DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

INHALT

Die Datenschutz-Grundverordnung – Ein erster Überblick für Sie

– Neues Datenschutzrecht und was Sie schon jetzt tun müssen

Am 25.05.2016 ist die EU-Datenschutz-Grundverordnung (DS-GVO) in Kraft getreten. Die DS-GVO gestaltet den Datenschutz in Deutschland grundlegend neu.

Die Zeitspanne bis zu ihrem Geltungsbeginn am 25.05.2018 muss daher dazu genutzt werden, die Verarbeitung personenbezogener Daten an diesen neuen Vorgaben auszurichten – so sieht es die DS-GVO vor.

1. Für welche Fälle gelten die Neuregelungen?

Für die DS-GVO ist – wie auch bereits jetzt – entscheidend, ob personenbezogene Daten verarbeitet werden. Die DS-GVO gilt für alle Informationen, die auf einen Menschen beziehbar sind. Nicht geschützt sind Daten über juristische Personen als solche (z. B. GmbH, AG, eG). Anders als im Verbraucherschutz oder Wettbewerbsrecht kommt es nicht darauf an, ob dies Gewerbetreibende, Verbraucher oder Privatpersonen sind – alle Menschen sind geschützt. Das gilt offensichtlich für Privatpersonen als Kunden und Beschäftigte, aber typischerweise gilt das auch für sonstige Kunden, Lieferanten und Beteiligte an Geschäftsbeziehungen. Denn selbst wenn es sich bei dem Vertragspartner um eine juristische Person handelt, werden typischerweise auch hier Daten von Menschen (Ansprechpartner, Geschäftsführer, etc.) gespeichert.

Gerade Online-Themen wie Cookies und IP-Adressen hat die DS-GVO im Focus. Ausgenommen sind hingegen reine Maschinendaten, was gerade im Rahmen von Industrie 4.0 relevant ist. Zuweilen wird aber übersehen, dass auch für diese Daten das Datenschutzrecht gilt, wenn mittelbar auch eine Aussage über einen Menschen getroffen wird (z. B. die Begleitperson der Maschine). Und BigData kommt nie an einer Datenschutzprüfung vorbei. Gerade Online-Themen und neuen Verfahren, aber auch etablierten Datenverarbeitungen zeigt der Datenschutz Grenzen auf. Es ist daher von besonderer Bedeutung, den Anwendungsbereich zu prüfen und alternative Gestaltungen zu identifizieren und zu bewerten.

Im Ergebnis gibt es kaum einen Bereich des Unternehmens, den der Datenschutz nicht erfasst.

2. Diese Konsequenzen hat das Datenschutzrecht

Personenbezogene Daten dürfen nur verarbeitet werden, wenn entweder die Einwilligung des Betroffenen vorliegt oder eine gesetzliche Regelung die Verarbeitung gestattet (Verbot mit Erlaubnisvorbehalt). Das bedeutet: Jeder Umgang mit personenbezogenen Daten ist unzulässig, wenn der Datenverarbeiter nicht die Zulässigkeit begründen und beweisen kann. Das ist bereits jetzt so und wird sich unter der DS-GVO nicht ändern. Die Änderungen werden später unter der Überschrift „Was zulässig ist, bleibt nicht automatisch zulässig!" vertieft.

Das Datenschutzrecht fordert als wesentlichen Grundsatz die Transparenz der Datenverarbeitung gegenüber dem Betroffenen. Kurzum: Es ist durch proaktive Unterrichtung sicherzustellen, dass der Betroffene jederzeit weiß, wer was mit welchen seiner Daten zu welchem Zweck tut. Während dies nach bisherigem Recht ausreichend war, erweitert die DS-GVO diese Transparenzpflicht erheblich. Dies geht so weit, dass zukünftig dem Betroffenen u. a. die Rechtsgrundlage der Datenverarbeitung und das berechtigte Interesse an der Verarbeitung benannt werden müssen.

In Bezug auf die proaktive Unterrichtung der Betroffene sind umfassende Anpassungen erforderlich. Denn Verstöße gegen diese Vorgaben sind offensichtlich und damit leicht angreifbar.

Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie rechtmäßig erhoben wurden. Sollen sie für einen anderen Zweck verwendet werden, muss wieder die Zulässigkeit für diesen Zweck – also Einwilligung oder gesetzliche Zulässigkeit – geprüft werden. Der Grundsatz der Zweckbindung besagt also: Auch bereits (rechtmäßig) erhobene Daten dürfen nicht beliebig weiterverarbeitet werden.

Der Grundsatz der Datensparsamkeit und -vermeidung fordert, dass nur Daten erhoben und verwendet werden, die wirklich für den Zweck erforderlich sind, und die Abläufe und Systeme so gestaltet sind, dass dies sichergestellt ist. Gerade dies wird für Aufwand sorgen. Denn bisher wurde dieser Grundsatz – mangels Bußgeldbewehrung – stiefmütterlich behandelt. Unter der DS-GVO sind auch Verstöße gegen den Grundsatz der Datensparsamkeit und -vermeidung mit bis EURO 20 Mio. bußgeldbewehrt und der Datenverarbeiter ist rechenschaftspflichtig in Bezug auf die Umsetzung dieses Grundsatzes.

3. Warum Ihr Unternehmen die Umstellung nicht verpassen darf!

Der beschriebene Anwendungsbereich ist nicht neu. Im Wesentlichen gilt das heute schon im deutschen Datenschutzrecht, was dazu verleitet, nach dem Prinzip „weiter so" die Datenschutz-Grundverordnung zu vernachlässigen. Neu ist allerdings das Aufdeckungs- und Sanktionsrisiko bei Verstößen. Denn die DS-GVO verschärft nicht nur die Bußgelder für Verstöße drastisch, sondern sieht weitere Anforderungen vor.

Der Bußgeldrahmen wird durch die DS-GVO um etwa den Faktor 60 erhöht und beträgt jedenfalls 10 Mio. und 20 Mio. EURO je nach Verstoß.

Das führt zwangsläufig zu signifikant höheren Bußgeldern. Denn ein zu verhängendes Bußgeld muss sich am Bußgeldrahmen ausrichten. Gleichzeitig ist absehbar, dass unter der DS-GVO auch deutlich mehr Bußgelder als bisher verhängt werden. Denn der Gesetzgeber fordert tatsächliche Sanktionen im Fall einer normierten Bußgeldandrohung. Die aktuelle Diskussion geht so weit, dass die Frage im Raum steht, ob die Aufsichtsbehörden überhaupt noch – wie bisher – von Bußgeldern absehen dürfen, wenn ein Bußgeld rechtlich möglich ist (Stichwort: Pflicht zur Sanktion). Auch die Datenschutzaufsichtsbehörden schließen in Zukunft deutlich mehr und höhere Bußgelder nicht aus.

Die Pflichten, deren Missachtung zu einem Bußgeld führt, werden durch die Datenschutz-Grundverordnung erweitert. Gerade Pflichten, die bisher nicht bußgeldbewehrt waren, laufen Gefahr, durch ein „weiter so" zur Falle zu werden.

4. Weitere Verschärfungen durch die DS-GVO

Diese zukünftige Bußgeldpraxis ist aber nur ein Aspekt der Verschärfung des Drucks zur Einhaltung des Datenschutzes. Die DS-GVO dreht auch an anderen Stellschrauben, die zur Aufdeckung von Verstößen führen. Das sind insbesondere Folgende:

- **Umfassende proaktive Informationspflichten:**
  Derjenige, dessen Daten verwendet werden, ist zukünftig viel umfassender proaktiv (!) über den Umgang mit seinen Daten zu informieren. Dabei muss ihm in bestimmten Fällen auch die Rechtsgrundlage genannt werden, welche zur Datenerhebung berechtigt. Das ist nur möglich, wenn der Datenverarbeiter diese davor ermittelt und geprüft hat.
- **Erweiterung der Aufdeckung von Datenpannen:**
  Kommt es zu einer Datenpanne – sprich insbesondere Verlust, Offenlegung der Daten oder Fremdzugriff – sind die Aufsichtsbehörde und der Betroffene zukünftig in deutlich mehr Konstellationen als bisher zu informieren. Diese Meldung hat innerhalb weniger Tage zu erfolgen. Das Unterlassen der Benachrichtigung ist für sich genommen wieder bußgeldbewehrt.
- **Pflicht zur Abstimmung mit der Aufsichtsbehörde:**
  Bei risikobehafteten Datenverarbeitungen muss eine Folgenabschätzung durchgeführt werden und gegebenenfalls sogar zwingend die Datenschutzaufsichtsbehörde zur geplanten Datenverarbeitung befragt werden.
- **Erweiterung der Haftung:**
  Für Dienstleister wird die Haftung auf Schadensersatz verschärft. Bildlich gesprochen sitzt er zukünftig mit dem Auftraggeber in einem Boot, wenn es um die Haftung geht. Hier werden klare vertragliche Regelungen zur Haftungsbegrenzung erforderlich.
- **Neue Betroffenenrechte:**
  Auskünfte sind den Betroffenen zukünftig unverzüglich – jedenfalls binnen eines Monats – zu erteilen. Hinzukommen das Recht auf Datenportabilität sowie das Recht auf Vergessenwerden. Bei Missachtung der Rechte der Betroffenen drohen Bußgelder.
- **Pflicht zur Organisation:**
  Die Datenschutz-Grundverordnung zwingt in mehreren Bereichen dazu, Organisationsstrukturen – bspw. zur Erfüllung der Rechte der Betroffenen – aufzubauen. Allein das Fehlen einer solchen Organisationsstruktur führt zum Verstoß. Der Aufbau solcher Strukturen ist eine Managementaufgabe.
- **Rechenschaftspflicht:**
  Die Datenschutz-Grundverordnung definiert explizit einen umfassenden und facettenreichen Katalog von Grundsätzen, für deren Einhaltung das Unternehmen – anders als bisher – isoliert rechenschaftspflichtig ist. Das bedeutet, dass nicht nur die Einhaltung des Datenschutzrechts im Einzelfall geprüft wird, sondern dass durch die Rechenschaftspflicht die Datenschutz-Compliance in das „organisatorische Vorfeld" verlagert wird.
- **Grenzüberschreitender Datentransfer:**
  Auch der grenzüberschreitende Datenverkehr wird neu gestaltet. Aufgrund der öffentlichkeitswirksamen Diskussion um Safe Harbor und das EU-US-Privacy Shield ist dieses Thema im Fokus der Betroffenen, der Aufsichtsbehörden und der Öffentlichkeit. Insbesondere beim Einsatz von IT-Lösungen von Dienstleistern – und nicht nur beim Cloud-Computing – sowie beim Datentransfer im Unternehmensverbund stellen sich neue Fragen.

- **Aufklärung von Fehlverhalten:**
  Die Aufklärung interner Pflichtverstöße muss sich an datenschutzrechtlichen Vorgaben messen lassen. Auch Compliance-Strukturen im Unternehmen und die interne Aufklärung von Vorfällen im Unternehmen müssen sich – wie sie auch jüngst aus der Presse bekannt geworden sind – dem Datenschutzrecht stellen. Soweit solche Pflichten aufgrund gesetzlicher Vorgaben vorgeschrieben oder durch Selbstverpflichtungen auferlegt sind (bspw. Whistleblowing), müssen diese im Licht der Datenschutz-Grundverordnung neu bewertet werden. Ihre Datenschutzkonformität muss auch nach dem Inkrafttreten der DS-GVO sichergestellt sein.
- **Datenschutz-Compliance als Vorgabe von Auftraggebern und Lieferanten:**
  Zunehmend sehen Verträge und vor allem Kooperationsverträge im Unternehmensalltag vor, dass sich ein Auftragnehmer vertraglich zur Einhaltung des Datenschutzes verpflichtet. Die fehlende Umsetzung der Vorgaben der Datenschutz-Grundverordnung führt dann zusätzlich auch zur Verletzung dieser Vertragspflicht.

5. Bußgelder, Abmahnung und Verbandsklage

Neben Bußgeldern besteht die Gefahr von wettbewerbsrechtlichen Abmahnungen. Denn Ende 2015 wurde ein Verbandsklagerecht für Datenschutzverstöße eingeführt. Die DS-GVO wird weitere Klagemöglichkeiten vorsehen.

6. Was zulässig ist, bleibt nicht automatisch zulässig!

Auch die Rechtsgrundlage für die Datenverarbeitung wird durch die DS-GVO grundlegend neu geregelt.

Einwilligungen in die Datenverarbeitung sind nach dem 25.05.2018 nur noch wirksam, wenn sie den Anforderungen der DS-GVO entsprechen.

Erfolgt also keine Überprüfung und erforderlichenfalls Umstellung auf die neuen Anforderungen, besteht die Gefahr, dass die Einwilligung als Rechtsgrundlage für die Datenverarbeitung entfällt.

Unter dem heutigen Recht wird zum Teil darauf abgestellt, dass Betriebsvereinbarungen im Datenschutzrecht eine rechtfertigende Grundlage sind. Dies ist aber umstritten. Die DS-GVO bezieht die Betriebsvereinbarung nicht (explizit) als Rechtfertigung der Datenverarbeitung ein. Hier besteht in jedem Fall Handlungsbedarf!

Die gesetzlichen Zulässigkeitsregelungen ändern sich grundlegend. Um es vorweg zu nehmen: Das bedeutet nicht, dass alles bisher Zulässige in Bausch und Bogen unzulässig wird. Aber es bedeutet gleichwohl: Eine Prüfung aller Verarbeitungen personenbezogener Daten anhand der DS-GVO ist erforderlich, um die Datenschutz-Compliance sicherzustellen. Gerade bei lebenswichtigen Datenverarbeitungen des Unternehmens ist das Risiko der Unklarheit nicht hinnehmbar und stellt ein Haftungsrisiko des Managements dar.

Auf den ersten Blick wird deutlich, dass dies Auswirkungen auf das Marketing hat, aber auch auf jedes Scoring und Profiling, auf die Meldung an und die Abfrage von Informationen aus Auskunfteien, die Verarbeitung von Beschäftigtendaten, die Videoüberwachung. Das ist aber nur der erste Blick – letztlich müssen die Verfahrensabläufe in jedem Unternehmensbereich anhand der neuen Rechtslage auf ihre Rechtmäßigkeit geprüft werden.

Entscheidend ist, diese Prüfung vor Geltungsbeginn der Neuregelung durchzuführen! Nur durch eine rechtzeitige Prüfung können die Rechtmäßigkeit der Datenverarbeitung sichergestellt und Sanktionen vermieden werden.

Das bedeutet:

- Bereits stattfindende Datenverarbeitungen müssen anhand der Datenschutz-Grundverordnung auf ihre Zulässigkeit geprüft und gegebenenfalls angepasst werden.
- Neu anstehende und umzugestaltende Datenverarbeitungen sollten bereits jetzt an den Vorgaben der Datenschutz-Grundverordnung ausgerichtet werden, um diese nicht zwei Mal prüfen zu müssen.
- Aufgrund der umfassenden Erweiterungen der Informationspflichten gegenüber Betroffenen müssen für bestehende und zukünftige Datenerhebungen und –verarbeitungen die Vorbereitungen zur Erfüllung der Informationspflichten geschaffen werden.

7. Kein Bestandsschutz!

Einen Bestandsschutz, dass alte Datenverarbeitungen nach altem Recht fortgesetzt werden dürfen, gibt es nicht! Um es deutlich zu sagen: Auch bereits stattfindende Datenverarbeitungen sind zukünftig nur noch datenschutzkonform, wenn sie den Anforderungen der Datenschutz-Grundverordnung entsprechen.

Auch für bereits begonnene und nur fortgesetzte Datenverarbeitungen kann nach der Maßgabe der Datenschutz-Grundverordnung ein Bußgeld verhängt werden.

Der EU-Gesetzgeber sieht daher die Übergangsfrist von Inkrafttreten (25.05.2016) bis zur Geltung (25.05.2018) zur Anpassung vor.

Um künftig die Datenschutz-Compliance sicherzustellen, müssen die Datenverarbeitungen an der Datenschutz-Grundverordnung ausgerichtet werden. Die Verantwortung hierfür liegt nach der DS-GVO beim Management.

8. In der Gesamtschau

Das ist nur ein Ausschnitt der Neuerungen. Die DS-GVO zwingt dazu, die gesamte Verarbeitung personenbezogener Daten bis zum 25.05.2018 auf den Prüfstand zu stellen und die Datenschutzorganisation im Unternehmen neu auszurichten.

Ab dem 25.05.2018 ist nur noch die Verarbeitung personenbezogener Daten zulässig, die der DS-GVO entspricht! Die DS-GVO regelt praktisch jeden Bereich der Verarbeitung personenbezogener Daten im Detail neu.

Das Risiko besteht dabei darin, dass dies auf den ersten Blick nicht auffällt. Denn viele Prinzipien des bisherigen Datenschutzes werden fortgesetzt – aber in neuer Gestalt und mit neuen Anforderungen.

Auch bei Verstößen durch bereits begonnene Datenverarbeitungen gilt der Bußgeldrahmen der DS-GVO!

9. Was jetzt getan werden muss!

2 Jahre sind kurz für die Neu-Ausrichtung der gesamten Verarbeitung personenbezogener Daten an einer neuen Rechtsordnung!

Wie gehen Sie es an?

- In einem ersten Schritt müssen Sie sich die neuen Anforderungen für Ihr Unternehmen verdeutlichen. Diese sind je nach Unternehmen unterschiedlich.
- In einem zweiten Schritt vergleichen Sie die Anforderungen mit dem Ist-Zustand im Unternehmen.
- Im dritten Schritt sind die Abläufe an die DS-GVO anzupassen. Achten Sie auch auf die Zeitschiene – nicht alle Anpassungen sind gleich schnell möglich. Setzen Sie dabei Prioritäten auf „lebenswichtige" Bereiche des Unternehmens.

Sprechen Sie uns an!

Wir unterstützen Sie in jeder dieser Phasen zur Ausrichtung Ihrer Datenverarbeitung an den neuen Anforderungen, damit in Ihrem Unternehmen auch in Zukunft die Datenschutz-Compliance gewährleistet ist. Wir bieten Ihnen unternehmensindividuelle Seminare und Workshops zur Einarbeitung

in die neuen Anforderungen, wir unterstützen bei der Erfassung des Ist-Zustands und der Analyse der für Ihr Unternehmen relevanten neuen Vorgaben. Wir begleiten Ihr Unternehmen bei der Umsetzung der Vorgaben der Datenschutz-Grundverordnung.

Natürlich stehen wir Ihnen und Ihrem Unternehmen auch fallbezogen für Fragen des aktuellen und zukünftigen Datenschutzrechts oder zu sonstigen Unternehmungen zur Seite – sei es beim Outsourcing, der datenschutzkonformen Beauftragung von Dienstleistern und beim Beschäftigten-Datenschutz oder sei es bei der Einführung von IT-Systemen und Cloud-Anwendungen. Gleiches gilt für die Aufklärung oder Prävention von Taten zum Nachteil des Unternehmens oder die Gestaltung einer rechtskonformen Nutzung von E-Mail und Internet am Arbeitsplatz sowie das Direkt- und Online-Marketing.

ABONNEMENT:
Möchten Sie unseren Newsletter regelmäßig erhalten – dann melden Sie sich bitte an unter:
witten-violetti@derra-d.de

IMPRESSUM:
Herausgegeben von
Derra, Meyer & Partner
Rechtsanwälte PartGmbB
Frauenstraße 14, 89073 Ulm
Tel. +49 731 922880, Fax +49 731 92288 88
www.derra.eu

Redaktion:
Rechtsanwältin Ruth Witten-Violetti

ANSPRECHPARTNER UND AUTOR DES NEWSLETTERS:
Rechtsanwalt Dr. Jens Eckhardt

BILDNACHWEIS:
Folgende Bilder entstammen fotolia.com:
fotolia_88738373: © Sergey Nivens
fotolia_77461865: © pict rider
fotolia_66316242: © Gajus
fotolia_64056386: © Imillian
fotolia_103886307: © ra2 studio

Rechtsanwalt Dr. Jens Eckhardt

Fachanwalt für Informationstechnologierecht und Datenschutz-Auditor (TÜV)
Derra, Meyer & Partner – www.derra.eu – eckhardt@derra-d.de

Seit 2001 berät er bundesweit nationale und internationale Unternehmen zu den Themen Datenschutz, Informationstechnologie, Telekommunikation und Marketing. Die Beratung umfasst die gerichtliche Vertretung, Vertretung gegenüber Aufsichtsbehörden, insbesondere im Datenschutz, die strategische Beratung bei der Einführung neuer System, die Bewertung von bestehenden Systemen, das Outsourcing sowie die Vertragsgestaltung.

Funktionen als

- Mitglied im **Vorstand von EuroCloud Deutschland_eco e.V.** (Ressort Recht)
- Mitglied im **Vorstand des Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.** (Ressort Recht)
- **Dozent zum Datenschutzrecht der udis Ulmer Akademie für Datenschutz und IT-Sicherheit** – gemeinnützige Gesellschaft mbH
- **Dozent der DeutscheAnwaltAkademie** Gesellschaft für Aus- und Fortbildung sowie Serviceleistungen mbH (Fortbildung im Bereich Fachanwalt IT-Recht und im Datenschutzrecht)
- **Lehrbeauftragter** der SRH Fernhochschule Riedlingen **zum Internet- und Medienrecht und Datenschutz** im Studiengang Medien und Kommunikation
- **Anhörung durch die Datenschutzaufsichtsbehörden als Fachexperte** für Werbung und Adresshandel
- **Moderator und Referent** verschiedener Datenschutzveranstaltungen und **Autor von Fachbeiträgen** zum **Datenschutz-, IT-, Zivil- und Wettbewerbsrecht**

Auswahl der Veröffentlichungen:

- **Beck'scher TKG Kommentar,** Mitautor, seit 4. Aufl. 2013, Verlag C. H. Beck München
- **Recht der elektronischen Medien,** Kommentar, Mitautor seit 1. Aufl., Verlag C. H. Beck München
- **Handbuch IT- und Datenschutzrecht,** Mitautor, seit 1. Aufl., Verlag C. H. Beck München
- **Digitalisierung und Transformation im Unternehmen,** Mitautor, KS-Energy-Verlag
- **Datenschutz und Marketing** – Praxisleitfaden für Datenschutzbeauftragte und Geschäftsleitung, TKMmed!a,
- **Datenschutz-Aktuell – Spezialreport zur EU-DSGVO**, TKMmed!a
- **Big Data im Marketing** – Chancen und Möglichkeiten für eine effektive Kundenansprache, 2015, Mitautor, Haufe Gruppe
- **„Wann ist ein Datum ein personenbezogenes Datum?"**, gemeinsam mit Dr. Brink (Landesbeauftragter für den Datenschutz Baden-Württemberg), ZD Editorial 1/2015 und ZD 2015, 205 ff.
- **Leitfaden – Datenschutz und Cloud Computing**, Mitautor und Leiter der Taskforce „Datenschutz" der AG „Rechtsrahmen im Cloud Computing", Trusted Cloud-Initiative des BMWi