LOSCHELDER

Newsletter Datenschutzrecht

April 2021

Sehr geehrte Damen und Herren,

Sie haben es sicherlich vernommen – im Zweifel aus unserem Ende März versandten Sondernewsletter: Das Bayrische Landesamt für Datenschutzaufsicht hat den Einsatz des US-Tools „Mailchimp“ in einem konkreten Fall für unzulässig erklärt, da ein angemessenes Datenschutzniveau in diesem Fall nicht abgesichert worden war. Dafür genügte es dem BayLDA, dass das betroffene Unternehmen die hinreichende Absicherung der personenbezogenen Daten beim US-Transfer nicht überprüft hatte. Zwar ist damit noch nicht gesagt, dass der Einsatz von Transfersystemen wie „Mailchimp“ generell unzulässig ist. Jedenfalls aber muss die Absicherung des Datenschutzniveaus gesondert geprüft werden, u.a. dahingehend, ob die Ergreifung zusätzlicher Maßnahmen im Sinne der EuGH-Entscheidung „Schrems II“ notwendig ist oder womöglich eine Einwilligung in den US-Transfer eine Lösung darstellen könnte. Von einer Bußgeldverhängung im konkreten Fall wurde abgesehen, weil nur in wenigen Fällen Daten unzulässig übermittelt wurden und E-Mail-Adressen allein nicht sonderlich sensible Daten sind.

Auch im Übrigen haben wir interessante Themen für Sie gesammelt. In unserem ersten Beitrag geht es um die prozessuale Frage der Beweislastumkehr bei Schadensersatzansprüchen. Sodann beschäftigen wir uns mit den technischen Anforderungen an eine E-Mail Verschlüsselung. Im Beitrag 3 befassen wir uns mit dem vielbeachteten Facebook Verfahren des Bundeskartellamts, das in die nächste prozessuale Eskalationsstufe geht. Und zu guter Letzt stellen wir Ihnen interessanten Bußgeldfälle und bemerkenswerte Randnotizen vor.

Inhalt

Keine Beweislastumkehr bei DSGVO-Schadensersatz

Es bleibt spannend in Sachen Schadensersatz bei DSGVO-Verstößen. In unserem März-Newsletter letzten Monat berichteten wir über eine Entscheidung des Bundesverfassungsgerichts zur Bagatellgrenze für Schadensersatzansprüche wegen eines DSGVO-Verstoßes nach Art. 82 Abs. 1 DSGVO. Wenig später sorgte das OLG Stuttgart mit einem Urteil vom 31. März 2021 zur Beweislast bei solchen Schadensersatzansprüchen für Aufsehen. Welche Aussagen das Gericht konkret zur Beweislast getroffen hat – und welche Konsequenzen die Beurteilung dieser eher rechtstechnisch anmutenden Frage für die Praxis hat – stellen wir Ihnen in diesem Beitrag vor.

In dem Berufungsverfahren vor dem OLG Stuttgart (OLG Stuttgart, Urteil vom 31.03.2021 – Aktenzeichen 9 U 34/21 – hier abrufbar) ging es um die Frage, ob und inwieweit der Anspruchsteller beweisen muss, ob die tatsächlichen Voraussetzungen des Schadensersatzanspruches nach Art. 82 Abs. 1 DSGVO gegeben sind. Im konkreten Fall war es zu einem Datendiebstahl bei einem Unternehmen gekommen, das Bonus- und Punkteprogramme für Kreditkarten anbietet. Der Kläger, dessen personenbezogene Daten von dem Datendiebstahl betroffenen waren, verlangte u.a. mindestens 4.000 Euro Schadensersatz nach Art. 82 Abs. 1 DSGVO vom Unternehmen, weil – so seine Vorwürfe – dieses seinen Datensicherungspflichten nach Art. 32 DSGVO nicht ausreichend nachgekommen und deshalb der Datendiebstahl überhaupt möglich gewesen sei. Beweise für einen konkreten Verstoß gegen die Datensicherungspflichten der DSGVO bot der Kläger nicht an – nach seiner Auffassung trägt der Datenverarbeiter als Anspruchsgegner die Pflicht zu beweisen, dass kein Verstoß gegen die DSGVO vorliegt und die Voraussetzungen des Art. 82 Abs. 1 DSGVO nicht gegeben sind.

Beweiserleichterung bei Ansprüchen aus Art. 82 Abs. 1 DSGVO?

Mit dieser Auffassung ist der Kläger nicht gänzlich allein: Einige Datenschützer leiten aus den Dokumentations- und Rechenschaftspflichten des Verantwortlichen nach Art. 5 Abs. 2 DSGVO her, dass Anspruchstellern eine Beweiserleichterung im Rahmen des Schadensersatzanspruchs nach Art. 82 Abs. 1 DSGVO zugute kommt. Anstatt den Vollbeweis zu erbringen, dass die Voraussetzungen des Art. 82 Abs. 1 DSGVO erfüllt sind, reiche im

Prozess der Vortrag, dass seine personenbezogenen Daten möglicherweise rechtswidrig unter Verstoß gegen die DSGVO verarbeitet worden wären und deshalb eine Verletzung des allgemeinen Persönlichkeitsrechts vorliege und ein ersatzfähiger Schaden entstanden sei. Es läge dann bei dem in Anspruch genommenen Datenverarbeiter (Verantwortlichen oder Auftragsverarbeiter), nachzuweisen, dass personenbezogene Daten DSGVO-konform verarbeitet wurden und die Voraussetzungen des Art. 82 Abs. 1 DSGVO nicht vorliegen.

OLG Stuttgart - Nationale Beweislastregeln reichen aus

Das OLG Stuttgart ist anderer Auffassung: Die Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO könne nicht als Beweiserleichterung für Schadensersatzansprüche aus Art. 82 Abs. 1 DSGVO herangezogen werden. Die Rechenschaftspflicht mache nur Vorgaben zum Nachweis gegenüber den Aufsichtsbehörden. Da die DSGVO keine eigenen Beweislastregeln vermittle, seien die nationalen Grundsätze, also die allgemeinen Beweisregeln der ZPO, anzuwenden. Grundsätzlich hat danach jeder das darzulegen und im Zweifel zu beweisen, was für ihn vorteilhaft ist – entsprechend hat der Anspruchssteller das Vorliegen der Voraussetzungen des Schadensersatzanspruchs inklusive des Verstoßes gegen DSGVO-Vorschriften darzulegen und im Zweifel zu beweisen.

Etwas Anderes ergebe sich auch nicht aus dem unionsrechtlichen Effektivitätsgrundsatz: Danach darf die Anwendung nationaler Beweislastregeln auf europäische Rechtssätze wie die DSGVO nicht dafür sorgen, dass die Anwendung des Unionsrechts wesentlich erschwert oder unmöglich gemacht wird. Diese Gefahr sieht das OLG Stuttgart hier nicht, zumal bei Beweisschwierigkeiten des Anspruchsstellers auf die Grundsätze der sogenannten sekundären Darlegungslast zurückgegriffen werden kann. Diese obliegt dem nicht primär darlegungs- und beweispflichtigen Anspruchsgegner, wenn es dem Anspruchssteller tatsächlich nicht möglich ist, den Sachverhalt weiter aufzuklären, der Anspruchsgegner dies aber ohne größere Schwierigkeiten kann (Sphärengedanke). Kann der Anspruchsgegner seine sekundäre Darlegungslast nicht erfüllen, gilt die nicht bewiesene Behauptung des Anspruchstellers dann als zugestanden – und damit im Rahmen des Zivilprozesses als gegeben.

Insofern reichten, so das OLG Stuttgart, die allgemeinen nationalen Regeln zur Beweislastverteilung aus, um die Interessen potentiell Verletzter ausreichend zu berücksichtigen und eine Beweislastumkehr oder -erleichterung für die Voraussetzungen des Art. 82 Abs. 1 DSGVO sei auch aus unionsrechtlichen Gründen nicht erforderlich.

Kausalität als beweispflichtige Voraussetzung

Zudem legte das Gericht dar, dass auch der kausale Zusammenhang zwischen dem DSGVO-Verstoß und dem Schaden, den die Person erlitten hat, eine Voraussetzung des Schadensersatzanspruchs aus Art. 82 Abs. 1 DSGVO sei und diese Kausalität ebenfalls vom Anspruchssteller zu beweisen sei. Der abweichenden Auffassung einiger Datenschützer, die für den Verzicht auf das Kausalitätserfordernis bzw. des Beweises der Kausalität durch den Anspruchsteller plädieren, folgte das OLG Stuttgart nicht.

Der BGH wird weiter entscheiden

Mit seiner Entscheidung bestätigte das OLG damit die erstinstanzliche Entscheidung, wonach die Voraussetzungen des Schadensersatzanspruches nicht gegeben bzw. nicht bewiesen wurden und lehnte die Berufung ab. Gleichzeitig ließ das OLG Stuttgart aber die Revision gegen das Urteil zu – weil die Fragen zur Beweisverteilung bei Art. 82 Abs. 1 DSGVO von grundsätzlicher Bedeutung seien, soll nun der Bundesgerichtshof (BGH) darüber entscheiden – die Klägerin hat dem Vernehmen nach bereits am 07.04.2021 Revision eingelegt.

Für die Praxis heißt diese Entscheidung vorläufig zweierlei: Übernehmen andere Gerichte bei der Beurteilung von Schadensersatzansprüchen nach Art. 82 Abs. 1 DSGVO die Rechtsauffassung des OLG Stuttgart, wachsen für Kläger die Hürden für die Darlegung und den Beweis von Schadensersatzansprüchen. Gleichzeitig ändert die Entscheidung nichts daran, dass Unternehmen gesetzlich und gegenüber den Behörden zur Dokumentation und Rechenschaft verpflichtet sind. Im Schadensersatzprozess hilft dem betroffenen Kläger zudem die sekundäre Darlegungslast, die den Datenverarbeiter im Zweifel verpflichtet, technische Interna und Umstände aus der eigenen Sphäre nach einem ersten Aufschlag des Klägers vorzutragen.

VG Mainz: Anforderungen an die Verschlüsselung von E-Mails

Wie sind E-Mails unter Geltung der DSGVO zu verschlüsseln? Genügt die standardmäßige Transportverschlüsselung oder muss stets eine Ende-zu-Ende-Verschlüsselung eingerichtet werden? Zu dieser Frage bezog das VG Mainz im Dezember 2020 Stellung. Im konkreten Fall ging es um die Pflichten eines Berufsgeheimnisträgers (konkret eines Rechtsanwalts), jedoch hat die Entscheidung auch Bedeutung für Wirtschaftsunternehmen.

In dem der Entscheidung zugrundeliegenden Fall (VG Mainz, Urteil vom 17.12.2020 – Aktenzeichen 1 K 778/19.MZ, hier abrufbar) hatte ein Rechtsanwalt per E-Mail Anhänge zu einer Erbschaftssache versandt, ohne dabei eine qualifizierte Verschlüsselung zu benutzen. Standardmäßig werden E-Mails mittels Transportverschlüsselung (SSL/TLS) versendet. Hierbei wird der Inhalt der E-Mail jeweils auf den beteiligten Servern ent- und wieder verschlüsselt. Daher besteht ein vollständiger Schutz durch Verschlüsselung lediglich auf dem Transport zwischen den Servern. Nur bei Verwendung einer Ende-zu-Ende-Verschlüsselung wie S/MIME oder PGP ist gewährleistet, dass die Informationen ausschließlich von Sender und Empfänger abgerufen werden können.

Da der Anwalt nur die reguläre Transportverschlüsselung nutzte, sprach die rheinland-pfälzische Datenschutzbehörde ihm gegenüber eine Verwarnung aus.

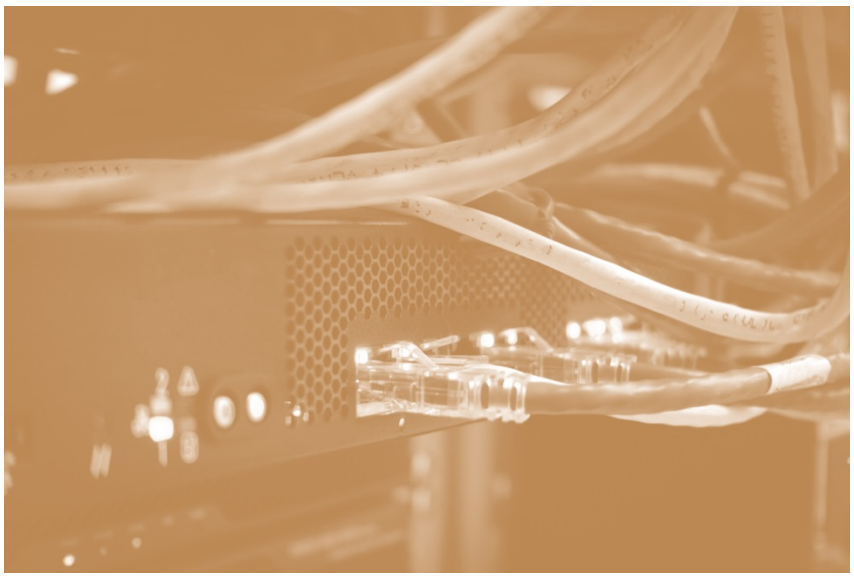
Begründet wurde diese mit einem Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO, wonach personenbezogene Daten nur in einer Weise verarbeitet werden dürfen, die eine angemessene Sicherheit der Daten gewährleistet: Als Rechtsanwalt sei der Kläger Berufsgeheimnisträger. Er sei also unter Strafandrohung zur Wahrung der Geheimnisse seiner Mandanten verpflichtet.

Dies allein führt nach Ansicht des VG Mainz allerdings nicht dazu, dass alle vom Rechtsanwalt versandten E-Mails als so sensibel anzusehen seien, dass nur eine Ende-zu-Ende-Verschlüsselung angemessen sei. Zwar mag eine besonders starke Verschlüsselung da erforderlich sein, wo Daten wie rassische und ethnische Herkunft, politische Meinungen, religiöse Überzeugungen oder ähnlich sensible Informationen verarbeitet werden. Jedoch sei nicht jede mandatsbezogene Information, die ein Rechtsanwalt verarbeitet hinreichend kritisch. Ob eine besonders aufwendige Ende-zu-Ende-Verschlüsselung vorzunehmen sei, müsse letztlich gem. Art. 32 DSGVO nach dem konkreten Eintrittsrisiko eines besonders schweren Risikos für die Rechte und Freiheiten der betroffenen Person entschieden werden.

Das Gericht betont explizit, dass somit regelmäßig eine einfache Transportverschlüsselung bei der Versendung von E-Mails ausreiche. Dies sei der Standard im geschäftlichen Verkehr und das potentielle, aber sehr geringe Risiko, dass es auf den Mailservern zur unerlaubten Kenntnisnahme von Inhalten komme, gehöre zum normalen Lebensrisiko.

Die Entscheidung ist auch für Nicht-Berufsgeheimnisträger interessant, da das Gericht herausarbeitet, dass ganz allgemein eine Ende-zu-Ende-Verschlüsselung nur in Einzelfällen erforderlich ist. Nur in den Fällen besonders sensibler Daten gemäß Art. 9 und 10 DSGVO oder in vergleichbar kritischen Fällen mit hohem Risiko ist es geboten, auf ein solches Sicherheitsinstrument zurückzugreifen. Im konkreten Fall dürfe die Auswahl der Verschlüsselungsmethode nicht zu schematisch beurteilt werden. Für Unternehmen gilt es daher, in Zweifelsfällen genauer die Risiken einer nur standardmäßig verschlüsselten Kommunikation zu evaluieren.

Das VG Mainz entscheidet damit aber auch entgegen strengerer Ansichten mehrerer Landes-Datenschutzbehörden. Ob sich die Rechtsansicht des VG bundesweit durchsetzen wird, bleibt daher abzuwarten.



Das Bundeskartellamt als Datenschutzbehörde? Facebook-Streit landet vor dem EuGH

Das OLG Düsseldorf bleibt skeptisch: Durfte das Bundeskartellamt Facebook das Datensammeln verbieten und liegt ein Missbrauch einer marktbeherrschenden Stellung des US-Konzerns vor? Der EuGH soll nun entscheiden. Den Hintergrund dieses Streits der letzten zwei Jahre sowie die problematisierten Fragestellungen, insbesondere im Hinblick auf die mögliche Schnittstelle von Datenschutz und Wettbewerb, stellen wir Ihnen im Folgenden kurz dar.

Der Streit zwischen dem Bundeskartellamt (BKartA) und Facebook beschäftigt die Justiz bereits seit Jahren intensiv, wir haben dazu bereits verschiedentlich berichtet. Spannend ist vor allem, dass das BKartA, welches sich ansonsten mit kartellrechtlichen Fällen befasst, hier datenschutzrechtliche Belange mit dem kartellrechtlichen Problem des Missbrauchs einer marktbeherrschenden Stellung verknüpft. Besitzt ein Unternehmen eine marktbeherrschende Stellung einerseits, und verstößt es gegen datenschutzrechtliche Vorgaben andererseits, könnte dies nach Auffassung des BKartA einen Missbrauch ebendieser Stellung

darstellen, weshalb es sich für zuständig sah, auch hierüber mitzuentscheiden. Ob es mit der grundsätzlichen Annahme, dass es dies dürfe, und auch in seinem Beschluss inhaltlich richtiglag, muss nun der Europäische Gerichtshof (EuGH) bewerten (Vorlageentscheidung des OLG Düsseldorf vom 24.03.2021-Aktenzeichen VI-Kart 2/19 (V)).

Nachdem das BKartA Facebook im Februar 2019 untersagt hatte, die Nutzerdaten der Facebook-Töchter WhatsApp und Instagram sowie Webseiten anderer Anbieter ohne ausdrückliche Zustimmung der Nutzer mit deren Facebook-Konten zu verknüpfen, landete dieser Fall nach Durchlaufen des Instanzenzugs wieder beim Oberlandesgericht in Düsseldorf, welches ihn nun dem EuGH zur Klärung vorlegte: Geklärt werden soll, ob das BKartA dem Datensammeln durch Facebook aus Gründen des Datenschutzes überhaupt einen Riegel vorschieben kann, und ob darüber hinaus Facebook tatsächlich eine marktbeherrschende Stellung missbräuchlich ausnutzt, indem es Daten der Nutzer unter Verstoß gegen Regeln des Datenschutzes sammelt und verwendet.

Das BKartA stellt sich auf den Standpunkt, ohne ausdrückliche und wirksame Einwilligung der Nutzer stelle das Ausmaß, in dem Facebook auf diese Art Daten sammle und zwischen seinen Diensten teile, einen Missbrauch seiner Marktmacht dar. Marktbeherrschend sei Facebook auf dem nationalen Markt für soziale Netzwerke für private Nutzer. Da die Verwendung von Datenverarbeitungskonditionen als Ausfluss von Marktmacht auch gegen datenschutzrechtliche Wertungen verstoßen kann, sei der angeführte Missbrauchstatbestand des § 19 Abs. 1 GWB auch hierauf anwendbar. Sollte eine solche Einwilligung außerdem versagt werden, dürfe Facebook den Betroffenen darüber hinaus nicht an der Nutzung seiner Dienste hindern. Facebook verneint hingegen schon eine Marktbeherrschung, da es mit vielen anderen Angeboten wie Youtube, Snapchat oder Twitter konkurriere.

Den Ausführungen des EuGH ist gespannt entgegenzusehen. Sollte es mit dem BKartA übereinstimmen, würde dies eine weitere Verschmelzung datenschutzrechtlicher und wettbewerbsrechtlicher Materie bedeuten, und gerade im Kartellrecht würden dann noch strengere und umfassendere Vorsichtsmaßnahmen marktbeherrschender Unternehmen gefordert, möchten sie neben

einem möglichen Verstoß gegen Datenschutzrecht auch dem Vorwurf des Missbrauchs marktbeherrschender Stellung entgehen.

Zu guter Letzt

Auch in diesem Monat gibt es wieder einige bemerkenswerte Randnotizen und interessante Bußgeldentscheidungen aus den anderen EU-Mitgliedstaaten. So hat sich die DSK zum „Energieversorgerpool" positioniert. Berichtenswerte Bußgelder der Nachbarländer bezogen sich auf Marketingmaßnahmen und – wie so oft – Mängel der Datensicherheit bzw. unzulängliche Meldungen nach einer Datenpanne.

- **DSK zum „Gläsernen Verbraucher" im „Energieversorgerpool"**

Seit einiger Zeit wird diskutiert, ob das Ansinnen in der Energiebranche, „wechselwillige Kunden" zu identifizieren, datenschutzrechtlich zulässig ist. Die Datenschutzkonferenz (DSK) positionierte sich nun dagegen: Auskunfteien in Zusammenarbeit mit Energieversorgern könnten sich nicht auf berechtigte Interessen i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO berufen, um sog. Positivdaten in einem Datenpool zu sammeln mit dem Ziel, festzustellen, ob ein Kunde ein langfristiges Vertragsverhältnis in Betracht zieht. Vermeintliche „Schnäppchenjäger" und wechselwillige Kunden, die etwa über die Erzielung eines Neukundenbonus besonders günstige Konditionen suchen, bereits bei Vertragsanbahnung als solche zu identifizieren und

gegebenenfalls von Angeboten ausschließen zu können, stelle kein berechtigtes Interesse i.S.d. Art. 6 UAbs. 1 Abs. 1 Satz 1 lit. f) DSGVO dar. Selbst wenn man ein berechtigtes Interesse der Unternehmen annähme, überwögen jedenfalls die schutzwürdigen Interessen und Grundrechte der Kunden. Diese dürften im vertragstreuen Rahmen erwarten, dass keine über den Vertragszweck hinausgehende Verarbeitung ihrer Daten erfolge, die gegebenenfalls ihre Möglichkeit einschränke, frei am Markt agieren zu können. Der Beschluss der DSK vom 15.03.2021 ist hier abrufbar. Unmittelbare Rechtswirkung entfaltet er nicht, letztlich gibt er lediglich die Rechtsauffassung der DSK wieder, Behördenentscheidungen in diesem Sinne bleiben voll gerichtlich überprüfbar.

- **Italien: Bußgeld in Höhe von 4,5 Mio. Euro wegen aggressiven Telemarketings**

Die italienische Datenschutzbehörde erließ gegen Fastweb SpA ein Bußgeld in Höhe von 4.501.686 €. Nach hunderten Beschwerden über aggressives Telemarketing durch Fastweb und dessen Vertriebsnetz stellte die Behörde zahlreiche Verstöße gegen die DSGVO fest. Für Fastweb tätige Callcenter verwendeten für ihre Anrufe häufig Telefonnummern, welche nicht im italienischen Register für Kommunikationsbetreiber gelistet waren. Außerdem verarbeiteten sie für Werbetätigkeiten Kontaktdaten, die Fastweb von externen Partnern ohne entsprechende Einwilligung der Betroffenen bezogen hatte. Weiterhin wurden von Dritten erhaltene Kundenlisten verwendet, ebenfalls ohne entsprechende Einwilligung der Betroffenen für künftige Werbemaßnahmen. Betroffen waren von der Verarbeitung ihrer Kontaktdaten ohne Einwilligung über 7.542.000 Personen.

Für Betroffene bestand auch keine Möglichkeit, eine freie, spezifische und informierte Einwilligung zu erteilen. Bevor das Ticket geschlossen wurde, wurden die Betroffenen in Abständen von 15 bis zu 20-mal zurückgerufen. Bei derart invasiven technischen Vorgehensweisen hätten die Betroffenen über sie informiert werden müssen, stellte die Datenschutzbehörde fest. Eine einfache, automatisierte Möglichkeit der Deaktivierung des Rückruf-Services bestand nicht. Es fehlte somit auch ein System des Bußgeldempfängers, das den Betroffenen die ordnungsgemäße Ausübung ihrer Rechte ermöglicht hätte.

Damit nicht genug: Die Telefonnummern der Betroffenen gelangten mangels Implementierung adäquater technischer und organisatorischer Maßnahmen für die Sicherheit der Verarbeitung personenbezogener Daten (Art. 32 Abs. 1 DSGVO) an Kriminelle, die diese dann via Whatsapp kontaktierten, um an Ausweisdokumente zu gelangen.

Erschwerend wurde berücksichtigt, dass es sich um schwere Verstöße mit hohem Risiko für die Betroffenen handelte, dass die Verstöße über einen langen Zeitraum bestanden hatten, dass viele Personen davon betroffen waren, dass sich die Verstöße teils aus einer schweren Fahrlässigkeit seitens Fastwebs ergaben und dass die Datenschutzbehörde zuvor bereits ähnliche Anordnungen an den Bußgeldempfänger ausgesprochen hatte. Mildernd kam zu tragen, dass Fastweb mit der Datenschutzbehörde koordinierte und entsprechende Maßnahmen zum Schutz der Verarbeitung umsetzte.

- **Spanien: Bußgeld wegen unzulänglicher Datensicherung bei Hackerangriff**

Die spanische Datenschutzbehörde verhängte ein Bußgeld von insgesamt 600.000 Euro gegen die Fluglinie Air Europa Lineas Aéras S.A. Über einen Zeitraum von mehreren Monaten konnten Hacker zahlreiche Kreditkartennummern von Kunden abschöpfen. Betroffen waren ca. 489.000 Kunden mit rund 1.500.000 zugehörigen Aufzeichnungen. Die Hacker verwendeten ein Entschlüsselungstool, das sie auf den Unternehmenssystemen fanden. Außerdem hatte das Unternehmen Kreditkartendaten nicht separat von anderen personenbezogenen Daten der Karteninhaber gespeichert. Hierin erkannte die spanische Datenschutzbehörde eine Verletzung der Pflicht des Verantwortlichen, angemessene technischen und organisatorische Maßnahmen zum Schutz der Verarbeitung personenbezogener Daten zu implementieren gem. Art. 32 Abs. 1 DSGVO. Außerdem hatte das Unternehmen die Datenpanne nicht fristgemäß binnen 72 Stunden nach Bekanntwerden an die Datenschutzbehörde gemeldet (Art. 33 Abs. 1 Satz 1 DSGVO). Berücksichtigt wurde zudem, dass der Vorfall nicht nur lokal beschränkt war, sondern sehr viele Menschen weltweit betraf und sich der Datendiebstahl über mehrere Monate erstreckte, sowie durch Versäumnis von Air Europa bezüglich angemessener Sicherheitsmaßnahmen begünstigt wurde.

- **Niederlande: Verspätete Meldung einer Datenpanne**

Auch ein internationales und bekanntes Online-Portal wie Booking.com ist vor Datenpannen nicht gefeit: Cyber-Kriminellen war es gelungen, die Daten von über 4.109 Kunden der Seite zu entwenden. Hierzu gehörten nicht nur Namen, Adressen, Telefonnummern und Details zu Hotelbuchungen, auch Kreditkarteninformationen – teilweise inklusive des Sicherheitscodes – befanden sich unter den gestohlenen Daten. Deshalb bestand ebenfalls für diejenigen Kunden, deren Kreditkartendaten nicht betroffen waren, ein hohes Sicherheitsrisiko. Auch Ihre Kontaktdaten wurden für Phishing-Angriffe verwendet. Da das Online-Portal diese Datenpanne aber nicht etwa innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls meldete (Art. 33 Abs. 1 Satz 1 DSGVO), sondern erst nach 22 Tagen, verhängte die niederländische Datenschutzbehörde ein Bußgeld in Höhe von 475.000 Euro.

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