entwickler.press

Die DSGVO verstehen und anwenden

Datenschutzkompetenz für Unternehmen

Michael Rohrlich

Michael Rohrlich

Die DSGVO verstehen und anwenden

Datenschutzkompetenz für Unternehmen

entwickler.press

Michael Rohrlich
Die DSGVO verstehen und anwenden. Datenschutzkompetenz für Unternehmen

ISBN 978-3-86802-366-4

Ein Imprint der Software & Support Media GmbH

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Ihr Kontakt zum Verlag und Lektorat:
Software & Support Media GmbH
entwickler.press
Schwedlerstraße 8
60314 Frankfurt am Main
Tel.: +49 (0)69 630089-0
Fax: +49 (0)69 630089-89
lektorat@entwickler-press.de
http://www.entwickler-press.de

Lektorat/Korrektorat: Frauke Pesch, Jonas Bergmeister
Proofreader: Nicole Bechtel
Satz: Sibel Sarli
Umschlaggestaltung: Maria Rudi
Titelbild: ©NothingIsEverything/Shutterstock.com, ©S&S Media

Inhaltsverzeichnis

Vorwort

EU-Datenschutz-Grundverordnung oder kurz: DSGVO: für viele das Unwort des Jahres. Mit diesem Regelwerk gibt der europäische Gesetzgeber allen Unternehmen in Europa – und auch über die EU-Grenzen hinaus – einen umfangreichen Anforderungskatalog an die Hand, der den einen oder anderen schier verzweifeln lässt. Auf den ersten Blick kommen nur noch mehr bürokratische Hürden auf unternehmerisch Tätige zu. Betrachtet man die DSGVO jedoch aus dem Blickwinkel eines Verbrauchers, ergeben sich daraus viele Rechte und Ansprüche, die es ihm in der modernen, zunehmend digitalisierten Welt ermöglichen sollen, die eigenen Grundrechte auch durchsetzen zu können.

Außerdem bringen Anforderungen, wie etwa das Beachten des aktuellen Stands der Technik, zum Teil auch positive Nebeneffekte für die Unternehmen mit sich. Denn dadurch werden letztlich alle Unternehmen dazu gezwungen, ein hohes Niveau an Datensicherheit zu gewährleisten, was unter dem Strich nicht nur dem jeweiligen Unternehmen selbst, sondern auch der Allgemeinheit zugutekommt. Je mehr Unternehmen beispielsweise auf signierte bzw. verschlüsselte E-Mail-Kommunikation setzen, desto höher das Sicherheitsniveau insgesamt. Oder das leidige Thema Verfahrensbeschreibung: Im Rahmen der Umsetzung der Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten lassen sich anhand der einzelnen Prozessbeschreibungen durchaus wertvolle Erkenntnisse für das Thema Qualitätsmanagement gewinnen. Dadurch erhält man wiederum einen neuen oder jedenfalls anderen Blick auf die Arbeitsabläufe im eigenen Unternehmen, sodass man eventuell Verbesserungspotenzial abseits der Bereiche Datenschutz und IT-Sicherheit entdeckt. Das Thema

Compliance ist ein weites Feld, das Unternehmen in vielen Bereichen zum Handeln zwingt.

In Deutschland ändert sich inhaltlich gar nicht mal so viel. Hierzulande herrschte auch vor der DSGVO schon ein sehr hohes Maß an Datenschutz. Daher hat sich die Europäische Union im Rahmen des Gesetzgebungsverfahrens auch in vielen Aspekten am deutschen Datenschutzrecht orientiert. Es gibt jedoch drei Punkte, die zusammengenommen dann doch eine gravierende Änderung mit sich bringen werden. Dabei handelt es sich um das Nachweisprinzip, die verschiedenen Dokumentationspflichten und die erheblich gestiegenen Bußgelder. Diese Neuerungen wirken beim ersten Lesen vielleicht nicht so aufregend, in der Praxis werden sie jedoch für erhöhten Arbeitsaufwand und vermutlich auch für einigen Unmut auf Seiten der Unternehmen sorgen. Das, was bisher vielleicht in der Praxis schon gelebt wurde, muss nun zusätzlich auch noch in geeigneter Weise niedergeschrieben werden, damit Unternehmen ihrer Nachweispflicht adäquat nachkommen können.

Insgesamt gibt dieses Werk einen fundierten Überblick über die zahlreichen Neuerungen, die die DSGVO mit sich bringt. Zusätzlich finden sich diverse Praxistipps, Checklisten und weiterführende Hinweise insbesondere auf Material von Datenschutzaufsichtsbehörden bzw. -verbänden. Natürlich geht es hier primär um die Vermittlung von allgemeinen Informationen, nicht um eine individuelle Rechtsberatung. Im Zweifel sollten Sie also fachmännischen Rechtsrat einholen und Unterstützung bei einem entsprechend spezialisierten Rechtsanwalt suchen. Insbesondere die praktische Umsetzung der zahlreichen Betroffenenrechte und Dokumentationspflichten dürften so manches Unternehmen vor große Herausforderungen stellen.

Ein gut gemeinter Ratschlag zum Schluss: Verschaffen Sie sich mit diesem Werk einen Überblick über die elementaren Grundlagen der DSGVO und fangen Sie anschließend gleich an, einen Plan zur Umsetzung in Ihrem Unternehmen zu erstellen. Starten Sie jetzt, nicht morgen! Und auch nach erfolgreicher Umstellung auf die DSGVO ab dem 25. Mai 2018 sollten Sie nicht die Füße hochlegen, sondern stetig

weiter an der Verbesserung von Datenschutz und IT-Sicherheit arbeiten. Denn auch das schreibt die DSGVO ausdrücklich vor: Die jeweiligen Prozesse müssen regelmäßig geprüft und gegebenenfalls an den aktuellen Stand der Technik oder an veränderte Sachlagen angepasst werden.

Rechtsanwalt Michael Rohrlich

www.ra-rohrlich.de

im März 2018

1 Einführung

Wenn Sie sich folgende Begriffe anschauen, was sagen sie Ihnen?

- DSGVO
- Compliance
- Recht auf Vergessenwerden
- Accountability
- Privacy by Design
- Privacy by Default
- Risikobasierter Ansatz
- One-Stop-Shop

Wenn Sie davon noch nichts gehört haben, dann wird es allmählich Zeit. Denn dabei handelt es sich um zentrale Begriffe des neuen europäischen Datenschutzrechts. Aber warum überhaupt Datenschutz? Weshalb ist diese Thematik in den letzten Wochen und Monaten so präsent in den Medien? Zwar herrschte in Deutschland in den letzten Jahrzehnten bereits ein vergleichsweise hohes Datenschutzniveau, mit der EU-Datenschutz-Grundverordnung (DSGVO) kommen aber dennoch gravierende Änderungen auch auf deutsche Unternehmen zu.

Und um es gleich zu Beginn deutlich zu sagen: **Die DSGVO gilt für alle europäischen Unternehmen, unabhängig von Branche, Größe, Organisationsform, Umsatz oder Mitarbeiteranzahl.** Sie gilt gleichermaßen für Behörden und Vereine. Insofern muss sie natürlich auch von Webdesignern, Programmierern und sonstigen Angehörigen der Entwicklerbranche beachtet werden.

1.1 Datenschutz als Grundrecht

Nun aber mal eins nach dem anderen. Datenschutz ist die Garantie für eine freie Entfaltung der Persönlichkeit durch den Schutz von Daten mit Personenbezug. Aus diesem Grund ist der Datenschutz in Europa auch verfassungsrechtlich verankert. Hierzulande wurde er traditionell als Ausfluss des allgemeinen Persönlichkeitsrechts gemäß Art. 1, 2 Grundgesetz (GG) betrachtet. Auch in der Europäischen Menschenrechtskonvention ist er geregelt (Art. 8 EMRK). Bislang war Datenschutzrecht allerdings eine nationale Angelegenheit, jeder Staat hatte also sein eigenes Datenschutzrecht. Innerhalb der Europäischen Union bestanden lediglich bestimmte Rahmenvorgaben, etwa durch die EU-Datenschutz-Richtlinie oder auch die sogenannte Cookie-Richtlinie sowie verschiedene Spezialnormen. Eine Richtlinie muss jedoch noch von den EU-Mitgliedsstaaten in das jeweilige nationale Recht umgesetzt werden, wobei mehr oder weniger großer Spielraum für nationale Besonderheiten besteht. Als Folge davon hatten die EU-Staaten bislang zwar ganz ähnliche Datenschutzregelungen, die aber doch noch teilweise recht große Unterschiede aufwiesen.

Hinzu kommt, wie in anderen Bereichen auch, dass die Gerichte ihrer Aufgabe der Rechtsfortbildung natürlich auch auf dem Sektor des Datenschutzrechts nachgekommen sind, und sich dadurch über die Jahre ein nicht unwesentlicher Bestand an gerichtlichen Entscheidungen angesammelt hat. Es gibt insbesondere wichtige Entscheidungen des Bundesverfassungsgerichts (BVerfG), beispielsweise zu den Themen

- Volkszählung,
- Genetischer Fingerabdruck,
- GPS-Überwachung,
- Rasterfahndung,
- Telekommunikationsüberwachung,
- Videoüberwachung auf Autobahnen,
- Videoüberwachung am Arbeitsplatz,
- E-Mail-Postgeheimnis oder auch
- Integritätsgrundrecht.

Natürlich gibt es auch zahlreiche Entscheidungen anderer Gerichte, die sich mit einzelnen Aspekten des Datenschutzrechts befasst haben, oftmals auch im Bereich des Arbeitsrechts, wenn es um den Beschäftigtendatenschutz geht.

Folgendes Zitat aus dem sogenannten „Volkszählungsurteil“[1] zeigt ganz deutlich den Stellenwert, der dem Datenschutz insbesondere in Deutschland zukommt: „Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.“

Anlass dieses Urteils war die im Jahr 1983 geplante, dann aber erst 1987 in veränderter Form durchgeführte Volkszählung in Deutschland. Die direkte Auswirkung der BVerfG-Entscheidung war die Entwicklung des Grundrechts auf informationelle Selbstbestimmung. Somit gibt es für den Bereich Datenschutz inzwischen also ein eigenes Grundrecht.

Allerdings stellen moderne Technologien, wie etwa die Möglichkeit, durch entsprechende Algorithmen riesigen Datenmengen auswerten zu können (Big Data), und der preisgünstige, nahezu unbegrenzt vorhandene Speicherplatz datenschutzrechtlich eine enorme Herausforderung dar. Nicht alles, was technisch machbar ist, darf auch in die Tat umgesetzt werden. Es muss vielmehr ein Ausgleich zwischen den Bedürfnissen der Unternehmen und dem Anspruch auf Schutz personenbezogener Daten gefunden werden. Letztlich benötigt jedes Unternehmen also ein individuelles Datenschutzkonzept.

Die **Leitlinie der Artikel-29-Gruppe (wp221)** gibt genauere Einblicke zum Thema Big Data.

1 BVerfG, Urteil vom 15.12.1983, Az. 1 BvR 209/83

1.2 Datenschutzkontrolle

Um sicherzustellen, dass das Recht auf informationelle Selbstbestimmung auch tatsächlich durchsetzbar ist, existieren Datenschutzaufsichtsbehörden sowie weitere Gremien. Warum gibt es eigentlich eine Datenschutzaufsichtsbehörde und wann wird sie tätig? In seltenen Fällen werden die Aufsichtsbehörden von sich aus aktiv und prüfen beispielsweise, ob Unternehmen auf ihrer Internetseite eine korrekte Datenschutzerklärung haben. Viel häufiger sind jedoch die Fälle, in denen der Behörde gezielte Hinweise gegeben werden. Und das geschieht nicht selten durch einen entlassenen Mitarbeiter, einen unzufriedenen Kunden oder auch durch einen Mitbewerber. Derartigen Hinweisen gehen die Behörden in aller Regel auch nach.

In Deutschland gibt es pro Bundesland einen Landesdatenschutzbeauftragten und zudem noch den Bundesdatenschutzbeauftragten, insgesamt also immerhin siebzehn Aufsichtsbehörden im Bereich Datenschutz. Wie der Name bereits vermuten lässt, üben sie die Aufsichtsfunktion für alle Unternehmen und öffentlichen Institutionen aus. Sie können aber nicht nur eine bestimmte Sanktion anordnen oder ein Bußgeld verhängen, sie haben auch den Auftrag, beratend und unterstützend tätig zu sein. Neben den Aufsichtsbehörden gibt es noch weitere Einrichtungen, die auf dem Gebiet des Datenschutzes wichtige Rollen einnehmen.

Konferenz der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten (Datenschutzkonferenz, kurz: DSK) ist eine Zusammenkunft aller Datenschutzbeauftragten des Bundes und der Länder und existiert seit Ende der 1970er Jahre. Die DSK nimmt zu unterschiedlichen Datenschutzfragen Stellung und versucht, einheitliche Anwendungshinweise dazu zu geben. Hierbei geht es etwa um Fragen der Verarbeitung von biometrischen Daten bis zur Problematik der Videoüberwachung. Es gibt verschiedene Arbeitsgruppen, in denen konkrete Lösungen für die einzelnen Problemstellungen entwickelt werden. Dies soll zu einer Vereinheitlichung und letztlich auch zu einer erhöhten Rechtssicherheit für Unternehmen und Aufsichtsbehörden gleichermaßen führen.

„Düsseldorfer Kreis"

Die Mitglieder des sogenannten „Düsseldorfer Kreises" sind im Grunde die gleichen wie die der DSK. Im Düsseldorfer Kreis werden jedoch primär Datenschutzfragen bei der Datenverarbeitung durch Unternehmen behandelt.

Europäischer Datenschutzbeauftragter

Der Europäische Datenschutzbeauftragte (EDSB) hat in erster Linie die Aufgabe, die Institutionen der Europäischen Union zu überwachen und auch zu beraten. Außerdem arbeitet er, falls notwendig, auch mit nationalen Aufsichtsbehörden zusammen, um ein möglichst einheitliches Datenschutzniveau im Bereich der EU zu gewährleisten.

Artikel-29-Datenschutzgruppe

Die bislang geltende EU-Datenschutzrichtlinie (95/46/EG) sieht in ihrem Art. 29 vor, dass eine unabhängige Gruppe mit Beratungsfunktion ins Leben gerufen werden soll. Diese sogenannte Artikel-29-Gruppe besteht aus je einem Vertreter der Datenschutzaufsichtsbehörden der einzelnen EU-Mitgliedsstaaten, einem Vertreter des EDSB sowie einem Vertreter der EU-Kommission. Ziel dieser Einrichtung ist es, konkrete Datenschutzfragen in den EU-Mitgliedsstaaten zu prüfen und dazu Stellung zu nehmen. Dadurch soll eine einheitliche Rechtsanwendung der europäischen Datenschutzvorschriften erreicht werden.

Europäischer Datenschutzausschuss

Mit Geltung der DSGVO zum 25.05.2018 tritt der Europäische Datenschutzausschuss (EDPB) als Nachfolger an die Stelle der Artikel-29-Gruppe. Gemäß Art. 68 DSGVO soll durch den neuen Ausschuss eine einheitliche Rechtsanwendung sichergestellt werden. Er soll verbindlich, aber gerichtlich überprüfbar, feststellen, wie einzelne Regelungen der DSGVO auszulegen sind. Zudem ist er für die Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren zu verschiedenen Datenschutzthemen zuständig.

1.3 Timeline DSGVO

Die Entstehungsgeschichte der DSGVO ist recht lang. Nachfolgend ein kleiner Abriss der Historie:

- **05.01.2012:** Entwurf der EU-Kommission
- **12.12.2015:** „Trilog-Fassung" (Kompromiss des EU-Parlaments, der EU-Kommission und des EU-Rates)
- **27.04.2016:** Formelle Beschlussfassung
- **04.05.2016:** Veröffentlichung im Amtsblatt
- **24.05.2016:** Inkrafttreten
- **25.05.2018:** Geltung (ohne weitere Übergangszeit!)

Von der ursprünglichen Gesetzesinitiative bis zum endgültigen Inkrafttreten hat es also über vier Jahre gedauert, die tatsächliche Wirkung entfaltet sich sogar erst über sechs Jahre später. Wichtig ist hierbei, dass es ab dem 25.05.2018 keine (!) Übergangsfrist mehr geben wird, die im Gesetz vorgesehene zweijährige Übergangsphase endet zu diesem Zeitpunkt. Rein theoretisch kann es also bereits ab dem 26.05.2018 zu ersten Prüfungen oder gar Bußgeldern durch die Aufsichtsbehörden kommen. Wie realistisch das ist und ab wann mit erhöhten Aktivitäten der Behörden gerechnet werden muss, lässt sich jetzt noch nicht sagen. Fakt ist aber, dass jedenfalls die deutschen Aufsichtsbehörden bereits seit 2017 personell massiv aufrüsten.

> Die **EU-Kommission** hat einen eigenen **Leitfaden zur DSGVO** veröffentlicht. Er kann online kostenfrei unter folgenden Link eingesehen werden: *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de.*

1.4 Einschlägige Normen

Die DSGVO resultiert aus dem Wunsch nach einer Harmonisierung des Datenschutzrechts auf EU-Ebene. Sie regelt die allgemeinen Voraussetzungen, speziell für den Onlinesektor ist die E-Privacy-Verordnung geplant. Ursprünglich sollte sie ebenfalls am 25.05.2018 in Kraft treten, wird sich jedoch wohl verzögern.