Dr. Martin Bahr

Das neue Datenschutzrecht: praktische Auswirkungen auf den Online-Bereich: Teil 1

In der letzten Ausgabe ging es um die neue E-Privacy-Verordnung (E-Privacy-VO). In der aktuellen Ausgabe soll das neue europaweite Datenschutzrecht – die sogenannte EU-Datenschutzgrundverordnung – betrachtet werden sowie deren Auswirkungen auf den Online-Bereich. In einer mehrteiligen Reihe zeigt Fachanwalt Dr. Bahr auf, was Betreiber von Online-Präsenzen erwartet und worauf sie sich künftig einstellen müssen.

DER AUTOR

Die **Kanzlei Dr. Bahr** *(http://www.Dr-Bahr.com)* ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter Suchmaschinen-und-Recht.de betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

Das neue Gesetz: die EU-Datenschutzgrundverordnung

Viele Leser werden schon das eine oder andere davon gehört haben: Ende Mai nächsten Jahres tritt ein neues Gesetz in Kraft, nämlich die EU-Datenschutzgrundverordnung (EU-DSGVO).

1. Zeitpunkt des Inkrafttretens:

Die neuen Regelungen treten zum 25. Mai 2018 in Kraft. Es gibt keinerlei Übergangsfristen. Dies bedeutet, dass bis 23:59 Uhr am 24. Mai 2018 noch das alte Recht gilt. Und Punkt 00:00 Uhr am 25. Mai 2018 gilt dann das neue Gesetz. Da es keinerlei Übergangszeiträume gibt, ist allen Online-Unternehmen dringend anzuraten, sich bereits heute, fast ein Dreivierteljahr vor dem Stichtag, mit diesem Thema zu beschäftigen.

2. Komplette Neugestaltung des Datenschutzrechts:

Durch die EU-DSGVO wird das komplette Datenschutzrecht neu gestaltet. Das Bundesdatenschutzgesetz (BDSG) in seiner bisherigen Fassung wird komplett abgeschafft und hierfür die Bestimmungen des EU-DSGVO eingeführt. Zukünftig wird man sich bei rechtlichen Ansprüchen somit nicht mehr auf das BDSG stützen, sondern direkt auf die EU-DSGVO.

Die EU-DSGVO ist unmittelbar anzuwendendes Recht, d. h., sie ist wie das BGB oder das StGB ein Gesetz und wird zukünftig von allen deutschen Gerichten direkt angewendet werden.

Es erfolgt eine Total-Sanierung des deutschen Datenschutzrechts. Somit wird nicht nur der Online-Bereich neu geregelt, sondern vielmehr der gesamte Bereich dieses Rechtsgebiets, von A wie Arbeitnehmer-Datenschutz bis hin zu V wie Videoüberwachung. Nicht nur der private Unternehmensbereich ist betroffen, sondern auch für Behörden und die sonstige öffentliche Verwaltung gelten die Neuregelungen.

Es ist somit nicht übertrieben, wenn man daher von einer neuen Ära des Datenschutzrechts spricht.

3. Ziele der Reform:

Die Reform hat drei große Ziele.

Erstens will sie EU-weit das Datenschutzrecht harmonisieren. Zukünftig gilt die EU-DSGVO somit europaweit, d. h., in Frankreich gelten nächstes Jahr die gleichen Regelungen wie in Deutschland oder Italien.

Zweitens will das Gesetz, so jedenfalls seine ursprüngliche Intension, das Datenschutzrecht fit machen für moderne Technologien wie z. B. „Cloud Computing“. Wir werden im Laufe dieser Reihe sehen, dass von diesem frommen Wunsch im Ergebnis leider nicht viel übrig geblieben ist.

Und drittens sollen dem einzelnen Verbraucher seine Grundrechte und seine Grundfreiheiten in puncto Datenschutz zurückgegeben werden. Zukünftig soll der Einzelne wieder bestimmen können, ob und an wen er seine persönliche Daten preisgibt.

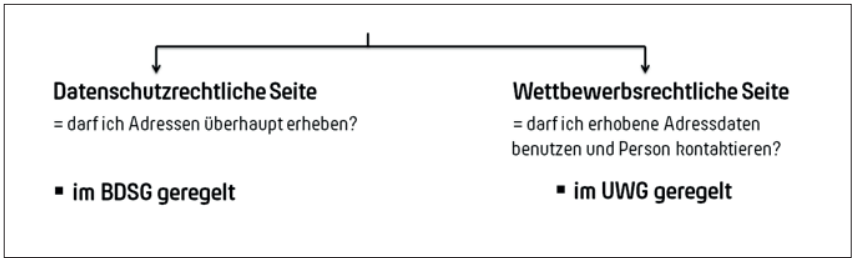

Abb. 1

4. Einordnung der Änderungen:

Immer wieder ist zu lesen, dass das Datenschutzrecht ganz massiv das Direktmarketing ändere. Eine solche Aussage ist grottenfalsch. Im wettbewerbsrechtlichen Direktmarketing ändert sich rein gar nichts.

Zum Verständnis siehe Abbildung 1.

Um die Reichweite der Reformen zu begreifen, ist es wichtig zu verstehen, wie das deutsche Direktmarketingrecht aufgebaut ist. Man unterscheidet hier zwischen dem Datenschutzrecht auf einer einen Seite und dem Wettbewerbsrecht auf der anderen Seite.

Beim Wettbewerbsrecht geht es um die Frage, ob und wie ich den Kunden kontaktieren darf, ob ich ihm beispielsweise eine E-Mail schreiben oder ihn anrufen oder ein Fax schicken darf. All dies ist im Gesetz gegen den unlauteren Wettbewerb (UWG) geregelt. Knapp 99,9 % aller bisherigen Streitigkeiten im Bereich des Direktmarketings haben sich im Wettbewerbsrecht abgespielt. Beim klassischen Fall von Spam-Mails oder einem unerlaubten Werbeanruf (Cold Call) ging es immer um Wettbewerbsverstöße. Den meisten Lesern dürfte die Norm § 7 UWG schon einmal über den Weg gelaufen sein. Erhielt ein Unternehmen eine Abmahnung wegen verbotener E-Mail-Werbung, wurde sich stets auf das Wettbewerbsrecht gestützt. Das Datenschutzrecht spielte hier in aller Regel keine Rolle.

Beim Datenschutzrecht hingegen geht es allein um die Frage, ob die Daten (z. B. die E-Mail-Adresse) überhaupt erhoben und gespeichert werden dürfen.

Durch die EU-DSGVO ändert sich auf der wettbewerbsrechtlichen Seite rein gar nichts. Keinerlei UWG-Norm wird verändert oder angepasst. Sämtliche Änderungen erfolgen vielmehr rein auf der datenschutzrechtlichen Seite.

Hierbei handelt es sich um keine bloße Formalie oder Spitzfindigkeit, sondern vielmehr um einen elementaren Baustein: Ist nämlich die Unterscheidung zwischen dem Wettbewerbsrecht auf der einen Seite und dem Datenschutzrecht auf der anderen Seite verstanden, erschließt sich auch sofort die genaue Reichweite der Neuregelungen.

Im Direktmarketingrecht ändert sich unmittelbar erst einmal nichts, denn das bisherige Wettbewerbsrecht bleibt bestehen: Die Voraussetzungen für Unternehmen, ob und wie sie einen potenziellen Kunden kontaktieren dürfen, bleiben auch 2018 gleich.

Es ändert sich hingegen der vorgelagerte Bereich, nämlich ob und wie Unternehmen an die Daten kommen. Im Ergebnis haben diese neuen Bestimmungen natürlich auch mittelbar Auswirkungen auf den Bereich des Direktmarketings. Denn wenn eine Firma über keine Daten verfügt, kann sie später auch keine Verbraucher kontaktieren und ihre Produkte bewerben. Insofern ist das Datenschutzrecht zwingendes Durchgangsstadium für einen erfolgreichen Abverkauf.

Falsch ist und bleibt jedoch die Behauptung, dass sich etwas bei der Frage verändert, ob und wie ich eine Person kontaktieren darf. Dies ist alleine eine Frage des Wettbewerbsrechts. Und daran ändert sich, wie bereits erläutert, rein gar nichts.

5. Warum ist die Einhaltung der neuen Gesetzeslage so wichtig:

Der eine oder andere Leser wird sicherlich bereits von den hohen drohenden Sanktionen gelesen haben, die die EU-DSGVO vorsieht. Geldbußen von bis zu 20 Mio. EUR oder 4 % des Jahresumsatzes werden in den allermeisten Artikeln genannt und entsprechende Horrorszenarien an die Wand gemalt.

Eine solche isolierte Betrachtungsweise geht an der wirklichen Problemlage vorbei und ist zudem außerordentlich gefährlich, weil sie ziemlich eindimensional ist.

Die EU-DSGVO sieht zukünftig zwei Sanktionen vor, die ein Unternehmen treffen können, wenn es sich datenschutzkonform verhält. Nämlich einmal die Verhängung einer Geldbuße und einmal die Geltendmachung von Schadensersatzansprüchen.

a. Geldbußen:

Es ist richtig, dass die zuständigen Behörden zukünftig Geldbußen von bis zu 20 Mio. EUR oder 4 % des Jahresumsatzes eines Unternehmens verhängen können. Das Gesetz bestimmt ausdrücklich, dass die Sanktionen zukünftig erheblich sein sollen und bewusst massiv und abschreckend ausgestaltet sind. Die Zeiten des zahnlosen Papiertigers Datenschutzrecht sollen dadurch ein für alle Mal beendet sein.

Die Realität spricht aber eine andere Sprache. Bereits aufgrund der personellen Ausstattung der deutschen Datenschutzbehörden kann und wird es keine flächendeckenden Kontrollen geben. Die Realität sieht nämlich so aus, dass bislang in Deutschland ein Unternehmen nur alle 39.400 Jahre damit rechnen musste, durch die Datenschutzbehörde geprüft zu werden. In der Praxis scheiterte bislang eine flächendeckende Kontrolle stets an der Personalknappheit der Mitarbeiter der jeweiligen Behörde. Die Aufsichtsämter haben trotz des Inkrafttretens der EU-DSGVO in aller

Regel keine zusätzlichen Arbeitskräfte erhalten, sodass am bisherigen Status quo der Prüfungen kaum eine Änderung eintreten wird.

Die Wahrscheinlichkeit, dass von dieser Seite her Ärger droht, ist somit überschaubar. Lediglich in dem Ausnahmefall, dass die Aufsichtsbehörde durch die Beschwerde eines Verbrauchers informiert wird, ist mit Ungemach zu rechnen. Denn dann richten sich möglicherweise die Argusaugen der Behörde auf das Unternehmen und eine Datenschutzprüfung vor Ort droht.

b. Schadensersatz:

Die deutlich praktischere Bedeutung kommt vielmehr der zweiten Sanktion, nämlich dem Schadensersatzanspruch, zu. Durch die EU-DGSVO wird für jede Person, deren Daten unerlaubt verarbeitet werden, das Recht eingeführt, den Verletzer auf Schadensersatz zu verklagen.

Bislang war dem deutschen Datenschutzrecht ein solcher Schadensersatzanspruch nicht bekannt. Datenschutzverletzungen spielten daher aus Sicht der meisten Unternehmen kaum eine wirkliche Rolle, da mit finanziellen Konsequenzen kaum zu rechnen war. Diese Hülle des Schattendaseins streift die EU-DSGVO nun komplett ab.

Die Höhe des Schadensersatzanspruchs ist gesetzlich nicht begrenzt, d. h., rein theoretisch können hier durchaus drei-, vier- oder gar fünfstellige Euro-Summen als Schadensersatz herauskommen. Niemand kann heute sagen, was die Gerichte zukünftig als Beträge auswerfen werden, zumal man immer berücksichtigen muss, dass die EU-DSGVO europaweit gilt. Auch wenn deutsche Gerichte möglicherweise eher nur zurückhaltend von diesem Rechtsinstitut Gebrauch machen könnten, kann es durchaus sein, dass beispielsweise italienische oder spanische Gerichte die Sache ganz anders sehen und erhebliche Beträge auswerfen werden.

Nun werden sich viele Leser die Frage stellen, was für einen tatsächlichen finanziellen Schaden denn der einzelne Verbraucher überhaupt hat, wenn seine Daten unerlaubt verarbeitet werden. Diese Frage beantwortet die EU-DSGVO relativ eindeutig: Der Betroffene muss keine unmittelbaren ökonomischen Nachteile erlitten haben, um einen Schadensersatz zu begehren. Vielmehr erhält er diesen Anspruch aufgrund seines quasi seelisch erlittenen Unrechts, nämlich dass seine Daten ohne seine Erlaubnis verarbeitet wurden.

Am besten vergleichbar ist diese Konstellation mit den bekannten Fällen aus dem Presserecht, wo Zeitungen aufgrund falscher oder frei erfundener Berichte Schadensersatz an Prominente bezahlen müssen. So beispielsweise vor Kurzem die Zeitung Bunte, die an Michael Schumacher 50.000,- EUR zahlen muss, weil sie unwahre Aussagen über den Gesundheitszustand des ehemaligen Formel-1-Fahrers abdruckte.

Mit der Einführung dieses Schadensersatzanspruchs verändert sich das bisherige Bedrohungsszenario ganz erheblich: Spielten in aller Regel bislang die Abmahnkosten und die Abgabe einer strafbewehrten Unterlassungserklärung die entscheidende Rolle, wird dies zukünftig nur noch ein Randproblem sein.

Vielmehr ist zu befürchten, dass sich „Schadensersatzvereine“ gründen, die nur ein Ziel haben: So viele Verbraucher wie möglich zu sammeln, um die Republik mit Schadensersatzansprüchen zu überziehen.

Bei mehr als 160.000 Rechtsanwälten in Deutschland wird es nur eine Frage der Zeit sein, bis entsprechende Internet-Portale gegründet werden, die sich auf die Suche nach vermeintlich geschädigten Verbrauchern machen. Ähnlich wie die bekannten Fälle von flightright.de (bei Flugverspätungen) oder myRight (beim VW-Abgasskandal) ist zu befürchten, dass sich auch hier entsprechende Interessengemeinschaften bilden werden, um eine möglichst große Anzahl vermeintlich geschädigter Verbraucher auf sich zu vereinen. Der Betreiber des Portals erhält eine entsprechende Provision am Schadensersatzanspruch. Für den vermeintlichen Verbraucher eine lukrative Sache: Er muss die Datenschutzverletzung nur melden, bezahlt keine Kosten für die rechtliche Durchsetzung und erhält den Löwenanteil des Schadensersatzes. Es dürfte nur eine Frage der Zeit sein, bis sich die ersten Start-ups diesen Themenbereich vornehmen werden.

Wenn also in der Praxis Gefahr droht, dann nicht durch die Geldbußen, sondern vielmehr durch die Einführung des Anspruchs auf Schadensersatz.

Ein wichtiger Umstand verstärkt noch diese Situation: Zukünftig liegt nämlich die Beweislast und Rechenschaftspflicht für eine ordnungsgemäße Datenverarbeitung bei dem Unternehmen. Kann eine Firma nicht nachweisen, wie sie an die Daten gekommen ist, dann geht das Gesetz von einer Datenschutzverletzung aus.

Ab 2018 kommt somit den Dokumentationspflichten eine noch entscheidendere Bedeutung zu: Nämlich nur dann, wenn das Unternehmen ausreichend belegen und notfalls auch gerichtlich nachweisen kann, dass alles datenschutzkonform erfolgte, bestehen keine Risiken.

Firmen, die beruflich personenbezogene Daten mit Geschäftspartnern austauschen (z. B. Stand Alone-Werbung im E-Mail-Marketing), sehen sich sofort Regressansprüchen ihrer Kunden ausgesetzt, wenn diese in Anspruch genommen werden. Es wird also noch mehr als bislang das A und O sein, auf eine rechtskonforme Erhebung von Daten (z. B. Einwilligungen bei Gewinnspielen) zu achten. ¶