LOSCHELDER

Newsletter Datenschutzrecht

November 2019

Sehr geehrte Damen und Herren,

Datenschutzsünder erleben einen heißen Herbst: Der österreichischen Post wurde für den Verkauf von Wählerpräferenzen ein sattes Bußgeld in Höhe von 18 Millionen Euro auferlegt. Massiv will auch die Berliner Datenschutzbeauftragte vorgehen: Sie erließ auf Grundlage des Bußgeldkonzepts der deutschen Aufsichtsbehörden am 30. Oktober gegen die Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro. Gleichzeitig wird es für Unternehmen immer schwieriger, die datenschutzrechtlichen Anforderungen in einigen Bereichen einzuhalten. Das zeigt das aktuell veröffentlichte und sehr umfangreiche behördliche Prüfschema zu Microsoft Windows 10, in dem die Behörden ihrerseits einräumen, dass eine umfassende technische und rechtliche Prüfung praktisch kaum möglich sein dürfte.

Wir stellen Ihnen die Grundzüge des umsatzorientierten Konzeptes in unserem ersten Beitrag vor. In unserem zweiten Beitrag beschäftigen wir uns dann mit einer neuen Stellungnahme der europäischen Datenschutzbehörden. Darin beschreiben die Aufsichtsbehörden, wann aus ihrer Sicht eine Datenverarbeitung für die Erfüllung eines Vertrages erforderlich ist (Art. 6 Abs. 1 lit. b DSGVO) – mit erstaunlichen Ergebnissen, die den Fortbestand einiger Geschäftsmodelle in Frage stellen. Weiter geht es dann mal wieder mit der Webseitengestaltung: Gegenwärtig wird das beliebte Analysetool „*Google Analytics*“ von den Datenschutzbehörden genauer unter die Lupe genommen. Der letzte Beitrag unseres Newsletters befasst sich dann mit der ePrivacy-Verordnung, von der es zwar nach wie vor nur einen Entwurf gibt, der aber aktualisiert wurde und gerade von der finnischen Ratspräsidentschaft mit voller Kraft zu einer Einigung geführt werden soll.

Inhalt

Bußgeldbemessungskonzept der Datenschutzbehörden veröffentlicht

Die DSK veröffentlichte Mitte Oktober das bereits im Sommer beschlossene Bußgeldbemessungskonzept. Wie wir im September Newsletter berichteten, wurde das Konzept zunächst zurückgehalten und lediglich einzelne Inhalte drangen an die Öffentlichkeit. Nachdem aber aus Transparenzgesichtspunkten Kritik an der Zurückhaltung laut geworden war, kam die DSK der Forderung nun nach und hat ihr Konzept veröffentlicht. Das Konzept gilt vorbehaltlich von Änderungen und Ergänzungen sowie einer gesamteuropäisch festgelegten Leitlinie zur Methodik der Bemessung. Bis dahin soll das vorliegende Bemessungskonzept die Grundlage für die Bußgelder in der Sanktionspraxis der deutschen Aufsichtsbehörden bilden. Bislang waren – gerade im europäischen Vergleich – die Bußgelder deutscher Aufsichtsbehörden moderat. Zukünftig sind nach dem neuen Konzept – wie auch das 14,5 Millionenbußgeld für Deutsche Wohnen (SE) zeigt – höhere Bußgelder – insbesondere für Datenschutzverstöße von Unternehmen mit hohen Umsätzen – zu erwarten; das Bußgeldrisiko steigt damit.

Anlass für die Veröffentlichung des Bußgeldbemessungskonzepts waren laut Pressemitteilung der DSK die ersten Verhandlungen auf europäischer Ebene zu dieser Thematik und das Ziel, mit dem Konzept „einen Beitrag zur Transparenz im Hinblick auf die Durchsetzung des Datenschutzrechts“ zu leisten. Mit dem Konzept soll den Datenschutzaufsichtsbehörden „eine einheitliche Methode für eine systematische, transparente und nachvollziehbare Bemessung von Geldbußen“ zur Verfügung gestellt werden. Inhaltlich knüpfe das Konzept an den wesentlichen Vorgaben des Art. 83 DSGVO an, die eine Verhängung von verhältnismäßigen Bußgeldern mit dennoch abschreckender Wirkung zum Ziel haben.

Das von der DSK beschlossene Konzept gilt ausschließlich für die Bußgeldbemessung in Verfahren gegen Unternehmen im Anwendungsbereich der DSGVO. Geldbußen gegen Vereine außerhalb ihrer wirtschaftlichen Tätigkeit werden demnach nicht nach den im Papier beschrieben Regeln berechnet. Ebenso sind sie weder auf grenzüberschreitende Fälle anwendbar, noch entfalten sie eine Bindung für deutsche Gerichte oder Datenschutzbehörden anderer europäischer Mitgliedstaaten.

In der Praxis wird das Konzept voraussichtlich zu einer Anhebung der Bußgelder führen. Vor allem Großunternehmen mit einem hohen Jahresumsatz werden zukünftig bei schwerwiegenden Verstößen mit Bußgeldern in Millionenhöhe rechnen müssen. Das Bußgeldkonzept legt bei der Umsatzbemessung einen funktionalen Unternehmensbegriff zugrunde, d. h. die wirtschaftliche Einheit stellt **ein** Unternehmen dar. Eine Unternehmensgruppe kann demnach also ein Unternehmen darstellen, beispielsweise die kontrollierende Holding und ihre Tochterunternehmen.

Das Konzept sieht eine Bemessung anhand der folgenden fünf Schritte vor:

1. Zunächst wird das Unternehmen in eine Größenklasse eingeordnet. Die Einteilung erfolgt in Kleinst-, Kleine und Mittlere Unternehmen sowie Großunternehmen (gesamter weltweit erzielter Vorjahresumsatz bis 2 Mio. Euro, über 2 Mio. Euro bis 10 Mio. Euro; über 10 bis 50 Mio. Euro, über 50 Mio. Euro), wobei diese Gruppen wiederum in Untergruppen unterteilt sind (das Bußgeldkonzept gruppiert dabei alleine nach den Umsatzzahlen, anders als die EU-KMU-Empfehlung, die u.a. auch die Mitarbeiterzahl berücksichtigt).

2. Im nächsten Schritt wird der mittlere Jahresumsatz der jeweiligen Untergruppe ermittelt.

3. Danach erfolgt die Berechnung des wirtschaftlichen Grundwertes. Dieser ist der durchschnittliche Tagesumsatz einer Unternehmensuntergruppe; rechnerisch wird dafür der mittlere Jahresumsatz durch 360 (Tage) geteilt. Abweichendes gilt nur für Unternehmen mit einem jährlichen Umsatz von über 500 Mio. Euro; bei dieser Unternehmensgröße ist der konkrete Jahresumsatz des betroffenen Unternehmens Berechnungsgrundlage.

   > Beispielsweise beliefe sich der wirtschaftliche Grundwert („Tagessatz“) im Falle eines Unternehmens mit einem Vorjahresumsatz von 42 Mio. Euro (mittleres Unternehmen, C.VII; also einem mittleren Jahresumsatz von 45 Mio. nach Tabelle 2) auf 125.000 Euro.

4. Der so ermittelte Tagessatz wird dann – nach einem Punktesystem – je nach Schweregrad der Tat mit einem Faktor von 1

bis „12<“ multipliziert. Die Schwere der Tat richtet sich nach den konkreten Umständen des Einzelfalls. Vorgesehen sind die Schweregrade „leicht“, „mittel“, „schwer“ und „sehr schwer“. Je nachdem, ob es sich um einen formellen (Art. 83 Abs. 4 DSGVO) oder einen materiellen (Art. 83 Abs. 5, 6 DSGVO) Verstoß handelt, ist ein unterschiedlicher Faktor zu wählen. Materielle Verstöße gegen die DSGVO (z.B. fehlende Verarbeitungserlaubnis) werden schwerer geahndet als formelle Verstöße (z.B. Zertifizierungsanforderungen werden nicht erfüllt).

Bei unserem Beispielunternehmen beliefe sich demnach das Bußgeld je nach Natur des Verstoßes (formell oder materiell) und Schweregrad des Verstoßes zwischen 125.000 Euro bis 1,5 Mio. Euro. Stellen wir uns nun ein datenschutzrechtliches worst case scenario vor, unser Beispielunternehmen verkauft vorsätzlich Gesundheitsdaten seiner Versicherungsnehmer ohne Einwilligung an Google; dann beliefe sich das Bußgeld voraussichtlich auf 1,5 Mio. Euro, bei einem nicht aktualisierten Verarbeitungsverzeichnis bewegte sich das Bußgeld eher am unteren Ende des Korridors, wenn nicht nur eine Verwarnung erfolgt.

5. Im letzten Schritt werden dann die bisher noch nicht berücksichtigten für oder gegen den Betroffenen sprechenden Umständen wie z.B. eine lange Verfahrensdauer oder eine drohende Zahlungsunfähigkeit des Unternehmens (vgl. Kriterienkatalog des Art. 83 Abs. 2 DSGVO) betrachtet und der errechnete Betrag dementsprechend angepasst.

Die Veröffentlichung des Konzepts erleichtert die Beurteilung von Bußgeldrisiken im Zuständigkeitsbereich deutscher Aufsichtsbehörden. Denn es ermöglicht Unternehmen, den Umfang zu erwartender Geldbußen im Vorfeld grob abzuschätzen. Zudem können eventuelle Bußgeldentscheidungen besser nachvollzogen und – insbesondere, wenn das endgültige Konzept zukünftig zu bindender Verwaltungspraxis wird – gerichtlich überprüft werden.

Zukünftige Veränderungen und Ergänzungen des Konzepts, sowie der Praxis der Aufsichtsbehörden bleiben aber möglich. Die DSGVO verlangt, dass eine europaweite Harmonisierung der Festsetzung von Geldbußen durch Leitlinien zu fördern ist (vgl. Art. 70 Abs. 1 lit. k DSGVO). Diese europaweiten Leitlinien würden vor-

rangig gelten und müssen vom Europäischen Datenschutzausschuss (EDSA) gestellt werden. Bis es aber dazu kommt, stellt das vorliegende Datenschutzkonzept die Marschroute der deutschen Aufsichtsbehörden dar.

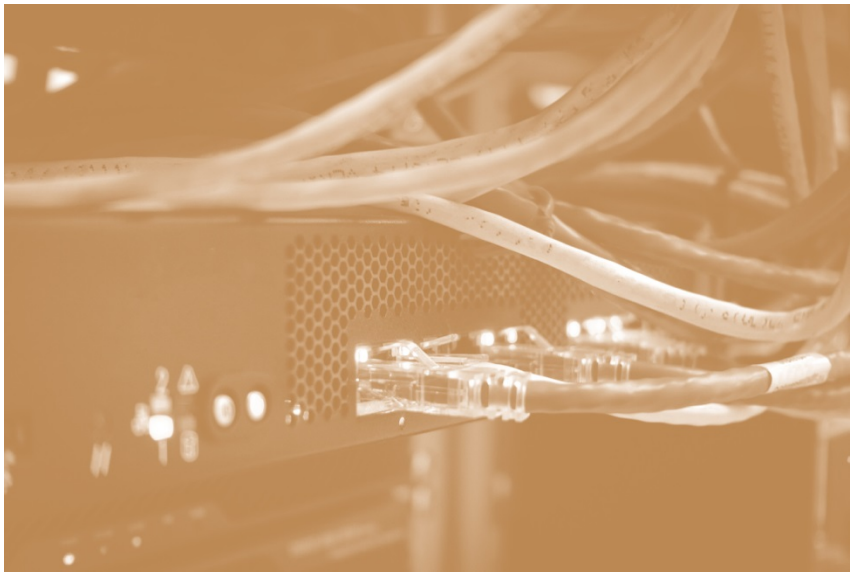
Beschwerden gegen Einsatz von Google Analytics

Das weit verbreitete Analysetool Google Analytics ist offenbar Anlass zahlreicher Beschwerden bei Datenschutzaufsichtsbehörden: Berichtet wird von bundesweit 200.000 Fällen. Nun hat sich am 14. November 2019 auch die Berliner Beauftragte für Datenschutz und Informationsfreiheit in einer Pressemitteilung geäußert. Nach ihrer Auffassung ist die Nutzung von Google Analytics nur mit Einwilligung zulässig.

Die hohe Beschwerdezahl sowie das Planet49-Urteil des EuGH bieten für die Behörden ausreichend Anlass, sich den Einsatz von Google Analytics sowie vergleichbarer Third Party-Analyse-Tools genauer anzusehen. Der baden-württembergische Landesbeauftragte für Datenschutz und Informationsfreiheit hatte bereits vor dem Planet49-Urteil (dazu ausführlich unser Newsletter vom Oktober) angedeutet, dass Cookies, die Daten an Dritte wie Google übermitteln, stets einer aktiven Einwilligung bedürfen. Dieser Einschätzung hat sich nun auch jüngst die Berliner Beauftragte für Datenschutz und Informationsfreiheit angeschlossen:

Webseiten-Betreiber benötigten eine Einwilligung der Besucherinnen und Besucher ihrer Webseiten, wenn darin Dritt-Dienste eingebunden werden sollen, bei denen der Anbieter dadurch erlangte personenbezogene Daten auch für eigene Zwecke nutze. Dazu gehöre auch das Produkt Google Analytics. Allerdings bedürfe nicht jeder Einsatz von Analysetools eines Drittanbieters der Einwilligung. Stets einwilligungsbedürftig ist nach Auffassung der Berliner Beauftragten für Datenschutz und Informationsfreiheit Google Analytics deswegen, weil sich Google Analytics mittlerweile vorbehalte, die Daten für eigene Zwecke zu verwenden. Gleiches gelte, wenn das Verhalten der Webseiten-Besucherinnen und -Besucher im Detail nachvollzogen und aufgezeichnet werden kann, etwa wenn Tastatureingaben, Maus- oder Wischbewegungen erfasst werden.

Anbieter, die sich nicht vorbehalten, erhobenen Daten zu eigenen Zwecken zu verwenden, können somit prinzipiell auch nach der Auslegung der Berliner Beauftragten für Datenschutz und Informationsfreiheit ohne Einwilligung als Auftragsverarbeiter eingesetzt werden – wenn eine Einwilligung nicht aus anderen Gründen erforderlich ist, wie z.B. beim Einsatz persistenter Cookies zum Zwecke websiteübergreifenden Retargetings. Sollten Sie sich nun fragen, ob ein von Ihnen eingesetztes Analysetool und die dazu verwendeten Cookies einer Einwilligung bedürfen, bietet Ihnen unsere Cookie-Ampel Hilfestellung.



Datenverarbeitung zur Vertragserfüllung: Was ist erlaubt?

Werden personenbezogene Daten im Rahmen eines Vertragsverhältnisses verarbeitet, kann dies über Art. 6 Abs. 1 lit. b DSGVO erlaubt sein. Der Vorteil: Unternehmen sind dann weder auf eine Einwilligung angewiesen, noch auf eine oftmals unsichere Interessenabwägung. Hierfür muss die Datenverarbeitung für die Erfüllung des Vertrags jedoch erforderlich sein. Der Europäische Datenschutzausschuss (EDSA) positioniert sich zur Frage der Erforderlichkeit in seinen jüngst veröffentlichten Leitlinien überaus restriktiv und engt die Vertragsgestaltungsfreiheit enorm ein. Was das in der Praxis bedeutet, erläutern wir in diesem Beitrag.

Vertragserfüllung als Erlaubnis

Der Erlaubnisgrund der Vertragserfüllung hat für Unternehmen zwei große Vorteile: Er erzeugt erstens keinen operativen Zusatzaufwand wie die Einwilligung und bietet zweitens – im Gegensatz zur Abwägung widerstreitender Interessen – ein hohes Maß an Rechtssicherheit. Grundvoraussetzung ist ein wirksamer Vertrag oder eine Vertragsanbahnung **zwischen dem Datenverarbeiter und dem Betroffenen**. Vertragsverhältnisse, aus denen der Betroffene lediglich profitiert, deren Vertragspartei er aber nicht ist, sind nicht ausreichend; damit verbundene Datenverarbeitungen können etwa aus berechtigten Interessen erlaubt sein.

Erforderlichkeit bis hin zur Vertragskontrolle?

Die Datenverarbeitung muss für die Durchführung des Vertrags **erforderlich** sein. Nach Ansicht des EDSA ist die Erforderlichkeit strikt objektiv zu bestimmen. Das gilt in mehrerlei Hinsicht:

- **Anknüpfung an Leistungserbringung**: Die Datenverarbeitung ist für die Durchführung des Vertrags nur dann erforderlich, wenn die vereinbarte Leistung andernfalls nicht erbracht werden kann; Beispiel: Verarbeitung von Adress- und Bankdaten bei Onlinebestellungen. Auch Beanstandungen von Warenlieferungen und Zahlungsaufforderungen bzw. -erinnerungen sind erforderlich.

- **Hypothetische Betrachtung**: Wenn die konkrete Vertragspflicht auch ohne die Datenverarbeitung erbracht werden

kann, ist sie nicht mehr erforderlich. Beispiel: Das Profiling über die Einkaufsvorlieben eines Kunden ist nicht mehr erforderlich für die Durchführung eines Kaufvertrags, da die Abwicklung des Kaufvertrags auch ohne das Profiling durchgeführt werden könnte. Das soll auch für Datenverarbeitungen, zum Zweck der Serviceverbesserung gelten.

- **Objektive Vertragskontrolle:** Bemerkenswert ist, dass es zudem nicht ausreichen soll, dass eine Datenverarbeitung im Vertrag als notwendig vereinbart oder vorausgesetzt wird. Die Erforderlichkeit soll insbesondere nicht „künstlich" durch entsprechende Abreden oder Klauseln im Vertrag herbeigeführt werden dürfen. Bei der Beurteilung der Erforderlichkeit komme es vielmehr auf den zwischen den Parteien vereinbarten Vertragszweck an. Dabei ist nicht nur auf die Sicht des datenverarbeitenden Unternehmens, sondern auch auf die Sicht des Betroffenen und dessen berechtigte Erwartungen abzustellen. Diese harmlos anmutenden Ausführungen haben indes massive Auswirkungen auf die Privatautonomie, denn sie führen zu einer objektiven Vertragskontrolle durch die Behörden. Künftig sollen also Behörden entscheiden, welche Vertragsinhalte „typisch" und damit datenschutzrechtlich unbedenklich sind und welche „untypisch" sind und daher keine Rechtfertigung für eine Datenverarbeitung bieten können.

Konkrete Anwendungsbeispiele

Der EDSA konkretisiert seine Position anhand einiger Beispiele:

- Datenverarbeitungen zur Betrugsprävention (z.B. durch Profiling) gingen i.d.R. über das Erforderliche hinaus und könnten daher nicht über Art. 6 Abs. 1 lit. b DSGVO gerechtfertigt werden.

- Ebenso nicht erforderlich ist die Verarbeitung von Daten zum Zweck der verhaltensbasierten Online-Werbung (Tracking und Profiling); selbst, wenn die Erbringung der Dienstleistung – z.B. die Zurverfügungstellung einer Plattform – indirekt über die personalisierte Werbung finanziert werde. Auch die Personalisierung von sonstigen Diensten ist nach Ansicht des Ausschusses nur schwer über Art. 6 Abs. 1 lit. b DSGVO zu rechtfertigen: Nicht erforderlich seien beispielsweise Da-

tenverarbeitungen, die den Nutzer dazu ermuntern sollen, stärker mit dem Dienst zu interagieren. Etwa die Profilbildung über einen Nutzer anhand früherer Hotelbuchungen, die genutzt werden soll, um dem Nutzer gezielt personalisierte Hotelvorschläge machen zu können, sei daher nicht erforderlich für den Vertrag. Die genutzten Finanz- und Verhaltensdaten seien vielmehr nur für den in der Vergangenheit geschlossenen Vertrag erforderlich aber nicht mehr für einen zukünftigen Vertrag.

Praxishinweis

Fehlt es an der Erforderlichkeit der Datenverarbeitung für den Vertrag, kann sie immer noch auf Grundlage einer anderen Rechtsgrundlage aus Art. 6 Abs. 1 DSGVO rechtmäßig sein; insbesondere eine Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) oder die berechtigten Interessen des Datenverarbeiters (Art. 6 Abs. 1 lit. f DSGVO) kommen als Grund in Betracht. Bei der Einholung einer Einwilligung in Datenverarbeitungen, die nicht mehr erforderlich für die Vertragsdurchführung sind, ist allerdings das Kopplungsverbot (Art. 7 Abs. 4 DSGVO) zu beachten: Hiernach darf die Durchführung eines Vertrags nicht an die Erteilung einer Einwilligung in diejenigen Datenverarbeitungen gekoppelt werden, die für die Vertragsdurchführung gerade nicht mehr erforderlich sind. Auch die Einzelheiten des Kopplungsverbots sind indes höchst streitig – bei Fragen hierzu helfen wir Ihnen natürlich gerne weiter.

Zusammenfassend lässt sich folgendes festhalten: Durch die strikt objektive Auslegung des Erforderlichkeitskriteriums in Art. 6 Abs. 1 lit. b DSGVO zieht der EDSA den Anwendungsbereich des Erlaubnistatbestandes sehr eng. Insbesondere werden die vertraglichen Gestaltungsmöglichkeiten datenintensiver Produkte geringer; die (Fort-) Entwicklung neuer Geschäftsmodelle in der digitalen Welt und Innovationen werden behindert. In der Sache überzeugt die restriktive Auslegung des EDSA auch nicht; auf dieser Auslegung fußende Bescheide einer Datenschutzaufsichtsbehörde können und sollten gerichtlich überprüft werden – je nach Fallgestaltung durchaus mit guten bis sehr guten Erfolgsaussichten. Die Leitlinien stellen ohnehin nur eine zentrale Auslegungshilfe für die Aufsichtsbehörden dar, sie ist aber für Gerichte rechtlich nicht bindend.

ePrivacy-Verordnung: Ein neuer Anlauf

Die ePrivacy-Verordnung wird gerne als kleine Schwester der DSGVO bezeichnet und hätte ebenfalls im Mai 2018 in Kraft treten sollen. Seit langem ringen die Mitgliedstaaten jedoch um eine Einigung bei der Ausgestaltung – bislang vergebens. Nun hat die finnische Ratspräsidentschaft einen neuen Anlauf gestartet und bemüht sich mit neuem Elan, bis zum Jahresende um eine konsensfähige Fassung. Für uns Grund genug, Ihnen zentrale Aspekte des neuen, aktuellen Verordnungsentwurfs vom 8. November 2019 vorzustellen.

Die ePrivacy-Verordnung löst die seit 2001 und als veraltet geltende ePrivacy-Richtlinie ab und regelt den Schutz der Privatsphäre in der elektronischen Kommunikation. Die ePrivacy-Verordnung ist sachlich nicht auf den Umgang mit personenbezogenen Daten beschränkt, sondern macht ganz grundsätzlich Angaben dazu, welche Daten eines Endnutzers unter welchen Voraussetzungen verarbeitet werden dürfen. Das betrifft unter anderem den Besuch von Websites oder den Einsatz von Cookies.

Die ePrivacy-Verordnung wird u.a. für Webseitenbetreiber und App-Anbieter relevant, insbesondere mit Blick auf die Regeln über die zukünftige Zulässigkeit der Verfolgung von Nutzeraktivitäten (sog. Tracking), unter anderem durch den Einsatz von Cookies. Neben dem Online-Tracking, wird die Verordnung auch das sog. Offline-Tracking z.B. mittels Bluetooth und *beacons* in Einkaufszentren oder Supermärkten – regulieren. Die rechtliche Kernfrage ist

dabei nach wie vor, welche Tools ohne Einwilligung der Betroffenen eingesetzt werden dürfen. Der aktuelle Entwurf deutet etwa in drei wesentlichen Punkten in folgende Richtung:

- *Cookies zur Messung des Webpublikums / Reichweitenmessung*: Cookies, die für die Messung des Webpublikums nötig sind, sollen keiner Einwilligung bedürfen. Ob und unter welchen Voraussetzungen die Messung des Webpublikums durch Drittanbieter (sog. Third Parties) ohne Einwilligung erfolgen darf, ist noch offen. Die Tendenz deutet hin zu einer Zulässigkeit, solange der Drittanbieter Auftragnehmer i.S.d. Art. 28 DSGVO ist. In diesen Kontext sind etwa Dienste wie Google Analytics zu verorten, wobei genau zu prüfen ist, ob diese tatsächlich als Auftragnehmer agieren.

- *Anforderungen an Tracking-Cookies und andere Tracking-Instrumente:* Für das individuelle Tracking einzelner Nutzer über verschiedene Webseiten hinweg – beispielsweise um auf deren Surf-Verhalten Werbung abzustimmen – soll stets eine Einwilligung erforderlich sein.

- *Art und Weise der Erteilung der Einwilligung des Nutzers:* Weiterer Diskussionspunkt ist die Frage, wie die Endnutzer eine Einwilligung abgeben (oder verweigern) können. Explizit zulässig ist die Nutzung „angemessener technischer Softwareeinstellungen" – es soll den Endnutzern eine übersichtlichere, einfacher handhabbare Möglichkeit geschaffen werden, Einwilligungen abzugeben und im Blick zu behalten, als dies aktuell der Fall ist. Im Raum steht dabei insbesondere, ob die Endnutzer ihre Präferenzen hinsichtlich der Einwilligung generell über ihre Browser-Einstellungen kommunizieren können sollen oder ob stets eine Einzelfalleinwilligung notwendig sein soll. Klargestellt werden soll, dass es für Nachweis einer abgegebenen Einwilligung dort, wo etwa der Website-Betreiber seine Nutzer nicht namentlich kennt, ausreicht, wenn protokollarisch die Abgabe der Einwilligung mit dem entsprechenden technischen Equipment nachweisbar ist.

Um eine effektive Anwendung der Regeln der ePrivacy-Verordnung zu gewährleisten, soll das Sanktions- und Bußgeldregime an das der DSGVO angelehnt (und damit gegenüber dem status quo ganz erheblich verschärft) werden. Als Aufsichtsbehörden

sollen die Behörden berufen werden, die auch für die Durchsetzung der Datenschutz-Grundverordnung zuständig sind.

Wann und mit welchem Inhalt die ePrivacy-Verordnung letztlich in Kraft tritt, bleibt abzuwarten. Auch im Zuge der DSGVO-Verhandlungen konnte indes zum Jahresende 2015 überraschend schnell Einigkeit erzielt werden. Unternehmen tun daher gut daran, sich auf die neue Rechtslage vorzubereiten.

Die Anforderungen der ePrivacy-Verordnung werden daher auch Inhalt unserer 3. Veranstaltung im Forum Digitalisierung „Digitaler Vertrieb“ am 22. Januar 2019 sein – weitere Informationen dazu finden Sie hier. Über Ihre Teilnahme würden wir uns sehr freuen.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Lucyne Ghazarian
+49 (0)221 65065-222
lucyne.ghazarian@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de