LOSCHELDER

Newsletter Datenschutzrecht
November 2020

Sehr geehrte Damen und Herren,

die letzten Wochen waren datenschutzrechtlich erneut turbulent. Das LG Bonn hat das 1&1-Bußgeld final verhandelt und am 11.11.2020 sein Urteil verkündet. Interessante Entscheidungen gab es darüber hinaus zu den zivilrechtlichen Folgen von Datenpannen und – erneut vom EuGH – zur Wirksamkeit von Einwilligungen. Schließlich ringen auch die Aufsichtsbehörden weiter um einen datenschutzkonformen und praktikablen Umgang mit den Folgen des EuGH-Urteils in Sachen Schrems II (Stichwort: US-Transfer von Daten), die Kommission versucht einen Beitrag mit ihren jüngst veröffentlichten Entwürfen für neue Standardvertragsklauseln zu leisten. All dies fassen wir für Sie in diesem Newsletter zusammen.

Ein besonders brisantes Thema greifen wir darüber hinaus in unserem nächsten **Lunch@Loschelder Webinar am 25.11.2020 um 12 Uhr** auf:

DSGVO-Bußgelder: Wer haftet wie hoch?

Anlässlich der Verhandlung des 1&1-Bußgeldes vor dem LG Bonn werfen wir einen Blick auf die wichtigsten Fragen zur Risikoermittlung: Wen kann ein Bußgeld treffen – das Unternehmen oder auch Geschäftsführer und Vorstände? Und wie lassen sich die Höhe und damit auch das konkrete Risiko für Ihr Unternehmen ermitteln? Dr. Kristina Schreiber und Dr. Simon Kohm werden sich diesen Themen im Gespräch widmen.

Die Teilnahme am Webinar ist kostenfrei. Über Anmeldungen freuen wir uns unter webinare@loschelder.de – weitere Informationen gibt es auch unter **https://loschelder.de/de/webinare.html**.

Inhalt

LG Bonn reduziert 9-Millionen-Bußgeld gegen 1&1 auf 900.000 Euro

Das LG Bonn hat in erster Instanz das vielbeachtete Bußgeld des BfDI gegen den Telekommunikationsunternehmens 1&1 in Höhe von 9,55 Millionen Euro mit Urteil vom 11.11.2020 auf 900.000 Euro reduziert. Anlass für das Bußgeld war der Erfolg eines Anrufers, durch Angabe des Namens und Geburtsdatums Informationen zu seinem Ex-Lebenspartner als Vertragsinhaber herauszufinden. Nach Ansicht des BfDI stellte die Authentifizierung über Name und Geburtsdatum keine ausreichende Schutzmaßnahme dar. Die nunmehr ergangene Entscheidung des LG Bonn hat ganz besondere Relevanz für die datenschutzrechtliche Compliance, weit über den Fall der 1&1 hinaus:

Unmittelbares Unternehmensbußgeld?

Umstritten war von Beginn an, ob ein Bußgeld unmittelbar gegen das Unternehmen überhaupt zulässig sein kann. Schwierig zu beurteilen ist dies deswegen, weil ein solches Bußgeld bei Anwendung des nationalen Ordnungswidrigkeitenrechts nur unter sehr engen Voraussetzungen möglich ist: Die nationale Norm des § 30 OWiG sieht dafür nämlich vor, dass eine Handlung einer Person benannt werden kann, die in besondere Verantwortung für das Unternehmen tätig geworden ist. Das LG Bonn kommt hier zu dem Ergebnis, dass eine unmittelbare Bußgeldhaftung des Unternehmens europarechtlich, unmittelbar aus der DSGVO heraus, geboten ist und daher die nationalen Bußgeldvorschriften zurücktreten.

Geeignete technische und organisatorische Maßnahme

Im Zentrum der Verhandlung stand ferner die Frage, ob 1&1 bei der Implementierung einer Authentifizierung mittels Name und Geburtsdatum eine ausreichende technisch und organisatorische Schutzmaßnahme im Sinne des Art. 32 DSGVO ergriffen hatte. Die Frage nach dem ausreichenden Schutzniveau muss sich der Verantwortliche immer schon vor Beginn seiner Datenverarbeitung und im Anschluss daran immer wieder regelmäßig stellen und je nach dem Ergebnis seiner Analyse Schutzmaßnahmen nachbessern. Die DSGVO gibt in Art. 32 Abs. 1 insgesamt acht Kriterien an die Hand, die bei der Beurteilung des erforderlichen Schutzes berücksichtigt werden müssen; darunter finden unter anderem der „Stand der Technik“, die Implementierungskosten und die

Eintrittswahrscheinlichkeit eines Risikos. Das LG Bonn hat die von 1&1 praktizierte Authentifizierung für unzureichend gehalten und einen Datenschutzverstoß festgestellt. Die dogmatische Begründung liefern wir Ihnen im Detail nach, sobald die Urteilsgründe verfügbar sind.

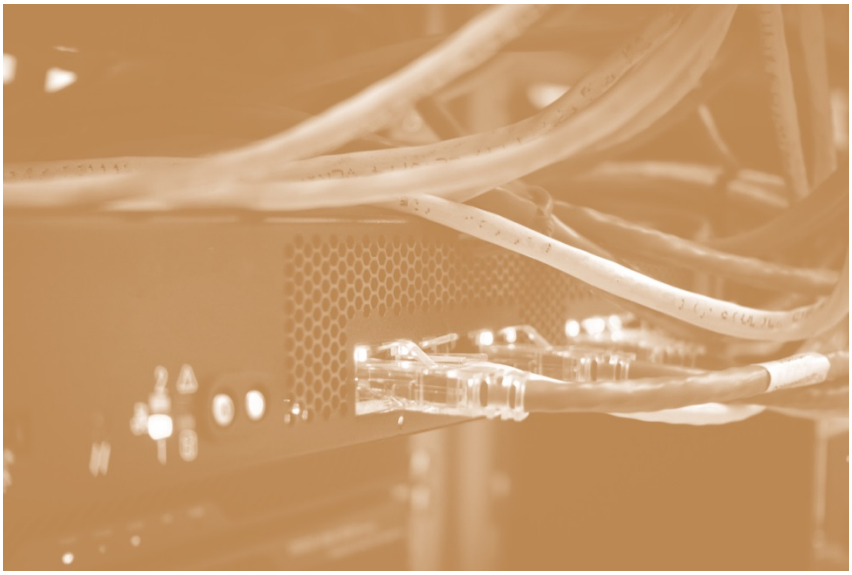
Bußgeldhöhe

Besonders interessant ist dieses Verfahren vor allem deswegen, weil sich ein deutsches Gericht zum ersten Mal mit dem Bußgeld-Bemessungskonzept der DSK befassen musste. Der BfDI hatte sich bei der Berechnung des Bußgeldes in erster Linie an dem Umsatz der Unternehmensgruppe, der 1&1 angehört (vgl. Tabelle auf Seite 6 des Konzepts), orientiert und darauf aufbauend eine Höhe von 9,55 Millionen Euro festgesetzt. Nach der DSGVO sind für die Bemessung eines angemessenen Bußgeldes die in Art. 83 Abs. 2 DSGVO aufgezählten Kriterien zu beachten, worunter beispielsweise die Art, Schwere und Dauer des Verstoßes oder der Umfang des Schadens, den der Verstoß zur Folge hatte, fallen. Der BfDI hatte den Verstoß u.a. aufgrund der Kooperationsbereitschaft und der zwischenzeitlichen Nachbesserung als gering eingestuft. Das im 1&1-Fall überprüfte Bußgeld orientierte sich nichtsdestotrotz in erster Linie und maßgeblich nach dem Unternehmensumsatz – vergleichbar mit einem „Tagessatz", als Ausgangspunkt, obwohl die DSGVO ein solches umsatzbezogenes Bußgeld nicht ausdrücklich vorsieht. Im Ergebnis hat das Gericht das Bußgeld denn auch auf 900.000 Euro herabgesetzt, dem Vernehmen der mündlichen Ausführungen nach gerade auch, weil die ursprüngliche Berechnung dem reinen Umsatz zu hohes Gewicht beigemessen hat. Das Verschulden von 1&1 sei gering. Im Hinblick auf die über Jahre geübte Authentifizierungspraxis, die bis zu dem Bußgeldbescheid nicht beanstandet worden sei, habe es dort an dem notwendigen Problembewusstsein gefehlt. Zudem sei zu berücksichtigten, dass es sich – auch nach der Ansicht des BfDI – nur um einen geringen Datenschutzverstoß handelte. Dieser habe nicht zur massenhaften Herausgabe von Daten an Nichtberechtigte führen können.

Konsequenzen für die Praxis

Die Konsequenzen für die Praxis sind erheblich. Insbesondere verdeutlicht das Urteil, dass bereits einfache und auf den ersten Blick kleine Verstöße, auch auf unterer Arbeitsebene, zu erheblichen

Bußgeldern führen können. Nicht notwendig ist, dass ein Verstoß von der Geschäftsleitung, einer Abteilungsleitung oder einem leitenden Mitarbeiter begangen wird. Das bedeutet, dass eine Schulung von Mitarbeitern und ihrer Sensibilisierung weiterhin ein enormes Gewicht zukommen. Nur so kann gewährleistet werden, dass Mitarbeiter bestehende Risiken erkennen und entsprechend agieren. Das gilt vor allem, weil die Erfahrung zeigt, dass sich oftmals kleine Fehler oder Unzulänglichkeiten zu erheblichen Risiken auswachsen können. In Sachen Bußgeldhöhe bedeutet die Entscheidung des LG Bonn vor allem, dass Fälle nicht nach „Schema F“ und rein nach Umsatzwerten beurteilt werden können, soweit sich diese Rechtsauffassung durchsetzt. Vielmehr ist eine differenzierte Einzelfallbetrachtung geboten, die vor allem die Schwere des Verstoßes und den Grad der Vorwerfbarkeit berücksichtigt – ein mit Blick auf die differenzierten DSGVO-Vorgaben überzeugender Ansatz. Hier bleibt abzuwarten, wann die Behörden die bereits angekündigte Überarbeitung ihres Bußgeldkonzepts veröffentlichen.



Zivilrechtliche Folgen von Datenpannen

Von einer Datenpanne Betroffene können sich beim Verantwortlichen auch zivilrechtlich schadlos halten. Einen solchen Anspruch auf Unterlassung und Schadensersatz hatte das Landgericht Frankfurt am Main kürzlich zu entscheiden – anknüpfend an die Veröffentlichung von rund 90.000 Kundendaten aus einem Mastercard-Kundenbindungsprogramm.

In seiner Entscheidung aus dem September hatte sich das LG Frankfurt am Main (LG Frankfurt am Main, Urteil vom 18.09.2020, Az. 2/27 O 100/20) mit den Folgen der unbefugten Veröffentlichung von Kundendaten zu befassen. Die Daten lagen bei einem Auftragsdatenverarbeiter, auf dessen Systeme unbefugt zugegriffen wurde. Noch währen umfangreiche Analysen zum Anlass und mögliche Auswirkungen dieses Zugriffs liefen, erfolgte die Veröffentlichung von rund 90.000 Kundendaten, womit sich das Risiko für die Betroffenen realisierte.

Das Spannende an dieser Entscheidung: Einer der 90.000 Kunden klagte in der Folge zivilgerichtlich auf Unterlassung der weiteren Verarbeitung seiner Daten und auf Schadensersatz sowie Auskunft, eine der ersten durchentschiedenen Klagen dieser Art.

Der **Unterlassungsanspruch** wurde überzeugend abgelehnt: Zu einer Unterlassung der Datenverarbeitung sei die verantwortliche Mastercard-Tochter nicht verpflichtet, solange die mit der Teilnahme am Bonusprogramm erteilte Einwilligung des Klägers in die Datenverarbeitung fortbesteht. Soweit der Kläger die Unterlassung der (unzulässigen) Veröffentlichung seiner Daten begehrt, fehlte es an einer Wiederholungsgefahr. Hier allerdings zeigt sich, dass Verantwortliche auch aus zivilrechtlicher Perspektive tätig werden müssen: Die Datenpanne führt dazu, dass eine Wiederholungsgefahr zunächst vermutet wird – der verantwortliche Datenverarbeiter muss diese Vermutung widerlegen, etwa durch die Implementierung technisch-organisatorischer Sicherheitsmaßnahmen, die vergleichbare Vorfälle künftig ausschließen. Kurzum: Beendet der Kläger seine Teilnahme am Bonusprogramm, endet auch die Datenverarbeitung, vorher aber nicht. Und: Eine Datenpanne spricht dann nicht zugleich für eine Wiederholungsgefahr, wenn der Verantwortliche anlässlich der Verletzung technisch-organisatorisch tätig wird, um erneute Sicherheitsvorfälle zu vermeiden.

Auch einen Anspruch auf Zahlung eines **Schadensersatzes** lehnte das Gericht ab, weil es keinen kausal auf der Datenpanne beruhenden Schaden des Klägers sah. Der Kläger begehrte Zahlung von 8.400 Euro wegen ihm entstandener immaterieller Schäden. Das LG Frankfurt prüft sehr präzise, welche Verletzungen der DSGVO der Kläger geltend macht und ob diese dem Beklagten anzulasten sind. So ist etwa die Veröffentlichung der Daten kein der Beklagten anzulastender DSGVO-Verstoß: Sie selbst hat die Daten nicht veröffentlicht, sondern ein Dritter. Denkbar wäre es wohl gewesen, unzureichende Datensicherheitsmaßnahmen nach Art. 32 DSGVO beim Auftragsverarbeiter und eine diesbezüglich unzureichende Kontrolle durch die verantwortliche Beklagte zu diskutieren. Eine solche Rüge aber hat der Kläger nicht hinreichend substantiiert erhoben. Im Zivilverfahren führt dies dann zu Anspruchsabweisung – anders, als im Verwaltungsverfahren ist der Kläger vollumfänglich darlegungs- und beweisbelastet.

Das LG Frankfurt verneinte schließlich einen **Auskunftsanspruch** des Klägers, gestützt auf § 242 BGB, über Dauer und Umfang von Rechtsverletzungen bei der Datenverarbeitung, da es schon an einem zugrundeliegenden Leistungsanspruch des Klägers fehlte.

EuGH: Einwilligung in AGB?

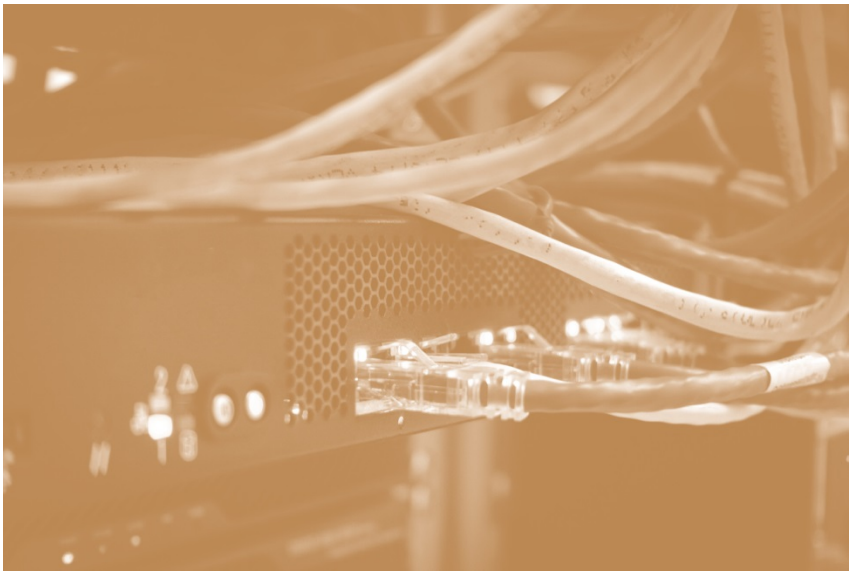
Der EuGH setzte sich jüngst mit dem Zusammenspiel von AGB und dem Nachweis einer Einwilligung in die Aufbewahrung von Ausweiskopien auseinander; in seinem Urteil formuliert der EuGH klare Voraussetzungen.

Der EuGH hat in einem Vorabentscheidungsersuchen eines rumänischen Gerichtes (Urteil vom 11.11.2020, Rs. C-61/19) für eine weitere Klarstellung in Sachen Wirksamkeitsanforderungen an eine datenschutzrechtliche Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchstabe a, Art. 7 DSGVO gesorgt: Ein angekreuztes Kästchen in den AGB zur Information und Einwilligung in die Datenverarbeitung reicht nicht aus, um die Erteilung einer wirksamen Einwilligung nachzuweisen. Ist ein solches Kästchen vorangekreuzt, kann darüber keine wirksame Einwilligung eingeholt werden (diese Aussage entspricht jener des EuGHs in der Sache Planet49 – wirksam ist eine Einwilligung nur, wenn der Betroffene selbst aktiv wird).

Anlass für die Entscheidung war die Praxis des Telekommunikationsunternehmen Orange Rumänien, in ihren AGB ein Kästchen zu der Klausel über die Bestätigung der Information zur Aufbewahrung von Ausweiskopien und die dahingehende Zustimmung vorzusehen und voranzukreuzen. Den Nachweis einer wirksam erteilten Einwilligung sieht der EuGH bei einer solchen angekreuzten Klausel in den AGB nicht gegeben: Es sei zu unklar, ob der Betroffene tatsächlich die Klausel gelesen und verstanden habe. Außerdem sei schon zweifelhaft, ob die Einwilligungen in dieser Konstellation überhaupt wirksam erteilt wurden: Orange Rumänien habe die Klausel zu der datenschutzrechtlichen Einwilligung nicht ausreichend von den sonstigen AGB-Klauseln abgesetzt. Außerdem sei bei Ablehnung der Einwilligung das Ausfüllen eines Sonderformulars erforderlich gewesen, was die Freiwilligkeit erteilter Einwilligungen in Frage stelle. Zu diesen Punkten wird das nationale Gericht in Rumänien noch weitere Aufklärung betreiben und dann entscheiden müssen.

Mit diesem Urteil bestätigt der EuGH die Einschätzung vieler Datenschützer zu den Anforderungen an eine wirksame Einwilligung samt Nachweispflicht nach Art. 7 Abs. 1 DSGVO. Wenn eine Einwilligung im Rahmen von AGB verortet wird, muss

diese klar hervorgehoben sein und vom Kunden aktiv und gesondert bestätigt werden. Neben dem so bestätigten Dokument erfordert der Nachweis die Absicherung, dass eben keine Kästchen „vorangekreuzt“ waren. In der Praxis ist dies etwa durch Protokolle und dokumentierte Programmierungseinstellungen im Online-Bereich möglich; offline ist eine Unterschrift hier eine sichere Option.



Weiter geht es in Sachen US-Transfer: Neue Empfehlungen des EDSA und überarbeitete SCCs

Nachdem der EuGH in seiner sog. Schrems II-Entscheidung im Juli den Datentransfer in die USA über das sogenannte Privacy Shield gekippt hatte, ringen deutsche und europäische Unternehmen um eine datenschutzkonforme Lösung: Unzählige Diensteanbieter sitzen in den USA, nicht immer gibt es alternative EU-Lösungen, nicht immer ist eine Migration der Daten mit verhältnismäßigem Aufwand möglich. Praktikable Lösungsansätze haben die Datenschutzaufsichtsbehörden bislang kaum veröffentlicht, sodass Rechtsunsicherheit herrscht. Wir stellen Ihnen dar, ob dies mit den neuesten Empfehlungen des Europäischen Datenschutzausschusses anders wird. Außerdem werden die Standardvertragsklauseln auf EU-Ebene aktuell überarbeitet.

Der Zusammenschluss der europäischen Datenschutz-aufsichtsbehörden, der Europäische Datenschutzausschuss (EDSA), hat Mitte November Empfehlungen zum Umgang mit Datentransfers in Drittstaaten veröffentlicht. Zurück gehen diese

auf das Schrems II-Urteil des EuGH aus Juli 2020 (wir haben das Urteil und seine Folgen in unserem Sondernewsletter sowie hier für Sie aufbereitet).

Zur Erinnerung: Der EuGH hatte das sog. EU-U.S.-Privacy Shield für unwirksam erklärt und auch die Nutzbarkeit von Standardvertragsklauseln für den US-Transfer bezweifelt. Damit stellt sich die Frage, ob und wie im konkreten Transferfall ein angemessenes Datenschutzniveau nach Maßgabe der Art. 44 ff. DSGVO in den USA gewährleistet werden kann – die bisher praktizierten „simplen" Lösungen, ohne Detailprüfungen auf das Privacy Shield zu verweisen oder Standardvertragsklauseln abzuschließen, entfielen mit diesem Urteil jedenfalls.

Die nun veröffentlichten Empfehlungen des EDSA sollen Datenübermittlern die Prüfung erleichtern, ob im Rahmen eines konkreten Transfers ein angemessenes Datenschutzniveau im Zielland gewährleistet ist: Sie setzten sich zusammen aus einem allgemeinen „Fahrplan" für die Feststellung, ob und welche Zusatzmaßnahmen für Datentransfers über Standard-vertragsklauseln zu ergreifen sind (Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data) sowie der Erläuterung, wann Regelungen über den Zugriff auf personenbezogene Daten durch staatliche Stellen den Rechtsstandards der EU entsprechen (Recommendations 02/2020 on the European Essential Guarantees for surveillance measures). Damit möchte der EDSA es Datenübermittlern erleichtern, die Anforderungen der DSGVO an Datentransfers in Staaten außerhalb der EU und des Europäischen Wirtschaftsraums (EWR) einzuhalten.

Aber wirken diese Empfehlungen auch in der Praxis als Erleichterung?

Fahrplan für Datentransfers

Hilfreich ist im Ausgangspunkt der „Fahrplan" des EDSA für die notwendigen unternehmensinternen Überprüfungen. Dessen Eckpunkte indes weichen kaum von dem ab, was wir bereits kurz nach dem EuGH-Urteil (siehe Sondernewsletter sowie hier) und etwa vor einigen Wochen auch bereits der LfDI BW geraten haben. Nichtsdestotrotz: Es reduziert die Rechtsunsicherheiten für die betroffenen Unternehmen, die sich durch ein klares Abarbeiten des

Fahrplans ein Stück weit entlasten und Bußgeldrisiken zumindest mindern können.

Der Sechs-Punkte-Fahrplan des EDSA umfasst:

1. **Kenntnis der Daten:** Welche Daten werden zu welchem Zweck, an wen und in welche Drittstaaten übermittelt?

2. **Grundlage des Transfers:** Auf welche Rechtsgrundlage wurde der Transfer bisher gestützt und „hält diese" auch künftig noch (z.B. Angemessenheitsbeschluss der Kommission, Standardvertragsklauseln).

3. **Überprüfung der rechtlichen Gegebenheiten im Zielland:** Wie sind die rechtlichen Gegebenheiten im Empfängerland, bestehen insbesondere Zugriffsrechte von nationalen Institutionen, die etwa durch vertragliche Regelungen zwischen den Parteien nicht begrenzt werden können? Welche Kriterien hierbei zu prüfen sind, konkretisiert der EDSA in seinen Empfehlungen 2/2020 (Recommendations 02/2020 on the European Essential Guarantees for surveillance measures).

4. **Auswahl von Zusatzmaßnahme:** Ergibt die Prüfung unter 3., dass etwa Zugriffsrechte bestehen, sind Zusatzmaßnahmen zur Sicherstellung des adäquaten Datenschutzniveaus zu prüfen. Diese können vertraglicher, organisatorischer oder technischer Natur sein. **Ein echter Zugewinn für die Praxis** ist die Liste des EDSA, welche Zusatzmaßnahmen denkbar sind: Der EDSA konkretisiert Anforderungen an eine wirksame Datenverschlüsselung, die Möglichkeiten der Übermittlung nur pseudonymisierter Daten, eine Aufteilung von Daten. Zudem listet der EDSA mögliche vertragliche Zusatzabsprachen und Pflichten zum Tätigwerden. All diese können Lösungsoptionen in Individualverhältnissen bieten – im Massengeschäft etwa über Facebook, Google o.ä. werden sie aber kaum helfen.

5. **Formelle Anforderungen:** Werden Zusatzmaßnahmen ergriffen, ist zudem zu prüfen, ob diese individuell von der Aufsichtsbehörde genehmigt werden müssen, Art. 46 DSGVO.

6. Die eingesetzten Maßnahmen sind **regelmäßig und fortlaufend zu überprüfen**, ob sie weiterhin geeignet sind, ein vergleichbares Datenschutzniveau herzustellen.

Kann nach alledem endgültig kein angemessenes Datenschutzniveau im Drittland sichergestellt werden, ist der weitere Transfer personenbezogener Daten einzustellen oder eine Meldung bei der Aufsichtsbehörde zu erstatten.

Damit im Einklang stehend gibt es auch Neuigkeiten von den nationalen Datenschutzaufsichtsbehörden: Der LDI Rheinland-Pfalz veröffentlichte ein Schaubild über die Prüfung eines datenschutzkonformen Datentransfers in Drittstaaten ebenso wie der Bundesbeauftragte für Datenschutz und Informationsfreiheit. Auch die LDI NRW informiert über die EDSA Empfehlungen und verspricht, bald weitere Informationen für Verantwortliche bereitzustellen. Der LfD Niedersachsen hat ebenfalls einen Prüfungsplan für Datentransfers veröffentlicht.

Die nationalen Datenschutzaufsichtsbehörden betonen, ebenso wie der EDSA, dass es die Pflicht jedes Datenexporteurs ist, die Angemessenheit des Datenschutzniveaus im Drittland zu überprüfen und diese Prüfung umfassend zu dokumentieren.

Überarbeitete Standardvertragsklauseln

Die Kommission überarbeitet zudem aktuell die Standardvertragsklauseln, die in ihren aktuellen Versionen bereits über 10 bis 19 Jahre alt sind und noch auf der alten Datenschutzrichtlinie fußen, die durch die DSGVO 2018 abgelöst wurde (Entscheidungen 2001/497/EG, 2004/915/EC und 2010/87/EC). Am 12. November 2020 wurden die ersten Texte veröffentlicht, zu diesen kann nun bis zum 10. Dezember 2020 Stellung genommen werden.

Die Überarbeitung dieser Klauseln hilft in der Praxis enorm, wird das Schrems II-Dilemma aber nicht lösen können: Auch überarbeitete Klauseln können als Vertrag nicht bewirken, dass gesetzliche (behördliche) Zugriffsrechte eliminiert würden.

Zu guter Letzt

Auch in den letzten Wochen wurden berichtenswerte Bußgelder und Schadensersatzpflichten verhängt bzw. festgestellt. Im Fokus standen erneut Gesundheitsdaten, aber auch eine zu späte Löschung von Daten. Der Höhe nach springt das Bußgeld gegen die British Airways ins Auge (22 Mio. Euro), die sich darüber indes fast schon freuen könnte – ursprünglich stand ein Bußgeld von über 200 Mio. Euro im Raum.

- **Schadensersatz nach rechtswidrigem Versand von Gesundheitsdaten per Mail**

  1.500 Euro Schadensersatz, da ein Unternehmen zwei Behörden per E-Mail über die „Krankschreibung" eines Mitarbeiters informierte: Diese Information sei bereits ein Gesundheitsdatum, ihr Versand nicht erlaubt – im konkreten Fall bestand keine Pflicht, die Behörden darüber zu informieren (Entscheidung des Arbeitsgerichts Dresden, Urteil vom 26.08.2020, Az. 13 Ca 1046/20).

- **Belgien: Postfachnutzung nach Ausscheiden aus einem Unternehmen**

  Die belgische Datenschutzbehörde hatte sich mit einem Fall zu beschäftigen, bei dem mehrere E-Mail-Adressen von ehemaligen Angestellten trotz ihres Ausscheidens durch ein Unternehmen benutzt wurden – in erster Linie um die

Absender der E-Mails darüber zu informieren, dass der Adressat aus dem Unternehmen ausgeschieden sei. Das konkrete Vorgehen des betroffenen Unternehmens war nach Ansicht der Aufsichtsbehörde unzulässig und wurde mit einem Bußgeld von 15.000 Euro belegt (Verstöße gegen den Grundsatz der Zweckbindung und der Datenminimierung).

Erwartet hätte die Aufsichtsbehörde, dass im Rahmen einer Richtlinie vorgegeben ist, wie mit dem E-Mail-Konto im Fall des Ausscheidens umgegangen wird; jedenfalls müsse ein ausscheidender Mitarbeiter die Möglichkeit haben, seine privaten Nachrichten selbst zu löschen. Nachrichten, die für den weiteren Betrieb des Unternehmens erforderlich sind, seien an einem anderen Ort zu speichern. Sodann müsse der Posteingang mit dem Tag des Ausscheidens gesperrt und eine automatische Nachricht an mögliche Absender programmiert werden, die über das Ausscheiden informiert. Nach Ablauf eines definierten, erforderlichen Zeitraums für die automatische Antwort (idealerweise zwischen einem und drei Monaten) sei der gesamte Posteingang zu löschen.

- **Dänemark: Speicherbegrenzung**

  Die dänische Datenschutzbehörde verhängte ein Bußgeld in Höhe von umgerechnet 148.000 Euro gegen eine Hotelgruppe, weil diese personenbezogene Daten in ihrem System speicherte, obwohl deren Löschfrist seit einiger Zeit – in manchen Fällen sogar mehrere Jahre – überschritten war.

- **Großbritannien: British Airways treffen 22 Mio. Euro anstatt 204 Mio. Euro**

  In Großbritannien wurde gegen British Airways ein Bußgeld in Höhe von 22 Mio. Euro verhängt; ursprünglich standen 204 Mio. Euro im Raum. Die Fluggesellschaft verarbeitete personenbezogene Daten nicht mit angemessener Datensicherheit. Obwohl es BA nach den Feststellungen der Aufsichtsbehörde möglich gewesen wäre, mit verfügbaren Mitteln das Sicherheitsleck zu schließen, sei dies nicht erfolgt. Dies ermöglichte im Jahr 2018 einen Cyberangriff, der erst zwei Monate später entdeckt wurde und bei dem mehr als 400.000 Kundendaten „erbeutet“ wurden – darunter unter

anderem Name, Adresse und Kreditkartennummer inklusive CVV-Nummern.

- **Polen: Bußgeld nach Diebstahl des privaten PCs**

  Einem Mitarbeiter der Universität Warschau wurde ein privater Computer gestohlen, den dieser – ohne Wissen seines Arbeitgebers – auch für dienstliche Zwecke nutzte. Auf dem Computer befanden sich personenbezogene Daten von Studienbewerbern der letzten 5 Jahre.

  In der Ermöglichung des eigenmächtigen Verhaltens des Mitarbeiters, seinen Computer auch für dienstliche Zwecke zu nutzen, sah die Datenschutzbehörde einen Verstoß gegen die Pflicht des Verantwortlichen, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten (Art. 32 DSGVO) zu ergreifen. Insbesondere sei der Datenschutzbeauftragte der Universität nicht in die Planung des Bewerbungsverfahrens einbezogen worden. Zum anderen bemängelte die Behörde, dass die Bewerberdaten der letzten 5 Jahre gespeichert wurden, obwohl die Universität selbst vorsieht, diese Daten nach 3 Monaten zu löschen. In ihren Augen ging dies über das erforderliche Maß hinaus und stellte so einen Verstoß gegen die Speicherbegrenzung dar. Beides ahndete die Behörde mit einem Bußgeld in Höhe von ca. 12.500 Euro.

- **Zypern: Unzureichende technische Vorkehrungen zur Beantwortung von Auskunftsersuchen**

  In Zypern wurde ein Bußgeld in Höhe von 15.000 Euro gegen eine Bank verhängt, weil sie die Vertragsunterlagen ihrer Kunden nicht in der Weise aufbewahrte, die eine Erfüllung von Auskunftsersuchen ihrer Kunden ermöglichte.

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