LOSCHELDER

Newsletter Datenschutzrecht

Juli 2020

Sehr geehrte Damen und Herren,

kurz vor der Sommerpause droht noch ein massiver Einschlag in der Datenschutz-Szene: Für morgen (16. Juli) wird das Urteil des EuGH zum umstrittenen EU-US Privacy Shield erwartet. Kippt der EuGH das Abkommen, führt das (erneut nach „Safe Harbour“) zu ganz erheblichen Fragezeichen für den transatlantischen Datenverkehr. Alle Unternehmen mit geschäftlichen oder technischen Beziehungen in die USA wären davon betroffen und müssten sich – vorbehaltlich etwaiger Übergangszeiträume – schnell auf die neue Situation einstellen.

Und auch im Übrigen dürfen wir Ihnen von einigen bemerkenswerten Entwicklungen und Fällen berichten: Der LfDI BW verhängte gegen die ortsansässige AOK ein Bußgeld von 1,24 Mio. Euro für den unrechtmäßigen Versand von 500 Werbemails. In die Höhe getrieben wurde das Bußgeld allerdings wohl aufgrund unzureichender Datensicherheitsmaßnahmen, ein bei den meisten höheren Bußgeldern in Deutschland zentrales Thema. Der BGH hat in Sachen Facebook entschieden und der BfDI hat Ende Juni sein Ergebnispapier zur Anonymisierung veröffentlicht. Und auch andere Aufsichtsbehörden haben sich zu den in der Praxis wichtigen Themen des Einsatzes von Google Analytics und Videokonferenzsystemen geäußert. Über all dies lesen Sie in unserem Juli-Newsletter.

Zudem noch ein Hinweis in eigener Sache: Am 12. August 2020 findet unser Lunch@Loschelder Webinar zum Thema „**Nach dem Cookie-Urteil des BGH: Datenschutzkonforme Websitegestaltung**“ von 12 Uhr bis 12.30 Uhr statt. Weitere Informationen finden Sie hier. Über Ihre Anmeldung unter webinare@loschelder.de würden wir uns sehr freuen.

Selbstverständlich ist bei alledem: Sie können der **Verwendung Ihrer Daten für diesen Newsletter-Versand jederzeit widersprechen,** indem Sie den Newsletter abbestellen. Bitte scrollen Sie dazu ans Ende dieser E-Mail.

Inhalt

1,24 Mio. Euro für 500 Werbemails ohne Einwilligung?

Für Aufsehen sorgte Ende Juni ein hohes Bußgeld aus Baden-Württemberg: 1,24 Mio. Euro verhängte der LfDI dort gegen die ortsansässige AOK. Dem Vernehmen nach ist das Bußgeld rechtskräftig. Der Anlass: 500 Werbemails waren ohne die benötigte Einwilligung verschickt worden.

Der eigentliche Grund für das Bußgeld in dieser Höhe aber lag in den unzureichenden Prozessen, die einen solchen Fehlversand überhaupt erst ermöglichten. Die AOK hatte im Rahmen von Gewinnspielen Daten erhoben und wollte an die Teilnehmer dann auch Werbemails verschicken, wenn diese hierzu gesondert eingewilligt hatten. In der Pressemitteilung des LfDI heißt es dazu weiter: „Mithilfe technischer und organisatorischer Maßnahmen … wollte die AOK hierbei sicherstellen, dass nur Daten solcher Gewinnspielteilnehmer zu Werbezwecken verwendet werden, die zuvor wirksam hierin eingewilligt hatten. Die von der AOK festgelegten Maßnahmen genügten jedoch nicht den gesetzlichen Anforderungen." Die unzureichenden Maßnahmen waren letztlich Grund dafür, dass es zu dem Fehlversand kommen konnte. Der eigentliche Verstoß lag denn auch in einer unzureichend sicheren Datenverarbeitung nach Art. 32 DSGVO. Kooperation und nachhaltige Verbesserungen des Datenschutzmanagements führten letztlich dazu, dass das Bußgeld nicht noch höher ausfiel. Das und die Höhe des Bußgeldes sind allerdings durchaus bemerkenswert, weil eine strenge Berechnung nach dem (umstrittenen) Bußgeldkonzept der deutschen Datenschutzbehörden bei der AOK Baden- Württemberg sicherlich zu einem Tagessatz in Millionenhöhe geführt hätte. Insoweit ist die Behörde weit „unter ihren [selbst gesetzten] Möglichkeiten" geblieben. Absolut betrachtet erschreckt die Höhe gleichwohl.

Einmal mehr verdeutlicht dieser Fall, wie wichtig datenschutzkonforme Prozesse und damit ein effektives Datenschutzmanagement sind. Hätte ein solches bestanden, wäre das Bußgeld deutlich geringer ausgefallen, so denn das Verfahren überhaupt zu einem Bußgeld geführt hätte.

Der BGH rügt Facebook: Einwilligungen ungenügend

Im vom Bundeskartellamt gegen Facebook geführten Verfahren hat nunmehr der BGH entschieden. Dieser bestätigte – anders, als noch das OLG Düsseldorf – das Bundeskartellamt in wesentlichen Punkten. Und er äußerte sich auch zur datenschutzkonformen Einwilligung.

Mit seinem Beschluss vom 23.06.2020 bestätigte der BGH im einstweiligen Verfahren – und daher vorläufig – den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook (Az.: KVR 69/19).

Ungeachtet der kartellrechtlich hoch interessanten Fragen, die diese Entscheidung mit sich bringt – und über die intensiv diskutiert wird –, ist der BGH-Beschluss auch datenschutzrechtlich interessant: Das Bundeskartellamt hatte einen Missbrauch durch Facebook ursprünglich u.a. damit begründet, dass die Plattform gegen die DSGVO verstoße. Konkret würden unwirksame Einwilligungen in die Zusammenführung von, auf verschiedenen Plattformen generierten, personenbezogenen Daten eingeholt, da den Nutzern keine Wahlmöglichkeit bliebe: Nutzen sie Facebook, ist die Einwilligung in die Zusammenführung der Daten damit zwingend verknüpft. Interessant ist aus datenschutzrechtlicher Perspektive insbesondere zweierlei: Zum einen kann danach ein DSGVO-Verstoß den Missbrauch einer marktbeherrschenden Stellung

begründen. Das eröffnet einen ganz neuen Risikoaspekt, den Datenschutzverstöße mit sich bringen. Zum anderen ist danach die Einwilligungspraxis von Facebook unzulässig, dies hilft bei der rechtssicheren Anwendung von Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 7 DSGVO.

Laut Bundesgerichtshof bestehen so auch keine ernsthaften Zweifel daran, dass Facebook als marktbeherrschendes Unternehmen seine Stellung mit den untersagten Nutzungsbedingungen ausnutzt. Entscheidend sei dafür allerdings nicht ein Verstoß gegen die DSGVO, sondern dass die Nutzungsbedingungen den Nutzern keine Wahlmöglichkeit beließen. Damit stellt der BGH – soweit sich dies der Pressemitteilung entnehmen lässt – nicht auf den formalen DSGVO-Verstoß, sondern einen wesentlichen materiellen Aspekt ab, nach dem eine Einwilligung eben nur dann wirksam sein kann, wenn sie mit Handlungsspielraum und damit „echt freiwillig" abgegeben wurde. Die fehlende Wahlmöglichkeit der Facebook-Nutzer beeinträchtigt ausweislich der Pressemitteilung des BGH „nicht nur ihre persönliche Autonomie und die Wahrung ihres – auch durch die DSGVO geschützten – Rechts auf informationelle Selbstbestimmung", sondern stärke auch den wettbewerblich bedenklichen Lock-in-Effekt. Bei funktionierendem Wettbewerb wäre der Umfang der Datenpreisgabe ein wesentliches Entscheidungskriterium, welchem sozialen Netzwerk ein Nutzer sich anschlösse.

Zum Hintergrund: Das Bundeskartellamt hatte Facebook die Zusammenführung von Nutzerdaten untersagt und die entsprechenden Einwilligungen als unwirksam eingeordnet (dazu unser Newsletter 02/2019). Das OLG Düsseldorf hatte diese Entscheidung zunächst – vorläufig – gekippt (dazu unser Newsletter 09/2019), der BGH bestätigte sie nun im einstweiligen Rechtsschutzverfahren. Die Entscheidungsgründe des BGH-Urteils liegen noch nicht vor – womöglich ergeben sich daraus noch weitere spannende Einsichten, insbesondere, inwieweit sich der BGH nun zur DSGVO äußert oder eben auch nicht.

Anonymisierung als erlaubnispflichtige Datenverarbeitung?

Nach einer umfassenden Konsultation hat der BfDI Ende Juni sein Positionspapier zur Anonymisierung veröffentlicht. Danach ist – wie auch bisher nach überwiegender Meinung – auch für die Anonymisierung eine Erlaubnisgrundlage erforderlich. In anderen Details ist das Papier hingegen durchaus bemerkenswert.

In der Praxis spielt die Anonymisierung personenbezogener Daten eine erhebliche Rolle. Zum einen lassen sich viele Geschäftsmodelle, gerade im Bereich Analyse und Big Data, erfolgreich mit anonymisierten Daten betreiben, da eine Individualisierung einzelner Person schlicht nicht notwendig ist. Ferner stellt sich für viele Unternehmen die Frage, ob eine dauerhafte Anonymisierung auch die Löschverpflichtungen aus der DSGVO erfüllen kann, beispielsweise bei der Löschung einzelner Angaben aus einem Gesamtkontext.

Neuen Wind in die Diskussion bringt der BfDI mit einem aktuellen Positionspapier zu diesem Thema. Als Anlass dafür verweist er darauf, dass die Nutzung anonymisierter Daten für zahlreiche Forschungsprojekte und Geschäftsmodelle bevorzugt wird (und für deren Erfolg ausreichend ist), in der DSGVO allerdings nur „rudimentär geregelt“ ist.

Der BfDI hält zunächst an der überwiegend vertretenen Position fest, dass die Anonymisierung eine Verarbeitung personenbezogener Daten darstellt und damit einer Erlaubnisgrundlage bedarf. Hier hätte eine differenziertere Betrachtung durchaus neue Spielräume eröffnet, überraschend ist dieses Ergebnis aber letztlich nicht. Für die Praxis ist also von entscheidend, dass eine Anonymisierung erlaubt werden muss und nicht etwa deswegen durchgeführt werden darf, weil sie ohnehin im potentiellen Interesse des Betroffenen an einem Höchstmaß an Datenschutz und -sicherheit liegt. Und auch alle sonstigen DSGVO-Anforderungen sind einzuhalten, insbesondere müssen Unternehmen die Betroffenen gemäß Art. 13, 14 DSGVO über eine geplante Anonymisierung informieren und den entsprechenden Prozess in das Verarbeitungsverzeichnis aufnehmen.

Die Weiterverarbeitung anonymisierter Daten, insbesondere die Übermittlung an Dritte, unterliegt, anders als der Prozess der Anonymisierung, allerdings nicht mehr dem Anwendungsbereich der DSGVO und muss daher auch nicht mehr gesondert erlaubt werden. Sie determiniert aber regelmäßig den Zweck der Anonymisierung selbst.

In praktischer Hinsicht sind folgende Äußerungen des BfDI von Interesse: Von einer Anonymisierung ist – laut des Positionspapiers – dann auszugehen, wenn personenbezogene Daten derart verändert werden, dass die persönlichen oder sachlichen Verhältnisse, die sich ursprünglich aus den Daten ergaben, nicht mehr oder nicht mit einem unverhältnismäßigen Aufwand einer Person zugeordnet werden können. Für die Bestimmung des unverhältnismäßigen Aufwandes kommt es auf den Aufwand an Zeit, Kosten oder Arbeitskraft an. Aus der Modalität des unverhältnismäßigen Aufwands ergibt sich, dass es für die Anonymisierung nicht zwingend darauf ankommt, dass die Wiederherstellung des ursprünglichen Personenbezugs für *niemanden* mehr möglich ist. Die Anonymisierung liegt also immer dann vor, wenn eine Re-Identifizierung wegen des zu hohen Aufwands praktisch nicht durchführbar ist. Ob auch der BfDI dies so sieht, ist zweifelhaft, da er an einer anderen Stelle seines Papiers als Anonymisierung nur eine solche Veränderung beschreibt, nach der die Wiederherstellung eines Personenbezugs „für jedermann zumindest praktisch unmöglich ist“ (S. 4). Dies erscheint sehr weit und mit den Erwägungsgründen der DSGVO nur schwerlich

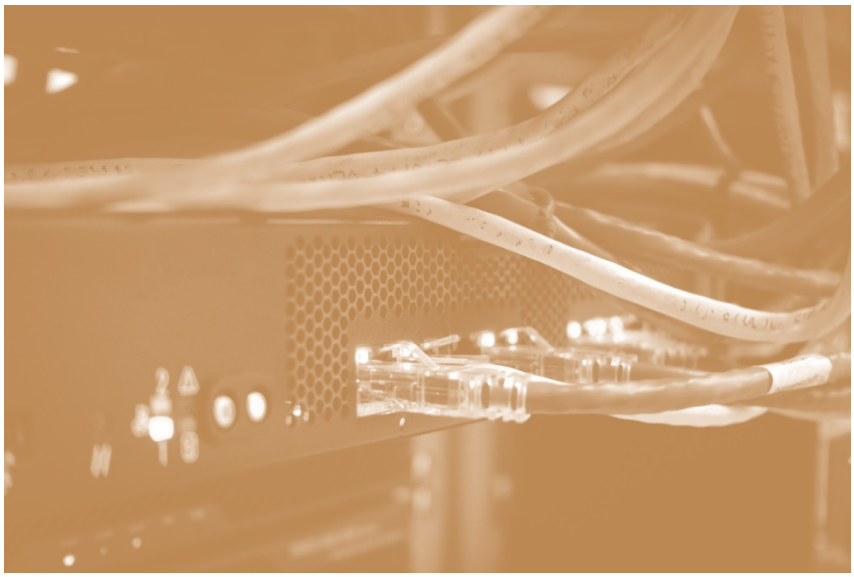
vereinbar. In jedem Fall aber ist stets sorgfältig zu prüfen, ob Daten wirklich anonymisiert werden.

Für die Praxis beachtlich sind denn insbesondere folgende Erwägungen des BfDI:

- Da es sich bei der Anonymisierung personenbezogener Daten um eine besonders komplexe und somit fehleranfällige Aufgabe handelt, sei regelmäßig eine Datenschutzfolgenabschätzung durchzuführen (Art. 35 Abs. 1 DSGVO).

- Die für die Anonymisierung benötigte Rechtsgrundlage könnte sich grundsätzlich aus allen Erlaubnistatbeständen der DSGVO ergeben. Wichtig: Sie sei ausnahmsweise verzichtbar, wenn der Zweck der Anonymisierung mit dem Zweck vereinbar ist, zu dem die personenbezogenen Daten ursprünglich erhoben wurden (Art. 6 Abs. 4 DSGVO), oder dies der Datenlöschung i.S.d. Art. 17 DSGVO diene, die dann Pflicht i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO sei. Laut BfDI kann ein Löschverlangen damit auch durch Anonymisierung erfüllt werden.

- Betroffene müssen informiert werden; Art. 13, 14 DSGVO greifen auch für die Anonymisierung.



Neues von den Aufsichtsbehörden zu Google Analytics und Videokonferenzdiensten

Die Datenschutzaufsichtsbehörden haben in den vergangenen Wochen insbesondere zwei für die Praxis wichtige Tools (erneut) bewertet: Den Einsatz von Google Analytics und von den aktuell so wichtigen Videokonferenzsystemen. Einheitlich fallen die Bewertungen dabei allerdings nicht aus.

So hilfreich die Hinweise der Datenschutzbehörden für die Praxis regelmäßig auch sein mögen, gilt dies nicht uneingeschränkt. Das ergibt sich bereits daraus, dass bloße Hinweise nicht gerichtlich überprüfbar sind und sich die Behörden zum Teil auch widersprüchlich positionieren.

Google Analytics

Diese Vorrede ist für den nachfolgenden Beitrag von enormer Bedeutung, um das unternehmerische Handeln vor dem Hintergrund der nachfolgenden Informationen auszurichten. Betroffen ist davon zunächst Google Analytics. Das Tool für statistische Auswertungen der Websitenutzung und – je nach Konfiguration – etwa auch dem Werbetracking steht seit Monaten in der datenschutzrechtlichen Kritik. Diese legte bislang den Fokus darauf, ob dieses Tool auch ohne aktive Einwilligung einsetzbar ist (nach Aufsichtsbehörden-Ansicht nicht, wir berichteten etwa im November 2019 dazu).

Nunmehr haben sich die Aufsichtsbehörden erneut positioniert und den datenschutzrechtskonformen Einsatz selbst mit Einwilligung in Frage gestellt: Ihrer Ansicht nach sind der Websitebetreiber und Google Analytics gemeinsam für die Verarbeitung personenbezogener Daten der Websitebesucher verantwortlich. Eine datenschutzkonforme Verarbeitung ist dann nur nach Abschluss eines entsprechenden „Joint Control-Vertrages“ nach Art. 26 DSGVO denkbar. Google stellt einen solchen (noch) nicht zur Verfügung, für kleinere Nutzer des Tools ist dieser in der Praxis aktuell auch kaum verhandelbar. Der Einsatz von Google Analytics ist angesichts dessen unter Risikogesichtspunkten selbst dann neu zu bewerten, wenn er mit Einwilligung der Nutzer erfolgt. In jedem Fall sollten die weiteren Entwicklungen eng begleitet werden.

Zoom, GoToMeeting, Teams & Co.

Unsicherheiten in der datenschutzrechtlichen Bewertung von Videokonferenzsystemen begleiten uns insbesondere seit dem schlagartigen Umzug ins Home-Office Mitte März diesen Jahres. Auch die Datenschutzaufsichtsbehörden begutachten die verschiedenen Anbieter seither intensiv. Nach einigen kurzgefassten Leitfäden und Übersichten zur Auswahl von und Umgang mit Videokonferenzdiensten zum Anfang der Corona-Krise, haben sich mehrere Datenschutzbehörden in den letzten Monaten umfassend mit diversen Anbietern, ihren Vor- und Nachteilen und dem möglichst datenschutzkonformen Einsatz ihrer Dienste auseinandergesetzt.

Gleich vorweg: Eindeutig sind die Aussagen nicht. So wird etwa Zoom auch in einer jüngsten Stellungnahme von der Berliner Behörde noch scharf kritisiert, während der LfDI BW explizit seine Bedenken aufgibt und unter dem 24.06.2020 titelt „Warnung des LfDI wurde gehört – Zoom bessert nach". Dies verdeutlicht, dass die Positionen der Aufsichtsbehörde nicht ungefiltert übernommen werden sollten. Gleichwohl sind ihre Einschätzungen sorgfältig einzubeziehen in die unternehmensinterne Prüfung, welche Tools mit welcher Konfiguration eingesetzt werden. Ihren Zugang möge die nachfolgende Übersicht erleichtern:

- **Berliner Beauftragte für Datenschutz und Informationsfreiheit:**

  Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, 03.07.2020

  Trotz des anders anmutenden Titels bietet der Leitfaden auch Informationen für Verantwortliche aus anderen Bundesländern, zumal er sich erstaunlich detailliert mit einer Vielzahl von Diensten auseinandersetzt, darunter Cisco WebEx, Skype, Microsoft Teams und Zoom. Den Schwerpunkt legte die Behörde dabei auf eine Beurteilung der Rechtskonformität der angebotenen Auftragsverarbeitungsverträge.

  Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg: Zoom bessert nach, 24.06.2020

Nachdem die Behörde noch Anfang April von der Nutzung des Dienstes Zoom abriet, zeigte sie sich nun mit den vorgenommenen Änderungen zufrieden und zog die gegenüber Schulen ausgesprochene Nutzungswarnung zurück. Damit hat Zoom jedenfalls in der Version 5.0. eine positive datenschutzrechtliche Bewertung erhalten. Einen weitergehenden Leitfaden zur Beurteilung von Videokonferenzdiensten unter Nennung einiger Beispiele veröffentliche der LfDI BW schon Anfang April.

- **Bundesamt für Sicherheit und Techni**k:

  Kompendium Videokonferenzdienste (KoViKO), April 2020

  Eine technische, umfassende Darstellung zum Umgang mit Videokonferenzdiensten bietet das KoViKo des BSI. Dabei wird einerseits dargestellt, wie Videokonferenzdienste mit einem, dem Unternehmen entsprechenden, Sicherheitsstandart in die interne IT eingebunden werden können, andererseits auch operative und funktionale Aspekte dargestellt. Gerade wer überlegt, auch langfristig Videokonferenzdienste im Betrieb einzusetzen, kann von den Darstellungen profitieren.

- **Bundesbeauftragter für Datenschutz und Informationsfreiheit**:

  In seinen Leitfragen zur Beurteilung von Angeboten stellt der BfDI in Form eines FAQ die wichtigsten Fragen und Antworten zur Auswahl eines „guten" Videokonferenzdienstes vor. Zudem veröffentlichte der BfDI eine Übersicht zu einer Auswahl von Messenger-Systemen mit Audio-/ Videounterstützung, die insbesondere auch den Datenstrom darstellt.

- **Bayerisches Landesamt für Datenschutzaufsicht**:

  Best-Practice Datenschutzrecht im Home-Office, 18.05.2020

  Eine eher allgemeine Übersicht zum datenschutzkonformen Umgang mit Videokonferenzdiensten bei der Nutzung im Home-Office bietet der Best-Practice Bogen des BayLDA.

- **Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen**:

  Leitplanken für die Auswahl von Videokonferenzsystemen während der Kontaktbeschränkungen aufgrund der Corona-Pandemie, 30.06.2020

  Die LDI NRW veröffentliche mit ihren Leitplanken einen umfassenden Leitfaden zu Videokonferenzdiensten. Neben einer Anleitung zum Vorgehen bei der Auswahl und der Anwendung als organisierende und als teilnehmende Person werden die wesentlichen Attribute der beliebtesten Dienste (Skype, Zoom, Cisco WebEx, Microsoft Teams) dargestellt.

- **Hamburgischer Beauftragter für Datenschutz und Informationssicherheit**:

  Auch der HambBfDI stellt in dem regelmäßig überarbeiteten FAQ „Datenschutz in Zeiten von Covid-19“ eine (nicht abschließende) Liste mit den wesentlichen Fragen, die bei Auswahl und Nutzung eines Videokonferenzdienstes entstehen, zur Verfügung.

- **Datenschutzbeauftragter des Kanton Zürich**:

  Datenschutz auch im Homeoffice und in der Schule zuhause

  Eine Kurzübersicht und Bewertung zum Einsatz in der Corona-Krise vieler gängiger Videokonferenz- und Kommunikationsdienste bietet der Datenschutzbeauftragte des Kanton Zürich. Jedenfalls um sich einen ersten Überblick über die Angebotsvielfalt zu machen, kann sich der Blick in das Nachbarland lohnen.

Erwähnenswert ist, dass nach der Einschätzung vieler Aufsichtsbehörden viele der beliebten Videokonferenzdienste erhebliche datenschutzrechtliche Mängel aufweisen. Teilweise lassen sich solche durch eine entsprechende Ausgestaltung der Auftragsverarbeitungsverträge beheben, teilweise ist von der Nutzung bestimmter Dienste ganz abzuraten. Insgesamt sollte, vor allem, wenn Videokonferenzen auch nach der Corona-Krise weiter Teil des Berufsalltags sein sollen, mit Vorsicht und Detailgenauigkeit vorgegangen werden. Die dargestellten Leitfäden

bieten hierfür einen guten Ansatzpunkt, um den Dschungel an Anbietern und Diensten etwas zu lichten.

Zu guter Letzt

Auch in diesem Monat gibt es – neben dem eingangs schon erwähnten Bußgeld gegen die AOK BW – auch einige interessante Entscheidungen ausländischer Datenschutzbehörden, die teils zu hohen Bußgeldern für die Verantwortlichen führten, in einem Fall wegen der Cookie-Nutzung bei Twitter. Zudem bestätigte ein französisches Gericht das Bußgeld der CNIL gegen Google in schwindelerregender Höhe.

- **Spanien**

Die spanische Datenschutzbehörde verhängte gegen das Telekommun Die spanische Datenschutzbehörde verhängte gegen das Telekommunikationsunternehmen Telefonica ein Bußgeld in Höhe von 40.000 Euro. Aufgrund des Versäumnisses eines Vertriebsmitarbeiters, die Identität eines vermeintlichen Kunden zu prüfen, wurde ermöglicht, dass dieser unter falscher Identität die Freischaltung von vier Anschlüssen bewirken konnte. Eine unzureichende Identifizierung hatte in Deutschland Ende letzten Jahres zu einem Bußgeld von fast 10 Mio. Euro gegen 1&1 geführt.

Zudem wurde gegen ein spanisches Kreditinstitut ein Bußgeld in Höhe von 75.000 Euro verhängt. Grund dafür war die Weigerung

seitens des Verantwortlichen, die Daten eines ehemaligen Kunden trotz dessen ausdrücklichen Wunsches zu löschen.

Zuletzt wurde in Spanien ein Verstoß bei der Nutzung von Cookies bei Twitter geahndet. Dort wurde zwar in einem Cookie-Banner über die Verwendung von Cookies informiert, allerdings gab es keine Möglichkeit, unerwünschte Cookies „abzuwählen“. Dies führte letztlich dazu, dass für die Benutzung von Twitter zwangsläufig alle Cookies akzeptiert werden mussten. Die Zusammenschau diverser Kriterien bewegte die Behörde zur Verhängung eines Bußgeldes in Höhe von 30.000 Euro.

- **Norwegen**

In Norwegen fragte ein Unternehmer aus Neugier die Bonitätsdaten eines Mitbewerbers ab. Durch eine Prüfung der Datenschutzbehörde stellte diese fest, dass für die Abfrage weder ein objektives Bedürfnis noch ein berechtigtes Interesse bestand, und belegte den Unternehmer mit einem Bußgeld von umgerechnet 28.000 Euro.

- **Finnland**

Die finnische Datenschutzbehörde verhängte gegen die nationale Postgesellschaft ein Bußgeld in Höhe von 100.000 Euro. Die Postgesellschaft hatte Kunden, die m Die finnische Datenschutzbehörde verhängte gegen die nationale Postgesellschaft ein Bußgeld in Höhe von 100.000 Euro. Die Postgesellschaft hatte Kunden, die mithilfe eines Online-Formulars die Postgesellschaft über Adressänderungen informieren konnten, nicht darüber aufgeklärt, an wen diese Daten weitergegeben wurden und dass ihnen ein Widerspruchsrecht gegen die Verarbeitung zusteht. Teilweise wurden die personenbezogenen Daten gar zu Marketingzwecken verwendet.

Daneben verhängte die finnische Datenschutzbehörde gegen ein Taxiunternehmen aus Helsinki ein Bußgeld in Höhe von 72.000 Euro. Dieses hatte in seinen Taxis Kameraüberwachungssysteme installiert, ohne vorher die Risiken und Auswirkungen der Verarbeitung personenbezogener Daten zu bewerten.

- **Frankreich**

In Frankreich der Conseil d'État das Bußgeld der CNIL gegen Google in Höhe von 50 Mio. Euro bestätigt. Die CNIL, die französische Datenschutzaufsichtsbehörde, hatte dieses im vergangenen Jahr gegen Google verhängt. Gründe dafür waren insbesondere eine unzureichende Transparenz, Google habe nicht ausreichend die wesentlichen Informationen über Verarbeitungszweck und Speicherdauer mitgeteilt. Häufig seien die Informationen über mehrere Seiten verteilt, die nur über verschiedene Links zu erreichen waren. Zudem seien die Informationen auch nicht immer so verständlich, dass sie den Betroffenen in ausreichendem Umfang über die Datenverarbeitung hätten informieren können.

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

Claudia Willmer
+49(0)221 65065-337
claudia.willmer@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