LOSCHELDER

Newsletter Datenschutzrecht

Februar 2021

Sehr geehrte Damen und Herren,

auch unser zweiter Newsletter des Jahres ist prall gefüllt: Ein Gesetzentwurf deutet auf neue Vorgaben für die Speicherung von Werbeeinwilligungen hin und die EU-Ratspräsidentschaft Portugals hat jüngst einen neuen Entwurf der ePrivacy-Verordnung veröffentlicht, der nunmehr in die Abstimmung geht. Darüber hinaus gibt es Neues in Sachen „datenschutzkonformer Einsatz von Microsoft-Produkten“ und der Generalanwalt beim EuGH hat sich mit der Frage beschäftigt, ob und wann IP-Adressen datenschutzkonform verwendet werden dürfen. Zudem fassen wir Ihnen die neuen Leitlinien des EDSA zum Umgang mit Datenlecks knapp zusammen und präsentieren – wie üblich – im Beitrag „Zu guter Letzt“ einige spannende Aufsichtsverfahren und Bußgeldfälle.

Bemerkenswert ist zudem, dass sich laut Medienberichterstattung bereits ein Angemessenheitsbeschluss der EU-Kommission für UK abzeichnet, jüngst berichtete dazu auch das Handelsblatt. Dies würde, ungeachtet der berechtigten Kritik, den Datenaustausch mit UK rechtlich absichern und vermeiden, dass es zu ähnlichen Schwierigkeiten kommt, wie diese aktuell für US-Transfers (und auch den Einsatz von US-Tools) bestehen.

In eigener Sache möchten wir uns denn auch herzlich für ihr reges und aktive Interesse an unserem Lunch@Loschelder-Webinar zur Digitalisierung mit oder ohne US-Tools bedanken. Unsere Webinar-Reihe zu aktuellen Digitalisierungsthemen wird in den beiden nächsten Monaten fortgesetzt:

Digitalisierung II: Apps und Services aus „Standardbausteinen“
Was ist urheberrechtlich zu beachten, insbesondere bei Nutzung von Open Source-Elementen?
Mittwoch, den 10.03.2021: 12.00 bis 12.30 Uhr
Dr. Patrick Pommerening / Dr. Hans-Georg Schreier, LL.M.

Digitalisierung III: Neues für Verträge über digitale Inhalte und Dienste
Die größte Reform des BGB seit dem Schuldrechts-modernisierungsgesetz? Wir geben einen Überblick über die anstehenden Änderungen durch die neuen EU-Vorgaben, die zum 01.07.2021 umzusetzen sind.
Mittwoch, den 14.04.2021: 12.00 bis 12.30 Uhr
Dr. Kristina Schreiber / Dr. Hans-Georg Schreier, LL.M.

Zur Anmeldung genügt eine E-Mail an webinare@loschelder.de mit Angabe des gewünschten Webinars; diese sind kostenfrei.

Inhalt

Gesetzesentwurf: Pflicht zur Aufbewahrung von Werbeeinwilligungen für 5 Jahre

Die Verarbeitung personenbezogener Daten zu Werbezwecken erfordert in vielen Fällen eine Einwilligung. Diese muss vom Unternehmen im Streitfall nachgewiesen werden. Wird eine Einwilligung widerrufen, kann die Nachweispflicht dies überdauern, wenn etwa noch Verfahren drohen. Die Bundesregierung legte nun jüngst einen Gesetzesentwurf vor, der die Anforderungen an Speicherung und Nachweis abgegebener Einwilligungserklärungen neu regelt – und das versteckt: Die Regelung findet sich in einem Entwurf zur Überarbeitung des UWG.

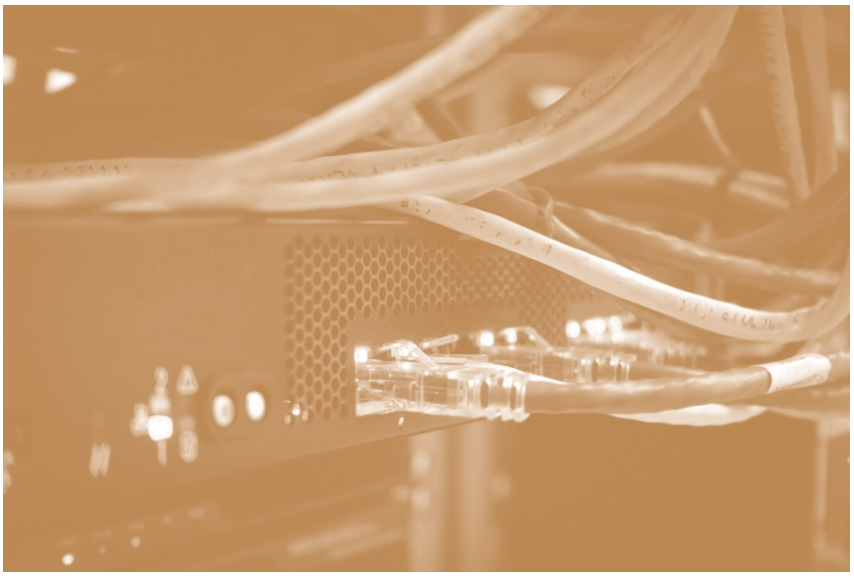
Am 01.01.2021 legte die Bundesregierung den „Entwurf eines Gesetzes für faire Verbraucherverträge“ vor. In dessen Artikel 3 wird die Schaffung eines neuen § 7a UWG vorgeschlagen, der eine Dokumentations- und Aufbewahrungspflicht für Werbe-einwilligungen im Zusammenhang mit Telefonwerbung vorsieht.

Nach § 7a Abs. 1 UWG-Entwurf muss derjenige, der mit einem Telefonanruf gegenüber einem Verbraucher wirbt, dessen vorherige ausdrückliche Einwilligung in die Telefonwerbung zum Zeitpunkt der Erteilung in einer angemessenen Form dokumentieren. Dieser Nachweis ist nach § 7a Abs. 1 S. 1 UWG-Entwurf ab Erteilung der Einwilligung sowie nach jeder Verwendung der Einwilligung - sprich nach jedem Telefonanruf zwecks Werbung - von dem werbenden Unternehmen **5 Jahre** lang aufzubewahren. Auf Verlangen der zuständigen Verwaltungsbehörde, namentlich der Bundesnetzagentur, muss der Nachweis nach § 7a Abs. 2 S. 2 UWG-Entwurf unverzüglich vom werbenden Unternehmen vorgelegt werden können.

Die Bundesregierung begründet den Gesetzesvorschlag damit, dass im Ordnungswidrigkeitenverfahren, anders als im zivilrechtlichen Verfahren oder nach Art. 7 Abs. 1 DSGVO nicht der Werbende, sondern die Behörde die Darlegungs- und Beweislast für das Vorliegen der Einwilligung trage, was u.U. ein umfangreiches und umständliches Verfahren nach sich ziehe. Zudem will die Bundesregierung durch die Einführung einer Dokumentationspflicht dazu beitragen, dass unerlaubte Telefonwerbung effektiver sanktioniert werden kann und weniger Anreize für diese Praxis bestehen.

Ob diese Aufbewahrungsfrist auch andere Einwilligungen erfasst und die datenschutzrechtlichen Aufbewahrungspflichten beeinflusst, wird aktuell bereits streitig diskutiert – und auch, ob die Vorgabe des § 7a UWG-Entwurfs überhaupt mit Art. 7 Abs. 1 DSGVO vereinbar ist.

Wird § 7a UWG-Entwurf in der vorgeschlagenen Art umgesetzt, müssen Unternehmen künftig Dokumente, die den Nachweis der Einwilligung in die Telefonwerbung erbringen, für 5 Jahre nachdem der letzte Telefonanruf vorgenommen wurde archivieren. Einiges spricht dafür, dass die Rechtsgrundlage für die damit einhergehende Verarbeitung personenbezogener Daten dann in § 7a Abs. 2 UWG-Entwurf i.V.m. Art. 6 Abs. 1 lit. c DSGVO liegt. Abzuwarten ist, ob die Vorgabe auch auf andere Einwilligungen und diesbezügliche Aufbewahrungsdauern übertragen wird.



Entwurf der X-te – Hat der neue ePrivacy-VO Aussicht auf Erfolg?

Die ePrivacy-Verordnung, mit der Regelungen zum Schutz der Privatsphäre und der Vertraulichkeit bei der Nutzung von elektronischen Kommunikationsdiensten europaweit vereinheitlicht und angepasst werden sollen, beschäftigt die EU nun schon seit mehreren Jahren. Ursprünglich sollte sie zeitgleich mit der DSGVO ergehen, eine Einigung für die Regelung der Nutzung von Cookies & Co. konnte aber bis heute nicht gefunden werden. Unter der neuen EU-Ratspräsidentschaft

Portugals ist nun ein neuer Entwurf veröffentlicht worden, der viele Änderungen gegenüber dem letzten – abgelehnten – Entwurf vorsieht. Einiges spricht dafür, dass diese neuste Fassung erstmals mehr Aussicht auf eine Einigung hat…

Die ePrivacy-Verordnung ist neben der DSGVO eines der wichtigsten Großprojekte der EU in Sachen „Datenschutz- und Datensicherheit" der letzten Jahre, um die Regelungen zur Verarbeitung von Daten zukunftsfest zu machen. Während die DSGVO den Fokus auf die Verarbeitung personenbezogener Daten legt, soll die ePrivacy-Verordnung den Umgang auch mit nicht-personenbezogenen Daten im Bereich der elektronischen Kommunikationsdienste regeln. Aktuell gilt dort noch die EU-Richtlinie 2002/58/EG, die zuletzt 2009 geändert wurde. Auch, weil diese Regelungen in weiten Teilen Unternehmen der Internetwerbeindustrie und Telekommunikationsdienstleistungen treffen, wird seit mehreren Jahren über die Ausgestaltung der ePrivacy-Verordnung diskutiert. Wesentliches Streitthema sind die Zulässigkeitsbedingungen für die Nutzung von Cookies & Co (wir berichteten über verschiedene Entwurfsversionen etwa in unseren Newslettern vom November 2019).

Nun scheint mit dem jüngsten Entwurf (abrufbar hier in der englischen Fassung) ein wichtiger Schritt in Richtung Einigung getan. Am 10. Februar 2020 beschlossen die Mitgliedsstaaten, der Ratspräsidentschaft die Verhandlungsmacht für Verhandlungen mit dem Europäischen Parlament über diese Entwurfsfassung zu gewähren. Die Ratspräsidentschaft ist bemüht, mit ihrem Entwurf den Geist und die Systematik der vorherigen Entwürfe zur ePrivacy-Verordnung beizubehalten, gleichzeitig aber die Regelungen zu vereinfachen und die Annäherung an die DSGVO voranzutreiben.

Zu den wesentlichsten Änderungen gehören:

- **Klare Definition „Location Data":** Location oder auch Geo-Daten, als typischer Unterfall der Metadaten, sind nun ausdrücklich in dem Entwurf definiert. Dies war bisher nicht der Fall und könnte bei der späteren Anwendung der Verordnung die Abgrenzung erleichtern.

- **Weiterverarbeitung von Metadaten**: Nach dem neuen Entwurf soll das Weiterverarbeiten von Metadaten und

sonstigen elektronischen Kommunikationsdaten zulässig sein, solange dies mit dem ursprünglichen Zweck der Datenerhebung vereinbar ist. Eine vorherige Version dieser Vorschrift, die ebensolche Weiterverarbeitung ausgeschlossen hatte, wurde aus dem Entwurf gestrichen.

- **Verarbeitung zur Erfüllung vertraglicher Verpflichtungen**: Die Verarbeitung von Telekommunikations- und Metadaten soll ohne Einwilligung zudem zulässig sein, wenn dies zur Erfüllung vertraglicher Verpflichtungen, insbesondere zur Erbringung von Telekommunikationsdienstleistungen, erforderlich ist. In einem vorherigen Entwurf war die Verarbeitung solcher Daten ohne Einwilligung nur gestattet, wenn dies für die Durchführung der elektronischen Kommunikation selbst erforderlich war. Wie viel mehr Spielraum mit dieser Änderung verbunden ist, bleibt angesichts der aktuell engen Interpretation der „Vertragserfüllung" unter Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO abzuwarten.

- **Zugriff auf Endgeräte**: Die Diensteanbieter sollen nun Zugriff auf die Daten auf den Endgeräten der Nutzer haben, wenn und soweit dies für die Erfüllung des Vertrages erforderlich ist. Zuvor war in den Entwürfen nur der Zugriff aufgrund der technischen Notwendigkeit gestattet. Dies betrifft etwa das Setzen von Cookies, Auslesen von Informationen oder die Nutzung des local storage. Auch hier wird sich in der Praxis insbesondere die Frage stellen, was „für die Erfüllung des Vertrages erforderlich ist" – die Neuregelungen zum digitalen Produktvertragsrecht deuten aber ohnehin auf einen weit verstandenen Vertragsschluss hin, so dass viele Online-Angebote künftig als vertragliches Angebot zu sehen sein dürften. Die Details sind hier höchst umstritten.

- **Vereinfachte Einwilligung in Cookies:** Die Einwilligung in den Einsatz von Cookies soll dadurch erleichtert werden, dass nun Voreinstellung im Browser hinsichtlich bestimmter Cookies oder Einsatzzwecke möglich seien sollen. Damit sollen einerseits die strengen Anforderungen der Einwilligung in den Cookie-Einsatz eingehalten werden, andererseits Internetnutzern der Besuch von Websites erleichtert werden – es entfiele dann das aufwändige „Durchklicken" von Consent Management Tools auf jeder

einzelnen Website, soweit Voreinstellungen getroffen wurden. Erforderlich für ein „Whitelisting“ bestimmter Cookies ist jedoch, dass die Nutzer dies selbst aktiv in ihren Browsereinstellungen vornehmen – ansonsten lägen die Voraussetzungen einer aktiven, vorherigen Einwilligung nicht vor.

- **Teilen anonymisierter Telekommunikationsdaten**: Soweit Telekommunikationsdaten anonymisiert mit Dritten geteilt werden sollen, haben die Verarbeiter nach dem Entwurf eine Datenschutzrisikoabwägung vorzunehmen und die Endnutzer zu informieren. Diese Regelung ist neu hinzugekommen.

Diese Änderungen, insbesondere die Streichung einiger strengerer Regelungen zur Verarbeitung von Metadaten, fanden nicht überall Zustimmung. Der Europäische Datenschutzausschuss (EDSA) forderte in seiner Rolle als Zusammenschluss europäischer Datenschutzaufsichtsbehörden in einer Stellungnahme nach der Veröffentlichung des Entwurfs unter anderem, dass die Verarbeitung von Metadaten ohne Einwilligung nur anonymisiert erfolgen sollte. Zudem sollten Regelungen geschaffen werden, die es den Datenschutzaufsichtsbehörden auch ermöglicht, die Überwachung über die Einhaltung der ePrivacy-Verordnung vorzunehmen.

Ob dieser Entwurf nun erfolgreicher sein wird als seine Vorgänger, bleibt abzuwarten. Die Vorzeichen sind angesichts des Verhandlungsmandats der Mitgliedstaaten jedenfalls besser als für frühere Entwürfe.

DSK-Studie zur Telemetriedatenübertragung bei Windows 10 Enterprise

Jüngst haben Datenschützer aus Niedersachsen und Bayern gemeinsam die Datenübertragung bei der Nutzung von Windows 10 Enterprise untersucht. Parallel hatte das Bundesamt für Sicherheit und Informationstechnik (BSI) eine ähnliche Studie zu Telemetriedatenübertragung durchgeführt. Die Konferenz der deutschen Datenschutzbehörden, die DSK, hat im November das Ergebnis dieser Untersuchungen veröffentlicht. Für die Praxis bringt dies hilfreiche Informationen zum datenschutzkonformen Einsatz.

Schon im November 2019 hatte die DSK, die Konferenz der deutschen Datenschutzaufsichtsbehörden, ein Prüfschema für die Nutzung von Windows 10 veröffentlicht. Im Oktober 2020 kam es zwischen den Aufsichtsbehörden zu einem Konflikt über die datenschutzrechtliche Beurteilung von Office 365. Damals hatte die knappe Mehrheit der Datenschutzbehörden für einen Beschluss gestimmt, der die Datenverarbeitung durch die Produkte für rechtswidrig befand. Andere Aufsichtsbehörden positionierten sich insb. wegen methodischer Mängel gegen den Beschluss – wir berichteten ausführlich in unserem Newsletter aus Oktober 2020 über diese Kontroverse.

Diese Datenschutzaufsichtsbehörden haben, in Kooperation mit den LfDI Mecklenburg-Vorpommern und dem Bundesbeauftragten für

Datenschutz und Informationsfreiheit (BfDI), in einer neuen Arbeitsgruppe die Telemetriedatenverarbeitung bei Windows 10 untersucht. Das Ergebnis hat die DSK Ende November 2020 veröffentlicht (hier abrufbar). Daneben kam es zu einer Untersuchung durch das Bundesamt für Sicherheit und Informationstechnik (BSI), in der ebenfalls die Telemetriedatenverarbeitung bei Windows 10 genauer unter die Lupe genommen wurde. Auch die Ergebnisse dieser Studie veröffentlichte die DSK in ihrem Bericht. Gemein haben beide Untersuchungen auch, dass mit dem Microsoft-Konzern zusammengearbeitet wurde – etwas, was vor dem Beschluss aus Oktober 2020 nicht geschah.

Deaktivierung der Telemetriedatenübertragung? – Jedenfalls teilweise!

Beide Untersuchungen beschränkten sich dabei auf die Telemetriedatenverarbeitung bei *Windows 10 Enterprise* – die anderen Windows 10 Angebote *Home* oder *Pro* wurden nicht untersucht. Grund hierfür ist, dass es bei der *Enterprise*-Version die Möglichkeit der Einstellung einer „Telemetriestufe Security" gibt, mit der nach den Aussagen des Herstellers in Kombination mit einem Zusatzprotokoll („Windows Restricted Traffic Limited Functionality Baseline" – V1903) die Übertragung von Telemetriedaten an Microsoft vollständig ausgestellt werden kann. Ob dies tatsächlich stimmt, wollte die DSK-Arbeitsgruppe herausfinden.

Hierzu machte die Arbeitsgruppe verschiedene Praxistests mit *Windows 10 Enterprise*, teilweise mit dem Zusatzprotokoll und der Einstellung „Telemetriestufe Security" und teilweise ohne. Das Ergebnis wurde vorsichtig erfreulich formuliert: Die Arbeitsgruppe konnte nicht feststellen, dass die Aussagen von Microsoft nicht stimmen. Das heißt, zumindest bei der Nutzung von *Windows 10 Enterprise* mit der Einstellung „Telemetriestufe Security" und der Verwendung des Zusatzprotokolls kann die Übertragung von Telemetriedaten unterbunden werden.

Weniger positiv scheint das Ergebnis der BSI-Studie zu sein, die sich ebenfalls mit *Windows 10 Enterprise* und dem Zusatzprotokoll befasste. Hier kam es im Testverlauf zu einer Datenübertragung an einen Endpunkt, bei dem zumindest die Möglichkeit besteht, dass Microsoft einseitig die technischen Vorgaben so anpasst, dass

Telemetriedaten gesammelt werden können. Das BSI geht in seinen Analysen und Hinweisen in der Regel vom „worst-case“-Szenario aus; deshalb empfiehlt es zur effektiven und sicheren Vermeidung der Datenübertragung an Microsoft, die Geräte nicht ans Netz anzuschließen.

Wann dürfen IP-Adressen datenschutzkonform verarbeitet werden?

In einem aktuellen Vorabentscheidungsverfahren zu Fragen der rechtlichen Verfolgung von Schadensersatzansprüchen wegen unerlaubten Teilens urheberrechtlich geschützter Werke in Peer-to-Peer-Netzwerken bekommt der EuGH Gelegenheit, zu einer grundlegenden datenschutzrechtlichen Frage Stellung zu nehmen: Wann ist die Erhebung und Speicherung von IP-Adressen zum Zwecke der Verfolgung von privatrechtlichen Rechtsansprüchen datenschutzrechtlich zulässig? Am 17.12.2020 wurden die Schlussanträge des Generalstaatsanwaltes dazu veröffentlicht. Meist folgt der EuGH den Schlussanträgen. Wir erläutern Ihnen im Folgenden die Hintergründe und stellen Ihnen die Argumentation des Generalstaatsanwaltes vor.

Dem Verfahren vor dem EuGH liegt ein Rechtsstreit zwischen dem zypriotischen Unternehmen Microm und dem belgischen Internetzugangsbetreiber Telenet zugrunde. Microm verfügt über Lizenzen von Film-Produzenten, ihre Werke im Internet öffentlichen wiedergeben zu dürfen, und hat sich vertraglich dazu

verpflichtet, Verstöße gegen das Urheberrecht im eigenen Namen zu verfolgen. In der in Antwerpen anhängigen Klage beantragt Microm, Telenet aufzugeben, Daten von Internetanschlussinhabern offenzulegen, über deren IP-Adressen Urheberrechtsverletzungen begangen wurden. Damit sollen die Anschlussinhaber identifiziert und anschließend Schadensersatzansprüche geltend gemacht werden zu können. Über die fraglichen IP-Adressen sollen geschützte Werke aus dem Angebot von Microm in Peer-to-Peer-Netzwerken mittels des BitTorrent-Protokolls in Filesharing-Diensten geteilt worden sein. Peer-to-Peer-Netzwerke basieren darauf, dass Dateien nicht nur von einem Server heruntergeladen, sondern gleichzeitig zwischen den Nutzer „geteilt" werden, indem einzelne Bestandteile der Dateien im Netzwerk wieder hochgeladen werden. Ermittelt hat Microm die IP-Adressen vor dem gerichtlichen Verfahren mit Hilfe eines deutschen IT-Unternehmens, das eine spezielle Software dafür einsetzte.

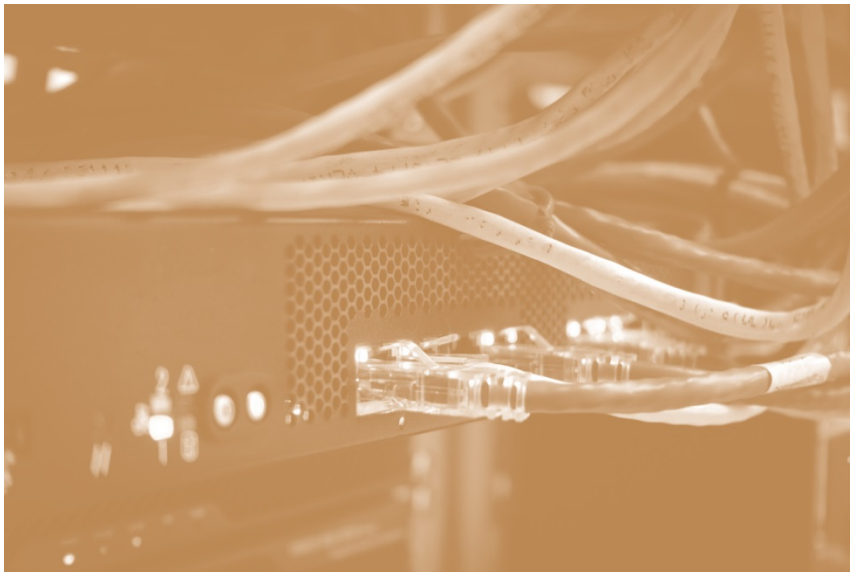
In diesem Zusammenhang stellt sich das vorlegende Gericht unter anderem die Frage, ob das Erheben sowie das Weiterverarbeiten der IP-Adressen der Internetnutzer nach Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt ist, um die Rechtsverletzungen zu verfolgen. Ein berechtigtes Interesse an der Erhebung und Speicherung der IP-Adressen liegt nach Ansicht des Generalstaatsanwaltes nur vor, wenn die Verfolgung der Rechtsverletzungen mit den rechtlichen Vorgaben übereinstimmt und nicht rechtsmissbräuchlich ist. Gerechtfertigt könne die Datenverarbeitung aber nur sein, wenn die ermittelten IP-Adressen auch dazu benutzt werden könnten, die Schuldner der Forderungen zu ermitteln.

Der Generalstaatsanwalt weist klarstellt darauf hin, dass, wenn eine Datenverarbeitung nicht rechtmäßig erfolgen dürfe, dies gleichsam dazu führe, dass die IP-Adressen keine personenbezogenen Daten darstellen. Dies ist folgerichtig, da die Qualifikation der IP-Adresse als personenbezogene Daten letztlich darauf beruht, dass ein rechtmäßiger Anspruch auf Identifizierung des dahinterstehenden Anschlussinhabers unter bestimmten Voraussetzungen bestehen kann.

Der Generalstaatsanwalt stellt zudem klar, dass es für die datenschutzrechtliche Erforderlichkeit auch ausreiche, wenn der Anschlussinhaber nicht derjenige ist, der die Rechtsverletzung begangen habe. Regelmäßig sei der Anschlussinhaber jedenfalls in

der Lage herauszufinden, wer der Verantwortliche ist, oder sei selbst für die Handlung haftbar.

Die Abwägung des berechtigten Interesses mit den Rechten der betroffenen Personen schließlich bleibt Sache des zuständigen Gerichts im Einzelfall.



Umgang mit Datenlecks – Neue EDSA Leitlinien

Datenlecks, ob durch böswillige Hacker-Attacken, unzureichende IT-Sicherheitsstrukturen oder schlicht Fehler von Mitarbeitern, sind ein großes Risiko für Unternehmen und lösen zudem regelmäßig kurzfristige Meldepflichten bei den Unternehmen aus. Ob eine Meldepflicht im konkreten Fall wirklich besteht, ggf. auch Betroffene zu benachrichtigen sind und wann die Fristen beginnen, ist in der Praxis oft schwierig zu beantworten. Der Europäische Datenschutzausschuss (EDSA) hat neue, praxisorientierte Leitlinien veröffentlicht, in denen fallbasiert der Umgang mit und die Vermeidung von Datenpannen dargestellt wird. Wir haben die wesentlichen Erkenntnisse für Sie in unserem Beitrag zusammengefasst.

Nachdem der EDSA bereits 2017 generelle Leitlinien zur Meldung von Verletzungen personenbezogener Daten durch Datenlecks veröffentlicht hat (Leitlinien der Art. 26-Datenschutzgruppe WP 250 in der deutschen Fassung), werden diese nun durch neue praxisorientierte Leitlinien zur Bewältigung von Datenpannen

ergänzt. In diesen Leitlinien 01/2021 (Guidelines 01/2021) stellt der EDSA an Beispielsfällen dar, wie Datenpannen entstehen, ob und inwiefern Pflichten zur Mitteilung an die Aufsichtsbehörden und die Betroffenen bestehen und wie ein konsequentes und sinnvolles Vermeidungsverhalten und die Behebung der Fehlerquellen aussehen könnte. Die neuen Leitlinien sollen damit für Datenverarbeiter eine erste Anlaufstelle bei der Organisation und Bewältigung konkreter Datenpannen sein. Die Orientierung an Beispielsfällen erleichtert dabei die praktische Anwendbarkeit erheblich.

Zu guter Letzt

Aus den vergangenen Wochen ist wieder über einige interessante Bußgeldfälle aus den umliegenden EU-Mitgliedstaaten zu berichten, die alltägliche Situationen betreffen: Gerügt wurden etwa Informationsmängel, Fehler bei der Datenberichtigung und – wie so oft – eine unzureichende Datensicherheit.

- **Spanien: Informationsmängel und unwirksame Einwilligungen kosten 6 Mio. Euro**

Die spanische Datenschutzbehörde verhängte ein Bußgeld in Höhe von insgesamt 6 Millionen Euro gegen die CaixaBank wegen mangelhafter Kundeninformationen und Verarbeitung personenbezogener Daten ohne Erlaubnis. Die Informationen, die die CaixaBank ihren Kunden in Bezug auf den Datenschutz zur

Verfügung stellte, entsprachen nach Ansicht der Behörde nicht den Anforderungen der Art. 13 und 14 DSGVO. Sie seien unpräzise, vage formuliert und inhaltlich unzureichend. Zudem seien sie nicht einheitlich ausgestaltet. Die Informationen seien von Fall zu Fall unterschiedlich umfangreich, nicht immer aktuell und terminologisch unterschiedlich - zum Teil in einer „Rahmenvereinbarung", in anderen Fällen in einer „Zustimmungsvereinbarung" oder in einer „Datenschutzrichtlinie" - eingekleidet worden. 2 Mio. Euro Geldbuße muss die CaixaBank für diese Informationsmängel zahlen. Weitere 4 Mio. Euro kostet das Unternehmen der Verstoß gegen Art. 6 DSGVO. Im vorliegenden Fall fehlte es aus Sicht der Behörde an einer tragfähigen Begründung für eine Datenverarbeitung im berechtigten Interesse. Auch die eingeholten Einwilligungen entsprechen offenbar nicht den gesetzlichen Anforderungen an Freiwilligkeit, Transparenz und Eindeutigkeit.

- **Spanien: Hohes Bußgeld für unterbliebene Aktualisierung der Adressänderung**

Die spanische Datenschutzbehörde verhängte zwei Bußgelder in Höhe von jeweils 50.000 Euro gegen das Stromversorgungsunternehmen Iberdrole. Nachdem ein ehemaliger Kunde dem Unternehmen die Änderung seiner Adresse mitgeteilt und um die Löschung seiner Daten gebeten hatte, wurden weiterhin Briefe an die bisherige Adresse geschickt. Nach Ansicht der Behörde verstieß das Unternehmen, indem es die Aktualisierung der Adressdaten versäumte, gegen Art. 5 Abs. 1 lit. d. DSGVO, der vom Verantwortlichen verlangt, dass personenbezogene Daten sachlich richtig verarbeitet und erforderlichenfalls auf den neusten Stand gebracht werden müssen. Das zweite Bußgeld sprach die Behörde für den Verstoß gegen Art. 17 DSGVO aus, der bei begründetem Verlangen des Betroffenen den Verantwortlichen zur Löschung der Daten verpflichtet.

- **Polen: Rund 46.000 Euro für unzureichende Sicherheitsüberprüfungen**

In Polen verhängte die Datenschutzbehörde ein Bußgeld von rund 460.000 Euro gegen Virgin Mobile Polska wegen des Vorwurfes, keine angemessenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der verarbeiteten Daten implementiert zu haben (Art. 5 Abs. 1 lit. f, Abs. 2; 25 Abs. 1; 32 Abs. 1 lit. b, d, Abs. 2 DSGVO). Anlass der behördlichen

Untersuchungen im Unternehmen war eine Datenpanne, die dazu führte, dass Unbefugte an Kundendaten aus einer Datenbank gelangten. Das Verwaltungsverfahren ergab, dass die Ursache eine Schwachstelle im IT-System war, die unerkannt blieb, da der Mechanismus vor der Implementierung nicht ausreichend auf seine Funktionsfähigkeit und Sicherheit getestet worden war.

Zudem entlarvte das Verfahren generelle Missstände bei den Sicherheitsüberprüfungen im Unternehmen: Um die Sicherheit der verarbeiteten Daten zu gewährleisten, hat der Verantwortliche gem. Art. 32 Abs. 1 lit. d DSGVO „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen“ sicherzustellen. Die etablierten Prozesse bei Virgin Mobile Polska konnten diesen Anforderungen nicht entsprechen. Unregelmäßige und unvollständige Prüfungen, Messungen und Bewertungen bei Verdacht auf Schwachstellen oder im Zusammenhang mit organisatorischen Änderungen seien keine regelmäßige, sondern nur zufällige Prüfung der Wirksamkeit technischer und organisatorischer Maßnahmen.

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. Malte Göbel
+49(0)221 65065-337
malte.goebel@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