

Dr. Martin Bahr

Das neue Datenschutzrecht: praktische Auswirkungen auf den Online-Bereich: Teil 2

In einer mehrteiligen Reihe werden die praktischen Auswirkungen auf den Online-Bereich dargestellt. In der letzten Ausgabe hatten wir bereits begonnen, uns mit dem neuen europäischen Datenschutzrecht, der sogenannten EU-Datenschutzgrundverordnung (EU-DSGVO), zu beschäftigen. Dieser zweite Teil setzt diese Darstellung fort und befasst sich schwerpunktmäßig mit der Beweislast und den damit verbundenen Dokumentationspflichten.

1. Geltungsbereich der neuen Regelungen:

a. Räumlich

Die neuen Regelungen sind immer dann anwendbar, wenn Daten von EU-Bürgern verarbeitet werden. Dabei ist es egal, wo das Online-Unternehmen seinen Firmensitz hat, ob in den USA oder in Afrika oder Europa. In allen drei Fällen gilt die EU-DSGVO, wenn die Webseite sich auch an EU-Bürger richtet. Die datenschutzrechtlichen Bestimmungen sind somit faktisch weltweit anwendbar, d. h., alle Unternehmen müssen sich an die Vorgaben halten, egal, wo sie sitzen.

b. Persönlich

Die Vorschriften der EU-DSGVO gelten nur dann, wenn die Informationen sich auf eine identifizierte oder identifizierbare Person beziehen. Die EU-DSGVO gilt somit immer dann, wenn eine natürliche Person namentlich ausdrücklich genannt wird oder diese sich aus den näheren Umständen bestimmen lässt.

Lediglich Daten, die sich ausschließlich auf eine juristische Person beziehen, fallen nicht unter das neue Datenschutzrecht. Diese Regelung entspricht den bisherigen Vorschriften des BDSG.

2. Beweislast und Rechenschaftspflicht:

Eine der grundlegenden neuen Vorschriften ist die Einführung einer Beweislastumkehr, die mit einer umfassenden Rechenschaftspflicht einhergeht.

Zukünftig trifft den Online-Unternehmer die Pflicht nachzuweisen, dass er die bei ihm gespeicherten Daten ordnungsgemäß erhoben hat. Befinden sich somit personenbezogene Informationen im Besitz einer Firma, von denen sie nicht mehr genau nachvollziehen kann, woher diese stammen, nimmt das neue Gesetz im Zweifel eine Datenschutzverletzung an.

Beispiel:

Im Newsletter der Firma A befinden sich aus dem Jahr 2007 noch zwanzig E-Mail-Adressen, von denen das Unternehmen nicht genau sagen kann, woher diese stammen. Ob die E-Mail-Adressaten sich damals selbst eingetragen haben oder ein Mitarbeiter der Firma, kann heute nicht mehr geklärt werden.

Da Firma A die Beweislast trifft, liegt nach neuem Recht eine Datenschutzverletzung vor.

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.

Den Unternehmer trifft eine ausführliche Rechenschaftspflicht zu belegen, wie er an die Daten gekommen ist. Das Gesetz selbst macht dabei keine formalen Vorgaben, wie eine solche Dokumentation auszusehen hat. Vielmehr stellt es dies in das Ermessen der Firma, welche Belege es für sinnvoll und notwendig erachtet.

Im deutschen Recht gibt es fünf Beweismittel: Sachverständiger, Augenschein, Parteivernehmung, Urkunde und Zeuge. Für den Bereich des Datenschutzrechts spielt lediglich der Augenschein keine Rolle. Das „sicherste“ Beweismittel ist erfahrungsgemäß die Urkunde, denn dort steht schwarz auf weiß und objektiv nachprüfbar, welche Erklärungen abgegeben wurden und welche nicht. Das „unsicherste“ Beweismittel hingegen ist der Zeuge, da dieser keine objektive, sondern stets nur seine subjektive Sichtweise wiedergeben kann. Untersuchungen haben gezeigt, dass die Genauigkeit der menschlichen Erinnerungen mit der Zeitdauer erheblich abnimmt.

Praxis-Tipp:

Ihre Nachweise sollten daher primär schriftliche Dokumente sein und nur ergänzend sollten Sie Mitarbeiter als Zeugen heranziehen. Wie genau Sie Ihre Nachweispflichten erfüllen können, wird vom konkreten Einzelfall abhängen, also welche Arten und wie viele Daten Sie speichern.

Als erste Orientierung können Sie sich folgendes plakatives Beispiel merken: Denken Sie an eine handelsübliche Excel-Tabelle, in der pro Datenfeld eine Ihrer Informationen gespeichert ist. In einer weiteren Spalte müssen Sie nun angeben, woher Sie diesen Datensatz haben, z. B. durch Vertrag oder durch ein Opt-in.

Besonders bei älteren Bestandsdaten werden Sie schnell an Ihre Grenzen stoßen, da es Ihnen häufig nicht mehr möglich sein wird, die hierfür notwendigen Informationen nachzuerfassen. Viele Unternehmen reagieren daher aktuell mit einer teilweisen Löschung ihrer Altdaten, um etwaigen Sanktionen zu entgehen.

Praxis-Tipp:

Eine solche Löschung sollte jedoch nur der allerletzte Ausweg sein, denn damit werden wertvolle immaterielle Vermögensgüter einfach aus dem Fenster geschmissen. Vorab sollte vielmehr jedes Unternehmen genau prüfen, ob es seine bisherigen Datensätze nicht auf anderem Weg „legalisieren“ kann.

Ein legaler Weg ist zum Beispiel, seine Kundendatei mit allgemein zugänglichen Daten (z. B. Internet, Telefonbuch oder Handelsregister) abzugleichen. Sind nämlich die Informationen für die Allgemeinheit verfügbar (z. B. Name, Adresse, E-Mail-Adresse), so können Sie dies als Speichungsgrund in ihrer Dokumentation angeben. Sie haben dadurch mit einfachsten Mitteln einen Großteil ihrer Daten, bei denen Ihnen die Nachweise fehlten, gerettet und können diese auch weiterhin nutzen. Lediglich der Teil, für den Sie nichts ermitteln können, muss dann entfernt werden.

Es ist daher zwingend notwendig, dass Online-Unternehmen ein umfassendes Archivierungs- und Versionsmanagement einführen.

Praxis-Tipp:

Das Ganze hört sich schlimmer an, als es in der Praxis ist. Geht es beispielsweise um den Nach-

weis Ihrer Newsletter-Abonnenten, verfügen Sie i. d. R. bereits über eine entsprechende Software. Denn schon heute speichern die meisten IT-Systeme solche Informationen wie Zeitpunkt des DOI, der Check-Mail, Bestätigung, Inhalt der Einwilligung usw. ab, um bei wettbewerbsrechtlichen Streitigkeiten den Nachweis erbringen zu können.

Dieses Tool kann nahtlos auch für die datenschutzrechtlichen Nachweispflichten verwendet werden. Sie fangen also i. d. R. nicht bei null an, sondern können auf bereits vorhandene Lösungen zurückgreifen.

3. Alte Werbe-Opt-ins trotz Datenschutzreform auch zukünftig nutzen:

Derzeit sind viele falsche Behauptungen hinsichtlich der Datenschutzreform im Umlauf. So ist immer wieder zu lesen, dass alte Werbe-Opt-ins durch die Reform grundsätzlich ab Mai 2018 unwirksam würden und nicht mehr benutzt werden könnten. Diese Aussage ist komplett falsch!

Lassen Sie sich von solchen Unwahrheiten nicht ins Bockshorn jagen! Sie dürfen selbstverständlich Ihre bisherigen Opt-ins problemlos weiterhin benutzen, wenn bestimmte Voraussetzungen, die in den meisten Fällen erfüllt sein werden, vorliegen.

Welche Voraussetzungen die neuen Opt-ins, die Sie nach Mai 2018 erheben, erfüllen müssen, werden wir im nächsten Abschnitt klären. Hier geht es nur um die Frage, ob alte Werbe-Einwilligungen auch weiterhin Bestand haben.

Die gute Nachricht vorweg: Alte Einwilligungen müssen nicht sämtliche der neuen Voraussetzungen erfüllen. So heißt es in Erwägungsgrund 171 der DSGVO ausdrücklich:

„Beruhen die Verarbeitungen auf einer Einwilligung (...), so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann.“

Vielmehr müssen Alt-Einwilligungen nur die wichtigsten dieser Voraussetzungen erfüllen, aber eben nicht alle. Die Frage ist nun: Was sind die wichtigsten?

Hierauf gibt es vonseiten der deutschen Datenschutzbehörden erfreulicherweise bereits verbindliche Einschätzungen: Der Düsseldorfer Kreis, das oberste Gremium der deutschen Datenschutzbehörden, hat festgelegt, dass zumindest die Merkmale der Freiwilligkeit und der Altersgrenze (16 Jahre) eingehalten sein müssen, damit alte Opt-ins weiterhin gelten. Das Bayerische Landesamt für Datenschutzaufsicht ist sogar noch unternehmerfreundlicher und sieht nur das Merkmal der Transparenz als wichtigen Faktor an.

Erfüllen Ihre Alt-Einwilligungen diese Voraussetzungen, so sind sie auch nach Mai 2018 wirksam, auch wenn andere Vorgaben der EU-DSGVO nicht eingehalten werden.

Praxis-Tipp:

Ein zeitliches Verfallsdatum für Alt-Einwilligungen existiert ebenso nicht. Benutzen Sie also Ihre alten Opt-ins auch nach Mai 2018 regelmäßig, so ist die zeitliche Nutzungsdauer unbefristet. Sie sehen also: Ihre wertvollen Alt-Einwilligungen sind keineswegs verloren. Im Gegenteil: Sie werden einen Großteil der bestehenden Opt-ins auch zukünftig nutzen können.

4. Neue Werbe-Opt-ins:

Viele der bisherigen Vorgaben, also beispielsweise Bestimmtheit oder Transparenz, gelten auch unter dem neuen Recht fort. Im Nachfolgenden wird daher nur auf die Neuerungen eingegangen.

a. Freiwilligkeit/Kopplungsverbot

Grundsätzlich sind Einwilligungen auch zukünftig nur dann wirksam, wenn sie freiwillig gegeben werden. Die neuen Vorschriften statuieren ein ausdrückliches Kopplungsverbot. Dies greift immer dann, wenn die Erteilung des Opt-ins unangebracht ist.

Beispiel:

Amazon verlangt beim Kauf von Briefpapier eine umfassende Einwilligung, dass das Unternehmen den Kunden per E-Mail und per Telefon kontaktieren und ihm Werbeangebote unterbreiten darf.

Eine solche Vorgehensweise würde gegen das Kopplungsverbot verstoßen.

Dieses Kopplungsverbot soll nach Ansicht der deutschen Behörden jedoch dann nicht greifen, wenn es sich um Gewinnspiele oder kostenlose Dienstleister (z. B. Freemailer) handelt. In einer solchen Konstellation – so das Bayerische Landesamt für Datenschutzaufsicht und die Datenschutzkonferenz – würde das Kopplungsverbot nicht greifen. Vielmehr könnten die Anbieter solcher Angebote – wie bislang schon – weiterhin vom Kunden umfangreiche Werbe-Einwilligungen abverlangen.

b. Umfangreiche Informationspflichten

Die nächste wichtige Änderung ist die Einführung umfangreicher Informationspflichten. Alleine Art. 13 EU-DSGVO stellt in zwölf Fällen konkrete Vorgaben auf.

Praxis-Tipp:

Leider sind diese Vorgaben sehr, sehr umfangreich, sodass viele Unternehmen hier teilweise zwischen 8 und 10 DIN-A4-Seiten Text erstellen müssen.

Verzweifeln Sie aber nicht allzu sehr. Hierbei handelt es sich primär um lästige Verwaltungstätigkeit. Der eigentliche Opt-in-Text wird durch diese Informationspflichten nämlich nicht berührt. Vielmehr können Sie diese neuen Informationen in Ihre Datenschutzerklärung „auslagern“.

c. Altersvorgabe

Bei Online-Angeboten, die sich an Minderjährige richten, darf zukünftig kein Werbe-Opt-in mehr von unter 16-Jährigen erhoben werden. Vielmehr ist die Einwilligung nur noch dann wirksam, wenn die Erziehungsberechtigten zugestimmt haben.

Dieses Verbot gilt aber nur für den Online-Bereich, im Offline-Bereich greift es hingegen nicht. Umstritten ist, welche genauen Anforderungen an die einzelne Webseite zu stellen sind: Gilt die Regelung für alle Portale oder nur für die, die sich gezielt an Kinder richten?

Praxis-Tipp:

Beachten Sie, dass auch nach allgemeinem Datenschutzrecht die Erhebung von Opt-ins bei Minderjährigen rechtlich nicht gänzlich unproblematisch ist. Hinzu kommt nun dieses neue Verbot. Überlegen Sie also sehr genau, ob es für Sie wirtschaftlich überhaupt sinnvoll ist, solche Zustimmungen zu bekommen, oder ob Sie auf diesen problematischen Bereich nicht von vornherein verzichten.