

DATENSCHUTZGRUNDVERORDNUNG

was wird neu?

CARSTEN J DIERCKS
RECHTSANWALT

Carsten J. Diercks

Rechtsanwalt

Chief Legal Advisor bei Miller & Meier Consulting Berlin

Mitglied des Rednerdienstes TEAM EUROPE der Europäischen Kommission

CARSTEN J DIERCKS
RECHTSANWALT

25.05.2018

DSGVO

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)

DSGVO

Harmonisierung der Datenschutzbestimmungen in der EU

Datenschutz gilt für alle Marktteilnehmer

Setzung internationaler Standards

DSGVO

(+BDSG +LDSG +TMG +TKG)

DATENSCHUTZ

Abwägung des Grundrechts auf informationelle Selbstbestimmung mit anderen Interessen

Schutz der Daten aller natürlichen Personen
(personenbezogene Daten)

generelles Verbot der Datenverarbeitung mit Erlaubnisvorbehalt

DSGVO

je automatisierte Verarbeitung oder Verarbeitung zur elektronischen Speicherung

Ausnahmen:

Verarbeitung durch natürliche Personen zu persönlichen oder familiären Zwecken

Verarbeitung durch Behörden zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten

Verarbeitung im Rahmen der Richtlinie über den elektronischen Geschäftsverkehr (RL 2000/31/EG und 2011/83/EU): Dienstanbieter bei Durchleitung von Informationen, Zwischenspeicherung, Host-Provider mit Haftungsprivilegien und ohne Überwachungspflicht

DSGVO

räumliche Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet
(EU-Niederlassung)

Verarbeitung von Daten von EU-Aufhäftigen, durch nicht in der EU ansässigen Verantwortlichen oder Auftragsverarbeiter im Zusammenhang mit Vertrieb von Waren und Dienstleistungen in EU oder Beobachtung von Verhalten (Nicht-EU-Niederlassung)

diplomatische und konsularische Vertretungen der EU und ihrer Mitgliedsstaaten

DSGVO

Terminologie: Art. 4 enthält die wichtigsten Definitionen
weitgehend gleich wie vorher, aber auch einige Neuerungen

DSGVO

Verfahrensvereinfachung und einheitliche Rechtsanwendung

One-Stop-Shop-Mechanismus

Kohärenzverfahren

DSGVO

Grundsätze neu formuliert

Artikel 5 DSGVO

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

- a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“);
- b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („**Zweckbindung**“);
- c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“);
- d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („**Richtigkeit**“);
- e) 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; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („**Speicherbegrenzung**“);
- f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).

DSGVO

Voraussetzungen der Rechtmäßigkeit der Datenverarbeitung:
Einwilligung oder Recht

Alte, rechtswirksame Einwilligungen gelten fort (Beschluss Düsseldorfer Kreis 14.09.2016).

Artikel 6 DSGVO

Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn **mindestens eine** der nachstehenden Bedingungen erfüllt ist:

- . a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- . b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung **vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- . c) die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
- . d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen der betroffenen Person** oder **einer anderen natürlichen Person** zu schützen;
- . e) die Verarbeitung ist für die **Wahrnehmung** einer Aufgabe erforderlich, die **im öffentlichen Interesse liegt** oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- . f) die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten** erforderlich, **sofern nicht** die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

Artikel 13 DSGVO

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- a) den Namen und die Kontaktdaten des **Verantwortlichen** sowie gegebenenfalls seines Vertreters;
- b) gegebenenfalls die Kontaktdaten des **Datenschutzbeauftragten**;
- c) die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- e) gegebenenfalls die **Empfänger** oder Kategorien von Empfängern der personenbezogenen Daten und
- f) gegebenenfalls die **Absicht** des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

- . a) die **Dauer**, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- . b) das Bestehen eines **Rechts auf Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- . c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu **widerrufen**, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- . d) das Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde;
- . e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen **Vertragsabschluss** erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
- . f) das Bestehen einer **automatisierten Entscheidungsfindung** einschließlich **Profiling** gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen **anderen Zweck** weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

(4) Beruht die Verarbeitung **zu einem anderen Zweck** als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, **nicht auf der Einwilligung der betroffenen Person** oder **auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten**, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

- . a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- . b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- . c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
- . d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- . e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

DSGVO

personenbezogene Daten

besondere Kategorien personenbezogener Daten:

rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit sowie genetische Daten, biometrische Daten zu eindeutiger Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung

DSGVO

CARSTEN J DIERCKS
RECHTSANWALT

Betroffenenrechte:

präzise, transparente, verständliche und leicht zugängliche Information in verständlicher Sprache

Pflicht zur Information bei Erhebung, an Betroffenen bei anderweitiger Erhebung, bei Zweckänderung,

Recht auf Auskunft,

Recht auf Berichtigung,

Recht auf Löschung „Recht auf Vergessenwerden“

Recht auf Einschränkung der Verarbeitung (Sperrung)

Recht auf Datenübertragbarkeit

Widerspruchsrecht bei besonderer Situation in Fällen der Verarbeitung in öff. Interesse oder bei Abwägung,

Profiling, ferner Direktwerbung

Grundsätzliches Verbot automatisierter Entscheidungen im Einzelfall, es sei denn Einwilligung, Vertrag oder Gesetz

Mitgliedsstaaten können unter definierten Voraussetzungen diese Rechte beschränken.

DSGVO

stärkere Verantwortlichkeit der Organisation für die Einhaltung aller Rechtsgrundsätze

Beweislastumkehr: Verantwortlicher muss Datenschutzkonformität aktiv nachweisen können

Dokumentationspflichten, technische und organisatorische Maßnahmen erforderlich

DSGVO

Verantwortlichkeit des für die Verarbeitung Verantwortlichen

Auftragsverarbeiter

Verzeichnis von Verarbeitungstätigkeiten bei Verantwortlichen mit mehr als 250 Mitarbeitern

DSGVO

Verzeichnis der Verarbeitungstätigkeiten

Datenschutz-Folgenabschätzung

DSGVO

Privacy by Design

Privacy by Default

Verpflichtung auf Datensicherheit

DSGVO

Meldung von Datenschutzverletzungen

Datenschutzbeauftragter

Stärkung der Selbstregulierung durch Zertifizierung und Verhaltensregeln

präzise Vorgaben für verbindliche interne Datenschutzvorschriften

DSGVO

konzerninterne Datenweitergabe

Übermittlung personenbezogener Daten in Drittländer

Privacy Shield Beschluss

DSGVO

Cloud Computing

Big Data

Profiling, Scoring und Screening

DSGVO

Was tun bis 28.05.2018?

Bestandsanalyse, GAP-Analyse, Organisation, Anpassung von rechtlichen
Dokumente und Prozessen, Schulung

CARSTEN J DIERCKS
RECHTSANWALT

Danke für die Aufmerksamkeit