LOSCHELDER

Newsletter Datenschutzrecht

Januar 2020

Sehr geehrte Damen und Herren,

wir wünschen Ihnen ein frohes neues Jahr und freuen uns, dass wir Sie auch in diesem Jahr wieder über spannende Entwicklungen rund um die Datennutzung und den Datenschutz informieren dürfen. Gleich zu Beginn unseres Newsletters möchten wir Sie auf die nächste Veranstaltung unseres Forums Digitalisierung hinweisen:

Compliance & Krisenmanagement: 12.02.2020,
16.00 Uhr – 18.00 Uhr

Diesmal geht es um neue Herausforderungen und Chancen in der digitalen Welt bei Compliance und Krisenmanagement. Wir würden uns sehr freuen, Sie dort begrüßen zu können!

Weitere Informationen dazu und die **Möglichkeit zur Anmeldung** finden Sie auf unserer Homepage.

In unserem ersten Newsletter des neuen Jahres geht es um Steuerberater, Standardvertragsklauseln, das viel besprochene berechtigte Interesse und das Resumée der Datenschutzaufsichtsbehörden zur DSGVO. Zudem eröffnen wir eine neue Rubrik: „Geldbußen und Kuriositäten des Monats“ – damit Sie „zu guter Letzt“ etwas zum Schmunzeln und für Ihre Risikoentscheidung finden.

Inhalt

Erfahrungsbericht der Aufsichtsbehörden

Ende 2019 veröffentlichten die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ihren Erfahrungsbericht zur DSGVO. Der Bericht lässt erkennen, dass die DSK häufige Unsicherheiten und den Compliance-Aufwand in der Praxis durchaus anerkennt. Die Änderungsvorschläge würden aber, was wenig überraschend ist, in erster Linie zu Verschärfungen der Rechtslage und zu weitergehenden Eingriffsmöglichkeiten der Aufsichtsbehörden führen. Bislang sind die Änderungsvorschläge nur Empfehlungen und es ist nicht abzusehen, ob der EU-Gesetzgeber diesen folgen wird. Bereits jetzt aber liefern die Befunde und Vorschläge der Behörden Anhaltspunkte dafür, in welche Richtung die Behörden mögliche Auslegungsspielräume zukünftig nutzen könnten und wo ihre Schwerpunkte liegen. In diesem Beitrag möchten wir Ihnen eine kleine Auswahl der interessanten Passagen vorstellen.

In ihrem Erfahrungsbericht setzen die Aufsichtsbehörden den ersten Schwerpunkt unter die Überschrift „Alltagserleichterung & Praxisdeutlichkeit". Sie sehen in drei Punkten Handlungsbedarf. Namentlich bei den **Informationspflichten**, dem Recht auf Kopie und der Pflicht zur **Meldung von Datenschutzbeauftragten**.

Die DSK fordert Erleichterungen bei den Informationspflichten. Unter bestimmten Voraussetzungen soll es ausreichen, die Informationen auf Verlangen des Betroffenen auszuhändigen. Bereits jetzt sieht die DSK die Möglichkeit für Verantwortliche, die Informationspflichten durch ein gestuftes Verfahren zu erfüllen, mit einer verkürzten Information auf erster Ebene und erst nachgelagert der umfassenden Information (der Bericht verweist unmittelbar auf den „Mehrebenen-Ansatz" der Artikel 29-Gruppe WP 260, Rn. 35). Insbesondere beim mündlichen oder telefonischen Kontakt sei es lebensfremd zu erwarten, dass Betroffene sofort eine umfangreiche Information erhalten. In geeigneten Fällen könnten die notwendigen Informationen auch durch einen Aushang oder mit der Übersendung der Auftragsbestätigung erteilt werden. Beim Recht auf Kopie sieht die Behörde auch Handlungsbedarf, legt sich aber nicht mit einem Vorschlag fest. Die Aufsichtsbehörden sehen ein Problem darin, wie auch viele betroffene Unternehmen in der Praxis, dass der Umfang des Auskunftsrechts unklar ist. Teilweise verlangten Betroffene ohne nähere Konkretisierung die Herausgabe aller beim Verantwortlichen vorhandenen Dokumente. Des Weiteren halten die Aufsichtsbehörden die Pflicht zur **Meldung von Datenschutz-**

beauftragten bei der Aufsichtsbehörde (Art. 37 Abs. 7 DSGVO) für überflüssig. Eine Veröffentlichungspflicht genüge.

Einen weiteren Schwerpunkt legt der Bericht auf die „**Datenpannenmeldung**". Das Papier lässt deutlich erkennen, dass die Aufsichtsbehörden der Ansicht sind, dass zu viele Datenpannen gemeldet würden – dies indes hat seinen Grund in dem sehr weiten Anwendungsbereich der Meldepflicht aus Art. 33 DSGVO. Nach Ansicht der Aufsichtsbehörden sollte nicht bereits bei der Wahrscheinlichkeit einer Verletzung des Schutzes personenbezogener Daten eine Meldepflicht bestehen, sondern erst dann, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen gegeben ist.

Interessant ist auch, dass die DSK eine **Herstellerverantwortlichkeit** fordert. Nach aktuellem Recht ist nur derjenige Verantwortlicher, der personenbezogene Daten verantwortlich verarbeitet, nicht aber der Hersteller der dazu eingesetzten Hard- und Software. Die Grundsätze *Data Protection by Design* und *Data Protection by Default* liefen ins Leere, wenn sie sich – wie gegenwärtig – nur an den Verantwortlichen richten, der das Hard- und Softwareprodukt nur einsetzt, aber nicht herstellt. Mit einer Herstellerpflicht könnte der Datenschutzstandard zudem beim Einsatz der Produkte im privaten Bereich erhöht werden; es fehlt in diesem Bereich nach dem aktuellen Recht nämlich an einem Verantwortlichen im Sinne der DSGVO, die damit nicht anwendbar ist.

Zudem fordert die DSK weitergehende **Verwarnungsmöglichkeiten**. Auch Verstöße, die von den Datenverarbeitungsgrundsätzen unabhängig sind (Art. 5 DSGVO), möchte die DSK verwarnen dürfen. Des Weiteren fordern die Aufsichtsbehörden, Auskunftsverweigerung und fehlende Informationsbereitstellungen, wie nicht befolgte Anweisungen gemäß Art. 83 Abs. 5 lit. e DSGVO, mit einem Bußgeld ahnden zu dürfen.

Auch die Äußerungen der DSK zur **Direktwerbung** sind interessant. Der Erfahrungsbericht verweist darauf, dass die Traditionen bei der Direktwerbung in den Mitgliedstaaten erheblich variieren. Mit der DSGVO seien viele nationale Vorschriften, die nach alter Rechtslage die entgegenstehenden Interessen gewichtet hätten, weggefallen. Der Gesetzgeber solle auch in die DSGVO eine Gewichtungsmöglichkeit aufnehmen.

Einen ganzen Schwerpunkt widmete die DSK außerdem dem **Profiling**. Dieses sei in der DSGVO zwar definiert, das Profiling an sich aber nicht geregelt. Sie fordern eine Regelung und Verschärfung des Rechtsrahmens, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen. Die betroffenen Personen sollen von einem größeren Maß an Transparenz über erstellte Profile profitieren und zugleich eine größere Kontrolle über die Verarbeitung ihrer Daten zur Profilbildung erhalten.

Es bleibt spannend, ob und mit welcher Zielrichtung die Änderungsvorschläge auf EU-Ebene aufgegriffen werden und inwieweit die Aufsichtsbehörden offene Auslegungsspielräume zukünftig nutzen werden, um ihre Standpunkte durchzusetzen.

(Vorläufige) Ruhe für den Drittstaatentransfer (in die USA)?

Im Dezember 2019 hat der Generalanwalt am EuGH seine Schlussanträge in der Rechtssache „Schrems II" (C-311/18) veröffentlicht. Nach seiner Ansicht sind die Standardvertragsklauseln rechtmäßig. Zweifel kündigt er indes an dem EU-US-Privacy Shield an. Was dies für den Drittstaatentransfer insbesondere in die USA bedeutet, erklären wir.

Der irische High Court hatte im Mai 2018 die von der Europäischen Kommission verfassten Standardvertragsklauseln für die Übermittlung personenbezogener Daten im Ausland (2010/87/EU-Kom;

Standard Contractural Clauses = „SCC“) dem EuGH zur Überprüfung vorgelegt. Werden personenbezogene Daten in einen Drittstaat außerhalb des EWR übermittelt, müssen neben den üblichen datenschutzrechtlichen Anforderungen geeignete Garantien geschaffen werden, die ein hinreichendes Datenschutzniveau auch im Drittstaat absichern. Die DSGVO erlaubt eine Datenverarbeitung nämlich nur dort, wo ein angemessenes Datenschutzniveau herrscht. Eine praktikable Möglichkeit hierfür ist der Abschluss von SCC, welche die datenempfangende Stelle zur Einhaltung konkreter datenschützender Maßnahmen verpflichten.

Nach Ansicht des Generalanwalts sind die SCC rechtmäßig und können damit auch künftig einen Datentransfer außerhalb des EWR tragen. Nach Ansicht des Generalanwalts entbindet der Abschluss von SCC indes nicht von einer Überprüfung: Gegebenenfalls müsse das datenexportierende Unternehmen die Datenübertragung aussetzen, wenn sich offenbart, dass die Standardvertragsklauseln nicht mehr eingehalten werden (z. B. Kollision von Pflichten gegenüber den nationalen Sicherheitsbehörden und dem Vertragspartner in Europa).

Besondere Brisanz hat das Verfahren für den Datentransfer in die USA. Denn der EuGH könnte dieses Verfahren aufgrund des zugrundeliegenden Sachverhalts auch zum Anlass nehmen, sich zum „EU-US-Privacy-Shield“ zu äußern. Der Generalanwalt riet davon zwar ab, äußerte aber vorsorglich seine Bedenken gegen das „EU-US-Privacy Shield“. Insofern ist offen, ob bzw. wie lange dieses den Datentransfer in die USA noch trägt – bis zu einer anderslautenden Entscheidung des EuGH ist dies aber der Fall und sowohl SCC als auch EU-US-Privacy Shield sind weiterhin gültig.

Zum Hintergrund: Dass nun der EuGH über die SCC entscheiden muss, geht auf eine Beschwerde des bekannten Datenschutzaktivisten Maximilian Schrems zurück. Auch in diesem Verfahren geht es wieder (siehe Schrems I) um datenschutzrechtliche Fragen im Zusammenhang mit Facebook, der Übertragung von personenbezogenen Daten in die USA und die Rolle der amerikanischen Geheimdienste. Er legte Beschwerde bei der irischen Datenschutzbehörde (Data Protection Commission- DPC) ein und forderte sie auf, Facebook Ireland die Übertragung seiner personenbezogenen Daten an das amerikanische Mutterunternehmen unter Anwendung des Art. 4 Abs. 1 lit. a) SCC zu untersagen. Schrems sieht in der (fortbestehenden) Möglichkeit nationaler amerikanischer Nachrichtendienste,

Unternehmen wie Facebook zur Herausgabe von personenbezogenen Daten zu verpflichten, eine Verletzung unionsrechtlicher Grundrechte. Dem Unternehmen sei es nicht möglich, die mit der europäischen Tochter nach den SCC vereinbarten Datenschutzstandards zu gewährleisten. Deshalb habe die DPC die Übertragung der Daten zu untersagen. Daraufhin leitete die DPC beim High Court ein Verfahren ein, um die Gültigkeit des Beschlusses 2010/87 durch Vorlage an den EuGH überprüfen zu lassen. Die abschließende Antwort des EuGH steht noch aus, aber die oftmals wegweisenden Schlussanträge des Generalanwalts liegen nun vor:

Nach seiner Ansicht ist maßgeblich, dass die effektive Einhaltung der durch die Standardvertragsklauseln zwischen den Vertragsparteien vereinbarten Verarbeitungsgrundsätze - und damit des Datenschutzniveaus - gewährleistet werde. Dies sei primär Aufgabe der beteiligten Unternehmen. Falls das Unternehmen dieser Aufgabe nicht (ausreichend) nachkommt, sei es die aus der DSGVO vermittelte Plicht der nationalen Datenschutzbehörden, entsprechende Maßnahmen zur Durchsetzung der Standardvertragsklausel und damit zum Schutz der personenbezogenen Daten zu ergreifen. Insbesondere für den Fall einer Kollision von Pflichten aus den Standardvertragsklauseln und den durch das Recht des Drittbestimmungslandes auferlegten Pflichten (z. B. gegenüber den nationalen Sicherheitsbehörden und dem Vertragspartner in Europa) müssen die nationalen Aufsichtsbehörden eine Übermittlung aussetzen oder verbieten können.

Bis zu einer anderslautenden Entscheidung des EuGH ist davon auszugehen, dass die SCC wirksam sind. Unternehmen können sich also bei der Datenübermittlung wie bisher auf ihre Gültigkeit verlassen. In der Behördenpraxis wird es möglicherweise zur erhöhten Kontrolle der Geltung von SCC durch nationale Datenschutzbehörden kommen. Von einer unterschiedlichen „Durchsetzungsdichte“ nationaler Datenschutzbehörden ist dabei auszugehen (so auch die DPC).

Steuerberater sind keine Auftragsverarbeiter?!

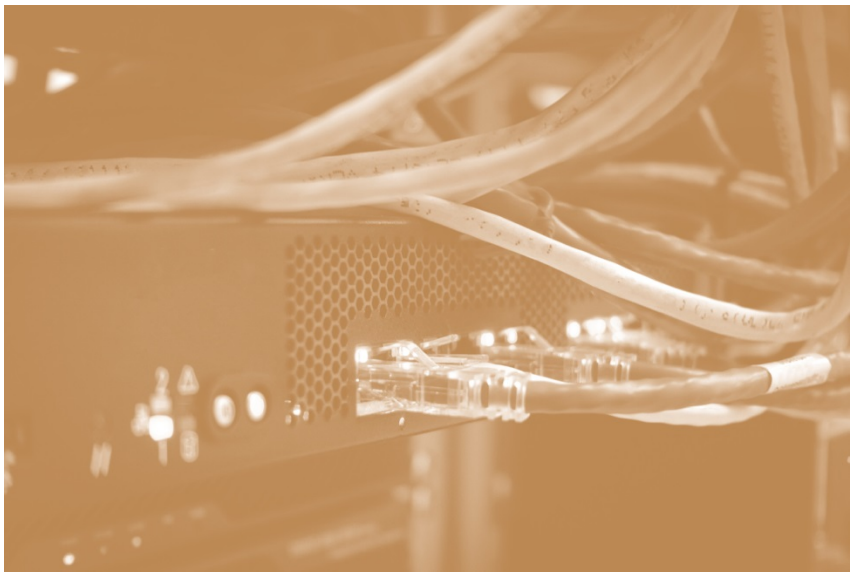
Der deutsche Gesetzgeber hat (für sich) entschieden, dass Steuerberater keine Auftragsverarbeiter sind und dies in § 11 des Steuerberatungsgesetzes (StBerG) festgehalten; die Änderung trat am 18.12.2019 in Kraft. Danach verarbeiten Steuerberater im Rahmen ihrer Tätigkeit personenbezogene Daten stets als Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO und nicht als Auftragsverarbeiter. Gelten soll dies für sämtliche Tätigkeiten des Steuerberaters.

Auch das „Buchen laufender Geschäftsvorfälle“, die „laufende Lohnabrechnung“ und das „Fertigen der Lohnsteuer-Anmeldungen“ sind laut der Gesetzesbegründung Tätigkeiten, die von der Steuerberatung umfasst sind (vgl. BT-Drs. 19/14909, S. 58). Das bedeutet, dass selbst die Leistung des mit der Lohnbuchführung beauftragten Steuerberaters keine Auftragsverarbeitung i.S.d. Art. 28 DSGVO (mehr) darstellt und ein Auftragsverarbeitungsvertrag mit dem Mandanten nicht erforderlich ist.

Die Gesetzesänderung gründet auf dem Verständnis, dass Steuerberater freiberuflich tätig sind und damit ihre Tätigkeit weisungsfrei und eigenverantwortlich ausüben; dies sei unabhängig davon, welche Art der „Hilfe in Steuersachen“ ausgeführt wird (vgl. § 1 StBerG). Eine solche *„unabhängige(...), eigenverantwortliche(…), gewissenhafte(…) und verschwiegene(…) Berufsausübung“* sei mit einer

fremden Zweckbestimmung, wie sie im Rahmen der Auftragsverarbeitung erfolgt, nicht vereinbar (vgl. BT-Drs. 19/14909, S. 58).

Unumstritten ist diese nationale Regelung indes nicht. Verschiedene Aufsichtsbehörden vertraten bisher die Ansicht, dass ein Steuerberater bei manchen Tätigkeiten als Auftragsverarbeiter i.S.d. Art. 28 DSGVO tätig würde. Für die Einstufung sollte es darauf ankommen, ob die in Frage stehende Tätigkeit des Steuerberaters klar umrissenen und ausführlichen Weisungen unterliege, sodass z.B. Datenverarbeitungen im Rahmen von Lohnbuchführungen, als Auftragsverarbeitung einzuordnen seien. Auch bisher lehnten andere diese Auffassung bereits mit der Begründung ab, ein solches Verständnis wiederspreche den berufsrechtlichen Pflichten des Steuerberaters als Berufsgeheimnisträger. Entscheiden kann der deutsche Gesetzgeber diese Frage aufgrund des Anwendungsvorrangs des EU-Rechts nicht. Entscheidend bleibt nach der vorrangig anzuwendenden DSGVO, wer *tatsächlich* die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt. Dies dürfte vorerst indes angesichts der nationalen Gesetzesregelung eine eher akademische Diskussion sein, solange keine anderweitige Gerichtsentscheidung vorliegt: Insbesondere die Bußgeldrisiken sind gering, bis ein (EU-) Gericht die nationale Regelung für unanwendbar erklärt hat. Grundsätzlich darf auf eine solche gesetzgeberische Regelung, wie den § 11 Abs. 2 S. 2 StBerG, vertraut werden.



Überwiegendes berechtigtes Interesse: neuer Input vom EuGH

Das „überwiegende berechtigte Interesse" ist datenschutzrechtliche Wunderwaffe und Risikofaktor zugleich: Der Erlaubnistatbestand eignet sich aufgrund seines offenen Wortlautes dazu, die unterschiedlichsten Maßnahmen zu erlauben. Gleichzeitig beinhalten derartige Bewertungen immer ein gewisses Maß an Rechtsunsicherheit, da es an eindeutigen Maßstäben ebenso fehlt, wie an einer hinreichend umfangreichen und verlässlichen Fallpraxis. In seinem Urteil vom 11. Dezember 2019 (Az. C-708/18) äußerte sich nun der EuGH zur Auslegung des Erlaubnistatbestandes des „überwiegenden berechtigten Interesses" (Art. 6 Abs. 1 lit. f DSGVO). Mit diesem Urteil nimmt der sehr offene Erlaubnistatbestand weiter Kontur an und seine Anwendung in der Praxis wird rechtssicherer.

Der EuGH bestätigte in seinem Urteil viele der Kriterien, die sich auch in der bisherigen Diskussion, u.a. zur Videoüberwachung im Konkreten und der Auslegung des überwiegenden berechtigten Interesses im Allgemeinen, wiederfinden. Anlass des Urteils war die Vorlage eines rumänischen Gerichtes, das den EuGH zur EU-rechtlichen Prüfung eines nationalen Gesetzes bat, welches die Anforderungen, unter denen eine Videoüberwachung zulässig ist, im Einzelnen regelt. Das Urteil erging zwar zu Art. 7 lit. f der Richtlinie 95/46 („Datenschutzrichtlinie"), die Aussagen können jedoch auf die Auslegung des fast wortgleichen Art. 6 Abs. 1 lit. f DSGVO übertragen werden:

I. Vorhandenes berechtigtes Interesse

Die Prüfung des Erlaubnistatbestandes beginnt stets mit dem „berechtigten Interesse". Nur wie konkret muss dieses sein? Der EuGH verlangt, dass das Interesse zum Zeitpunkt der Verarbeitung bereits entstanden und vorhanden, nicht bloß hypothetisch und rein abstrakt ist. Gleichzeit muss es nicht schon zu einer Beeinträchtigung des Interesses gekommen sein. Mit anderen Worten: Eine Videoüberwachung aus Sicherheitsgründen ist beispielsweise auch schon zulässig, wenn es noch keinen Einbruch und auch keinen Einbruchsversuch gegeben hat, aber ein Risiko bzw. eine Gefahr besteht. Der EuGH ist damit großzügiger als das BVerwG; wir berichteten dazu in unserem April Newsletter des letzten Jahres. Nach Ansicht des BVerwG ist die Videoüberwachung zur Verhinderung

von Straftaten nur berechtigt, wenn eine erheblich über das allgemeine Lebensrisiko hinausgehende Gefährdungslage besteht.

II. Erforderlichkeit

Zur zweiten Voraussetzung, der Erforderlichkeit der Verarbeitung der personenbezogenen Daten für die Verwirklichung des berechtigten Interesses, hat der EuGH sich auch geäußert. Hierzu führte er aus, dass sich Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten und die Achtung des Privat- und Familienlebens auf das absolut Notwendige beschränken müssen. Es sei deshalb stets zu prüfen, ob das berechtigte Interesse nicht mit anderen Mitteln, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere die in den Art. 7 und 8 der Charta verbürgten Rechte auf Achtung des Privatlebens und Schutz personenbezogener Daten, eingreifen, *vernünftigerweise* ebenso wirksam erreicht werden kann. Zudem sei die Voraussetzung der Erforderlichkeit der Datenverarbeitung gemeinsam mit dem sogenannten Grundsatz der „Datenminimierung" zu prüfen, der verlangt, dass die personenbezogenen Daten dem Zweck angemessen und erheblich sind sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

III. Abwägung

Hinsichtlich der schließlich in jedem Einzelfall notwendigen Abwägung des berechtigten Interesses mit den Interessen der Betroffenen bestätigte der EuGH, dass in die Abwägung die unterschiedlich schwere Beeinträchtigung der Grundrechte der betroffenen Person und die öffentliche Zugänglichkeit der Daten einbezogen werden dürfen. Des Weiteren müsse der Art der in Rede stehenden personenbezogenen Daten, der konkreten Modalitäten ihrer Verarbeitung, die Zahl der Personen, die Zugang zu diesen Daten haben, sowie den Zugangsmodalitäten Rechnung getragen werden. Auch seien die berechtigten Erwartungen der betroffenen Person, dass ihre personenbezogenen Daten nicht verarbeitet werden, zu berücksichtigen, wenn diese Person unter den konkreten Umständen vernünftigerweise nicht mit einer Weiterverarbeitung der Daten rechnen kann (dazu nunmehr Erwägungsgrund 47 DSGVO).

Für die Videoüberwachung heißt das nach Ansicht des EuGH, dass alternative Maßnahmen geprüft werden müssen, wie zum Beispiel in Form eines am Gebäudeeingang installierten Sicherungssystems

mit Gegensprechanlage und Magnetkarte. Der Verantwortliche muss zudem prüfen, ob es ausreicht, wenn die Videoüberwachung nur in der Nacht oder außerhalb der normalen Arbeitszeit in Betrieb ist. Bilder, die in Bereichen aufgezeichnet wurden, in denen die Überwachung nicht erforderlich ist, müssen blockiert oder unscharf eingestellt werden.

Zu guter Letzt: Geldbußen und Kuriositäten des Monats

Diesen Monat starten wir unsere neue Rubrik: „Zu guter Letzt". Darin möchten wir Ihnen neben skurrilen und abseitigen Datenschutzthemen auch eine Auswahl bemerkenswerter Bußgelder vorstellen. So sind Sie besser informiert, als die Europäische Kommission, die laut Spiegel-Schlagzeile „keinen Überblick über Bußgelder" hat. So viel vorab: Teuer wurde es diesen Monat wieder für Verantwortliche, die sensible Daten (angeblich) unter Verstoß gegen die DSGVO verarbeiten…

- **Rheinland-Pfalz**

Dass insbesondere strukturelle Versäumnisse im Unternehmen hohe Geldbußen zur Folge haben können, zeigt das Bußgeld der rheinland-pfälzischen Datenschutzbehörde gegen ein Krankenhaus in Höhe von 105.000 Euro. Die Geldbuße beruht auf mehreren Verstößen gegen die DSGVO, die im Zusammenhang mit einer Patientenverwechslung entdeckt wurden. Die Patientenverwechslung hatte eine falsche Rechnungsstellung zur Folge und offenbarte strukturelle technische und organisatorische Defizite des Krankenhauses beim Patientenmanagement. Es kann davon ausgegangen werden,

dass das Bußgeld noch höher ausgefallen wäre, hätte das Krankenhaus nicht, wie der LfDI RLP in seiner Pressemitteilung schreibt, belastbar seine Bemühungen vorgetragen, die Fortentwicklung und Verbesserung des Datenschutzmanagements nachhaltig voranzutreiben.

- **Belgien**

Wegen des Einsatzes von Google Analytics ohne Einwilligung wurde in Belgien gegen den Betreiber der Website jubel.be ein Bußgeld in Höhe von 15.000 Euro verhängt. Details, wie Google Analytics eingestellt war (etwa mit oder ohne Anonymisierung der IP-Adresse, unter Vergabe einer UserID etc.), sind nicht verfügbar.

- **Norwegen**

Die norwegische Datenschutzbehörde hat gegen die Stadt Oslo eine Geldbuße in Höhe von 49.300 Euro verhängt, weil die Stadt von 2007 bis November 2018 Patientendaten in den städtischen Pflegeeinrichtungen außerhalb des elektronischen Patientenakten-Systems in sog. Arbeitsblättern gespeichert hatte. Diese Arbeitsblätter enthielten Informationen zu den Bewohnern, u.a. zu ihren täglichen Bedürfnissen und Pflegeroutinen, die unproblematisch den entsprechenden Personen zugeordnet und bis zum Verlassen des Bewohners nicht nur von Pflegepersonal, sondern auch von Externen wie z.B. Reinigungspersonal eingesehen werden konnten.

- **England**

In England hat das Information Commissioner's Office (ICO) eine in London ansässige Apotheke anlässlich mangelhafter Sicherheitsvorkehrungen beim Umgang mit besonderen Kategorien von personenbezogenen Daten mit einer Geldbuße von 275.000 GBP belegt. Die Doorstep Dsipensaree Ltd lagerte ca. 500.000 Dokumente, die personenbezogene Daten wie Namen, Anschriften, Geburtsdaten, NHS-Nummern und medizinische Informationen und Rezepte enthielten, in unverschlossenen Behältern auf der Rückseite des Firmengeländes. Dort waren die auf Daten zwischen Juni 2016 und Juni 2018 datierten Dokumente nicht angemessen gegen unbefugten Zugriff und versehentlichen Verlust bzw. Zerstörung geschützt und dem Einfluss der Witterung ausgesetzt.

- **Schweden**

Die schwedische Datenschutzbehörde hat im Dezember 2019 eine Geldbuße in Höhe von 35.000 Euro gegen das Unternehmen Nusvar wegen Verstoßes gegen die DSGVO und das schwedische

Kreditinformationsgesetz verhängt. Das Unternehmen soll beim Betrieb seiner Website Mrkoll.se, auf der Kreditinformationen aller Schweden, die älter als 16 Jahre sind, veröffentlicht werden, gegen das Kreditinformationsgesetz, sowie gegen darin enthaltene Verweisungen in die DSGVO verstoßen haben. Ein Großteil der Datenverarbeitungen des Unternehmens sei zwar von einem sog. Veröffentlichungszertifikat erfasst; die DSGVO findet auf diese keine Anwendung. Allerdings sei die Veröffentlichung von Informationen, wie dass keine Zahlungsausfälle gemeldet wurden oder eine Person bereits strafrechtlich verurteilt wurde, eine Verarbeitung von Kreditinformationen, die wegen des Zertifikats zwar keiner vorherigen Genehmigung der Datenschutzbehörden bedürfe, aber dem Kreditinformationsgesetz und der dortigen Verweisung auf die DSGVO unterfällt. Gegen die Vorschriften des Kreditinformationsgesetzes habe der Betreiber bei der Veröffentlichung verstoßen.

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

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

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

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

Impressum

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

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