

Im Alltag angekommen?

2020

Datenschutzverantwortliche haben sich durch Verarbeitungsverzeichnisse gekämpft, mit Datenschutzerklärungen gerungen und Cookies gebändigt. Und nun können alle wieder zur Tagesordnung übergehen, oder? Mitnichten, denn die DSGVO ist ein Dauerbegleiter. Die Gefahr saftiger Strafen sorgt für die notwendige Aufmerksamkeit.

Von Joerg Heidrich

Nachdem zunächst über ein Jahr lang so gut wie keine Geldbußen durch die Aufsichtsbehörden verhängt wurden und auch die fälschlicherweise prophezeiten Abmahnwellen nicht stattgefunden haben, ist vielerorts das Interesse am Datenschutz schlagartig wieder erlahmt. Doch das Vertrauen darauf, dass dieser Zustand auf Dauer anhält, wird sich als einigermaßen naiv erweisen. Dies zeigt nicht nur der Blick ins europäische Ausland, in dem die Strafen bereits mühelos sieben- und achtstellige Höhen erreicht haben. Auch hierzulande gibt es inzwischen Bußgelder im achtstelligen Bereich, die jedem Unternehmen wehtun und die sich zudem auch nicht gerade rufördernd auswirken.

Ohnehin wendet sich der anfangs eher gütige Blick der Aufsichtsbehörden zunehmend Bereichen zu, die in vielen Unternehmen immer noch nicht oder nur ansatzweise umgesetzt sind. Doch auch die bisher im Rahmen etwa von TOMs oder den Verzeichnissen der Verarbeitungstätigkeiten gefertigten Dokumentationen dürfen nicht für alle Zeiten in den Tiefen der Büroschränke verschwinden. Vielmehr müssen sie regelmäßig überholt und angepasst werden. Das Jubiläum zur zweijährigen Anwendung der DSGVO könnte hier einen angemessenen

Zeitpunkt bieten, die Unterlagen einmal durchzusehen und zu überarbeiten.

Stand der Technik umsetzen

Dies gilt etwa für die TOMs: Diese technisch-organisatorischen Maßnahmen muss ein Datenverarbeiter zum Schutz der von ihm vorgehaltenen Daten nicht nur umsetzen, sondern auch detailliert dokumentieren. Einfluss auf diese Strukturen hat dabei vor allem die zentrale Vorgabe zur IT-Sicherheit in Art. 32 DSGVO. Vereinfacht gesagt kann man sich diese Vorgaben als Waage vorstellen. Auf der einen Seite liegen dabei die Daten. Je sensibler diese sind und auch je mehr Informationen vorhanden sind, desto höher sind auf der anderen Seite die Anforderungen an die IT-Sicherheit.

Gerade bei hoch schützenswerten Daten, wie solchen aus dem Bereich der Gesundheit, entstehen enorm hohe Vorgaben, die bisweilen auch einem reibungslosen Betrieb des Unternehmens nicht immer förderlich sind. Zugleich enthält Art. 32 DSGVO noch die Anforderung, den „Stand der Technik“ zu beachten, was in sehr vielen Unternehmen immer noch nicht umgesetzt wurde (siehe dazu den Artikel ab S. 94).



Gut abgeschätzt

Ebenso große Defizite weisen die meisten Unternehmen im Bereich der Folgenabschätzung auf. Dies sind Gutachten, die Unternehmen zur Risiko-bewertung abfassen müssen, wenn sie bei geplanten Vorhaben Risiken feststellen (siehe Artikel ab S. 98). Wichtig dabei: Die Risiken sind nicht aus der Perspektive des Verarbeiters, sondern aus derjenigen der Betroffenen zu beurteilen, also etwa der Kunden oder der Mitarbeiter.

Darüber hinaus hat der Gesetzgeber eine Reihe von Sachverhalten festgelegt, in denen immer eine Folgenabschätzung durchzuführen ist. Hierzu gehört insbesondere der praxisrelevante Bereich der großflächigen Videoüberwachung, aber auch die „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 DSGVO“, also etwa von Krankendaten.

Praktisch ist dabei, das bestehende Risiko der Datenverarbeitung zu analysieren und das Ergebnis in ein Verhältnis zu den Gefahren für die Betroffenen zu stellen. Die Analyse und das Ergebnis sind zu dokumentieren. Je nach Komplexität des Projekts kann der Umfang einigen Blättern, einem Reclam-Heft oder auch einer Buddenbrooks-Ausgabe entsprechen.

Diese Analysen verschwinden nach ihrer Auswertung im günstigsten Fall für immer in der Schublade des Datenschutzbeauftragten und werden nie wieder benötigt. Wehe aber dem Verantwortlichen, dem etwas passiert und der in diesem Fall keine ordentliche Folgenabschätzung vorweisen kann! Diese Verfehlung kann leicht eine zusätzliche Null bei der Bemessung der Geldstrafe durch die Aufsichtsbehörde nach sich ziehen. So gab es bereits in Schweden eine Strafe gegen eine Schule, welche die Anforderungen nach Art. 35 DSGVO ignoriert hat.

Vervielfachte Strafen

Überhaupt, die Strafen: Ein halbes Jahr dauerte es, bis es im Fall „Knuddels“ überhaupt die erste in Deutschland verhängte Strafe gab – und die war mit 20.000 Euro angesichts der im Raum stehenden Verfehlungen doch sehr gering. Spätestens mit der Einführung einer einheitlichen Bußgeld-Berechnung durch die Behörden werden solche Summen allenfalls noch gegenüber Kleinstunternehmen verhängt werden. Größeren Unternehmen drohen da-

gegen die bereits in anderen europäischen Ländern üblichen sechs-, sieben- oder gar achtstelligen Geldbußen (siehe Artikel ab S. 68).

Allerdings bleiben solche Strafen natürlich nicht unwidersprochen, sodass daraus Gerichtsurteile resultieren werden, die hoffentlich etwas mehr Licht in die bisweilen doch sehr trübe Rechtslage der DSGVO bringen. Dabei wird es auch spannend sein, zu sehen, in welchen Bereichen die immer noch personell stark unterbesetzten Aufsichtsbehörden die Prioritäten bei der Verfolgung von Verstößen sehen werden.

Still ruht der Abmahnsee

Währenddessen ist von den erwarteten Abmahnwellen in der Praxis bis auf einige bisweilen eher exotisch-komische Versuche wenig zu sehen. So sorgte ein Schreiben eines Anwalts aus Berlin in der Fachwelt für Schmunzeln, mit dem er versuchte, für seinen Mandanten eine fünfstellige Summe als Schadensersatz für das unverschlüsselte Senden von Kontaktdaten über ein Formular zu erbetteln.



Ein Grund für die bisherige Ruhe ist vor allem, dass der Abmahnanwalt ein eher scheues Tier ist, das vor allem auf eine klare und eindeutige Rechtslage setzt, um auf Beutezug zu gehen. Diese Rechtssicherheit fehlt jedoch, da immer noch nicht abschließend geklärt ist, ob Abmahnungen auf Basis von DSGVO-Verstößen tatsächlich wirksam sind. Nicht nur die Fachwelt ist sich hier uneins, auch die

Gerichte kommen zu höchst unterschiedlichen Ergebnissen.

Auf zur nächsten Runde!

Insgesamt gilt also: Die DSGVO ist ein Dauerprojekt und unterliegt ständigem Wandel. Nicht nur die Dokumentationen müssen Unternehmen und andere Institutionen regelmäßig anpassen und bei Bedarf erneuern. Auch neue Entwicklungen und Herausforderungen müssen sie verfolgen und beachten. Denn eins ist sicher: Bußgelder werden nicht nur zahlreicher, sondern auch schmerzlicher. Auf der anderen Seite darf man hoffentlich darauf vertrauen, dass mit anstehenden Gerichtsurteilen auch mehr Rechtssicherheit in die vielen noch ungeklärten Fragen hinsichtlich der Anwendung der DSGVO kommt. (anm)

DSGVO

Das sollten Sie wissen

Mit der DSGVO hat sich im Datenschutz vieles geändert, vieles aber auch nicht. Nach über einem Jahr der Anwendung zeichnet sich nun klarer ab, worauf man im Alltag unbedingt achten muss.

Von Nick Akinci

Mit dem Erscheinen dieses Ratgebers liegen die ersten anderthalb Jahre mit der europäischen Datenschutz-Grundverordnung (DSGVO) hinter uns. Viele strittige Details zur Auslegung der Verordnung werden nach wie vor heftig diskutiert, da erst nach und nach wegweisende Gerichtsurteile ergehen, die sich mit der Auslegung der Normen beschäftigen. Trotzdem haben wir in der praktischen Umsetzung bereits viel dazugelernt und können für das Jahr 2020 besser einschätzen, was wichtig wird und was nicht.

Was Sie über die DSGVO erfahren

Das vorliegende Heft vermittelt Unternehmen wie Privatpersonen das wichtigste Wissen über die DSGVO in einfacher und strukturierter Form und dient gleichzeitig als Nachschlagewerk für konkrete Probleme. Dabei beleuchten wir die Rechte der

Bürger, die Pflichten von Unternehmen und die technischen Aspekte des Datenschutzes. Darüber hinaus geben wir Ihnen Lösungen an die Hand, die Ihnen den rechtssicheren Umgang mit personenbezogenen Daten vereinfachen.

Was ist eigentlich die DSGVO?

Bei der DSGVO handelt es sich um eine vom europäischen Gesetzgeber erlassene Verordnung. Zwar war diese bereits am 25. Mai 2016 in Kraft getreten - wirksam wurden die neuen Regelungen jedoch erst zwei Jahre später, am 25. Mai 2018. Im Unterschied zu seinem Vorgänger, der europäischen Datenschutz-Richtlinie aus dem Jahre 1995, ist eine EU-Verordnung direkt in allen Mitgliedsstaaten der europäischen Union anwendbar. Daher kann sich nun beispielsweise jeder Bürger direkt auf die Rechte berufen, die ihm nach der DSGVO zustehen, und muss nicht erst auf eine nationalstaatliche Um-

setzung warten. Vereinzelt beinhaltet die Verordnung jedoch auch Öffnungsklauseln, die dem nationalen Gesetzgeber die Möglichkeit geben, bestimmte Details in eigenen Gesetzen zu regeln. Solche länderspezifischen Vorschriften sind in der Bundesrepublik im neuen Bundesdatenschutzgesetz (BDSG-neu) zu finden, das ebenfalls am 25. Mai 2018 wirksam wurde.

Was war vor der DSGVO?

Aufgrund der großen Spielräume, die die Datenschutz-Richtlinie den Gesetzgebern in den einzelnen europäischen Ländern bei der Umsetzung einräumte, bestanden teils gravierende Unterschiede hinsichtlich des Datenschutzniveaus. Unternehmen flüchteten regelmäßig vor strengeren Datenschutzregimen, indem sie ihren Hauptgeschäftssitz in Länder verlegten, in denen die Anforderungen an den Datenschutz besonders niedrig waren beziehungsweise in denen Rechtsbrüche selten verfolgt wurden. So unterhielten beispielsweise Social-Media-Größen wie Facebook, Twitter und LinkedIn ihre europäische Niederlassung in Irland, wo die zentrale Aufsichtsbehörde gerade einmal 30 Mitarbeiter vorhielt, um die Rechte von Millionen von europäischen Nutzern zu schützen.

Die DSGVO vereinheitlicht nun das Datenschutzrecht im Sinne einer Vollharmonisierung europaweit und sorgt damit im Idealfall dafür, dass in der gesamten europäischen Union ein einheitliches Datenschutzniveau herrscht. Dabei wird der Datenschutz auf ein hohes Niveau angehoben, das in etwa dem entspricht, das in Deutschland schon seit längerer Zeit herrscht. Abgesehen von der Erhöhung des Datenschutzniveaus in vielen Ländern bietet die Verordnung aber auch den großen Vorteil, dass sowohl für Unternehmen als auch für Privatpersonen und Verbraucher europaweit einheitliche Regeln gelten, womit eine enorm große Transparenz erreicht wird.

Die wichtigsten Neuerungen auf den Punkt gebracht


Eine der vielleicht wichtigsten Neuerungen, die die DSGVO mit sich bringt, sind die deutlich gestiegenen und nunmehr abschließend geregelten Informationspflichten bei der Datenverarbeitung. So

sind die von der Verarbeitung betroffenen Personen beispielsweise darüber zu informieren, welche Daten zu welchem Zweck verarbeitet werden und wie lange diese gespeichert werden. Selbstverständlich muss aber nicht jeder, der irgendwie Daten verarbeitet, hierüber informieren. Über den Anwendungsbereich der DSGVO erfahren Sie mehr im nachfolgenden Artikel „Gilt die DSGVO auch für mich?“. Wichtige Begrifflichkeiten erläutern wir im Artikel „Grundsätze des Datenschutzrechts“ ab Seite 16.

Auch die qualitativen Anforderungen an die Informationspflichten wurden deutlich angehoben. Die Verordnung legt hier großen Wert auf Verständlichkeit und Transparenz. Was dies bedeutet, erklären wir im Kapitel „Pflichten für Unternehmen“ ab Seite 52.

Mit der DSGVO legt der Gesetzgeber weiterhin erstmals auch einen Schwerpunkt auf das Thema technischer Datenschutz. Mit den nun eingeführten Begriffen *Privacy by Design* und *Privacy by Default* widmet sich die Verordnung auch der technischen Umsetzung von datenschutzrelevanten Vorhaben und Projekten. Mehr hierzu erfahren Sie ab Seite 94.

Bei den Bürgerrechten hält die DSGVO ebenfalls einige Neuerungen bereit. So führt die Verordnung zum Beispiel das Recht auf Datenübertragbarkeit und das Recht auf Vergessenwerden ein. Ihre erweiterten Rechte lernen Sie ab Seite 44 kennen.

Eine deutliche Veränderung haben schließlich noch die Sanktionen erfahren, die verhängt werden können, um Datenschutzverstöße zu ahnden. Nachdem Bußgelder nach den bisherigen Regelungen maximal 300.000 Euro pro Einzelfall betragen durften, sind nun Bußgelder in Höhe von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes eines Unternehmens möglich, je nachdem, was höher ist. Details zu Bußgeldern, Abmahnungen und Schadensersatz stellen wir Ihnen im Artikel ab Seite 68 vor. (anm) 



Gesetzestexte

ct.de/wvux