2
Spreepalais am Dom
10178 Berlin

Tel.: 030-2693 95 0
Fax.: 030-2693 95 15
Kai.bodensiek@bvm-law.de
www.bvm-law.de