LOSCHELDER

Newsletter Datenschutzrecht

August 2020

Sehr geehrte Damen und Herren,

nicht nur wegen der Temperaturen ist es für Datenschützer ein heißer Sommer. Neben den andauernden besonderen Arbeitssituationen rund um Homeoffice und Videokonferenzen sowie Fragen der Zutrittskontrolle und Befragung der Belegschaft nach Urlaubsaufenthalten hat der EuGH kürzlich für einen abermaligen Paukenschlag gesorgt, indem er das zwischen der EU und den USA bestehende Privacy Shield Abkommen gekippt hat. Der transatlantische Datenverkehr ist damit mehr denn je mit großen Fragezeichen versehen. In unserem Sondernewsletter hatten wir sie bereits darüber informiert. Unser erster Beitrag greift das Thema nochmals auf.

In unserem zweiten Beitrag widmen wir uns der praxisrelevanten Frage, ob Datenschutzbeauftragte in Kurzarbeit geschickt werden dürfen.

Unser dritter Beitrag befasst sich mit personenbezogenen Angaben in Restaurants und Betrieben zum Zwecke der Coronaprävention.

Und zu guter Letzt haben wir auch in diesem Monat einige spannende Bußgeldfälle für Sie zusammengetragen.

Inhalt

Datentransfer in die USA – „Klappe die 2."

Der EuGH hat am 16.07.2020 das EU-U.S.-Privacy Shield für ungültig erklärt und für die Verwendung der Standardvertragsklauseln eine Einzelfallprüfung vorgeschrieben. Wir haben darüber schon kurz nach Veröffentlichung des Urteils informiert. Inzwischen haben sich auch einige Aufsichtsbehörden positioniert und ihre Erwartungen an die Unternehmen konkretisiert. Und am 10.08.2020 haben die EU-Kommission und die USA Gespräche aufgenommen. Was danach jetzt zu tun ist, fassen wir hier zusammen.

Zur Erinnerung: Wenn personenbezogene Daten verarbeitet werden, benötigt der dafür Verantwortliche eine Erlaubnisgrundlage. Werden diese Daten dabei in ein Drittland außerhalb des EWR übermittelt, ist außerdem, zusätzlich, auf zweiter Stufe, noch eine Absicherung des Datenschutzniveaus im Drittland erforderlich. Das kann etwa ein Angemessenheitsbeschluss der Kommission sein, wie das EU-U.S.-Privacy Shield einer war, oder eben der Abschluss von sog. Standardvertragsklauseln, die von der Kommission herausgegeben werden. Ein Transfer von Daten in ein Drittland geschieht meist durch Nutzung von Online-Tools wie Cloud-Lösungen, CRM-Systemen, Analysetools o.ä., wenn die Anbieter Server außerhalb des EWR nutzen. Prominente Beispiele sind Facebook, Google, Salesforce, Microsoft, AWS u.v.m.

Das EuGH-Urteil hat nun enorme Auswirkungen auf die Absicherung auf zweiter Stufe für den Datentransfer in die USA, aber auch für alle anderen Drittstaaten, wenn der Datentransfer dorthin über Standardvertragsklauseln oder sog. Binding Corporate Rules abgesichert ist.

Auch unter Berücksichtigung der Positionierungen der Aufsichtsbehörden ist es daher aktuell dringend notwendig, aktiv zu werden, wie wir dies in unserer Sonderausgabe des Newsletters dargestellt haben:

1. Datenflüsse überprüfen: Wo werden personenbezogene Daten in ein Drittland übermittelt?

2. Alternative Garantien schaffen: Wie wird bei den identifizierten Drittlandübermittlungen ein angemessenes Datenschutzniveau im Zielland abgesichert?

- EU-U.S.-Privacy Shield: Da dieses nun ungültig ist, muss eine andere Lösung gefunden werden.

- Standardvertragsklauseln, Binding Corporate Rules: Hier muss jetzt noch ergänzend im Einzelfall geprüft werden, ob die Vertragspartner im Drittland die Vertragsklauseln auch wirklich einhalten können. Dies kann im ersten Schritt durch eine konkrete Anfrage mit spezifischen Fragen zu Zugriffsrechten von Geheimdienstbehörden u.ä. geschehen. Kritisch ist dies gerade für die USA, da überaus fraglich ist, ob durch vertragliche Regelungen ausgeschlossen werden kann, dass US-Geheimdienste die Daten gemäß den US-Gesetzen einsehen.

- Denkbar sind auch andere Stützen, etwa Einwilligungen in besonderen Fällen oder die Vertragserfüllung; die jeweiligen in Art. 49 DSGVO gelisteten Optionen sollten stets im Einzelfall geprüft werden.

3. Dokumentieren und Datenschutzerklärung anpassen: Ergriffene Schritte sind zu dokumentieren, die Betroffeneninformationen (insbesondere auch die Datenschutzerklärungen auf den Websites und in Apps) anzupassen.

4. Notfalls: Behörde informieren / Datentransfer beenden: Kann das Datenschutzniveau im Drittland nicht abgesichert werden, ist der Datentransfer zu stoppen oder – bei Fortsetzung – die Behörde zu informieren.

Von Seiten der Aufsichtsbehörden wird kommuniziert, dass diese Prüfung und Entscheidung über das weitere Vorgehen – je nach Bundesland – „sofort“ oder jedenfalls „unverzüglich“ zu erfolgen hat. Zu empfehlen ist in jedem Fall, so zeitnah wie möglich die Überprüfung zu beginnen und zu dokumentieren.

Eine umfassende Übersicht über die Folgen des EuGH-Urteils aus Sicht der Europäischen Aufsichtsbehörden bietet der FAQ des EDSA. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Lände stellt in einer Pressemitteilung ausdrücklich klar, dass sie die

Positionierung des EDSA befürwortet. Konkret für Schritt 2 gilt es danach zu beachten:

- Standardvertragsklauseln sind weiterhin wirksam und können einen Drittstaatentransfer grundsätzlich absichern.

- Eine Einzelfallprüfung ist aber zwingend durchzuführen, ob im konkreten Fall die Vertragsklauseln auch eingehalten werden (können). Dies kann über Abfragen beim Vertragspartner nebst Überprüfung der Antworten erfolgen oder auch durch eine Begutachtung der Rechtslage im betroffenen Drittstaat.

- Fällt die Einzelfallprüfung negativ aus und stehen keine anderen Instrumente zur Verfügung (etwa kein Angemessenheitsbeschluss, kein Fall des Art. 49 DSGVO), muss der Datentransfer beendet oder die Aufsichtsbehörde informiert werden.

Einige der großen US-Anbieter sind auch selbst schon aktiv geworden. Google etwa hat Standardvertragsklauseln auf die meisten seiner Produkte ausgeweitet und verspricht in den AGB zusätzlich, diese auch einzuhalten. Dieses Versprechen klingt prima facie angesichts des geltenden US-Rechts nur bedingt überzeugend. Facebook hat neue Bedingungen für Business-Lösungen veröffentlicht, die überraschenderweise nach wie vor auf das EU-U.S.-Privacy Shield verweisen. Insgesamt ist hier aktuell viel im Fluss und eine abschließende Bewertung kaum möglich. Wichtig daher: Prüfen Sie Drittstaatentransfers und werden Sie so dokumentiert aktiv!

Kurzarbeit für interne Datenschutzbeauftragte?

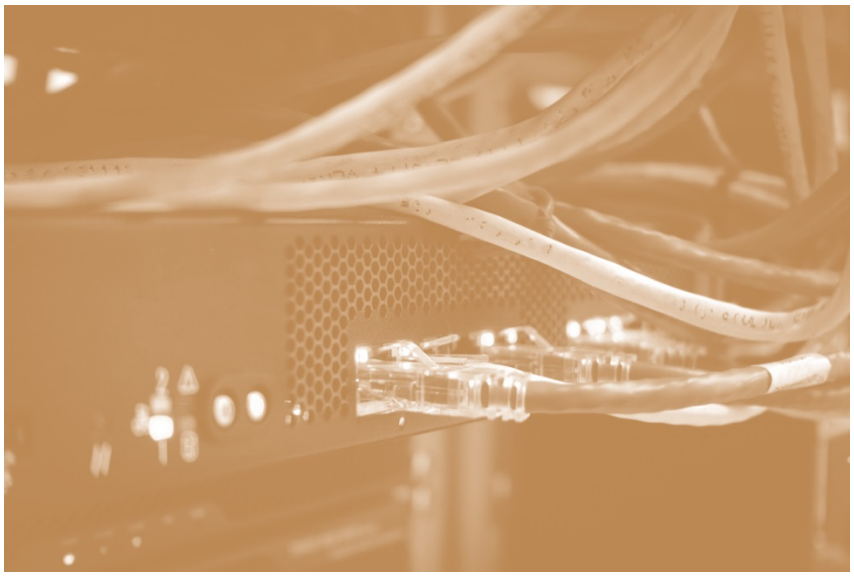
Die Coronakrise hat zahlreiche Unternehmen gezwungen, die Belegschaft ganz oder teilweise in Kurzarbeit zu schicken. Das galt und gilt zum Teil auch für interne Datenschutzbeauftragte und deren Mitarbeiter bzw. Vertreter. Die LDI NRW befasst sich in einer aktuellen Kurzmitteilung mit diesem Thema.

Die DSGVO formuliert keine festen Arbeitszeitkontingente für den Datenschutzbeauftragten. Es heißt in Art. 38 Abs. 2 DSGVO nur, dass der Datenschutzbeauftragte zur Erfüllung seiner Aufgaben über die *„erforderlichen Ressourcen“* verfügen muss. Das kann je nach Größe des Unternehmens und Komplexität und Sensibilität der Datenverarbeitungsvorgänge stark variieren und kann eine Teilzeitbeschäftigung bedeuten, aber auch den Einsatz eines mehrköpfigen Datenschutzteams umfassen. Unternehmen müssen daher stets – auch außerhalb von Krisenzeiten – dokumentiert bestimmen, welcher Arbeitsaufwand notwendig ist, um die Aufgaben des Datenschutzbeauftragten in der konkreten Situation erfüllen zu können.

In der noch andauernden Coronakrise bzw. im Zuge einer „2. Welle“ muss differenziert werden: Einerseits führen der Einsatz von Home-Office, Videokonferenzlösungen etc. zu einer Vielzahl von datenschutzrechtlichen Fragestellungen, die es zu klären gilt, andererseits mag das Tagesgeschäft und die laufenden

datenschutzrechtlichen Themen und Einzelanfragen zurückgehen. Gleichzeitig können Datenschutzbeauftragte die so frei gewordene Zeit nutzen, um das Verarbeitungsverzeichnis zu pflegen oder sonstige Arbeiten zu erledigen, die im hektischen Tagesgeschäft bisher keine Berücksichtigung finden konnten. Hier haben Unternehmen einen angemessenen Ausgleich zu finden, die LDI NRW weist darauf hin, dass das Arbeitsfeld der oder des Datenschutzbeauftragten keinesfalls vollständig „brach liegen" darf, da eine wirkungsvolle Überwachung des Datenschutzes auch in Krisenzeiten notwendig ist.

Unternehmen müssen hier eine bewusste und dokumentierte Entscheidung treffen. Eine praktische Lösung beinhaltet jedenfalls immer eine wirkungsvolle Vertretungslösung, wenn der Datenschutzbeauftragte einen oder mehrere Tage nicht im Betrieb anwesend ist.



Personenangaben in Gaststätten/Betrieben

Wer heutzutage ein Restaurant oder ggf. einen fremden Betrieb oder Büro als Besucher aufsucht, muss seine Kontaktdaten angeben. Dies gilt in den meisten Bundesländern seit Beginn der Lockerung der Corona-Maßnahmen. Dabei stellt sich natürlich schnell die Frage nach dem Datenschutz.

So auch in einem Eilverfahren vor dem VGH Baden-Württemberg (VGH Baden-Württemberg, Beschluss vom 25.06.2020, 1 S 1739/20).

Die Klägerin, die regelmäßig geschäftlich Restaurants aufsucht, sah sich durch die Verpflichtung, ihre Kontaktdaten anzugeben, nicht nur in ihrem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) verletzt, sondern meinte auch einen Verstoß gegen die DSGVO zu erkennen. Namentlich ging sie davon aus, ihr Name und Adresse lasse Rückschlüsse auf ihre „ethnische Herkunft und Rasse“ zu. Damit wären diese alltäglichen Informationen besonders sensible Daten im Sinne des Art. 9 Abs. 1 DSGVO – für deren Verarbeitung durch die Restaurants reiche die baden-württembergische Corona-Verordnung nicht aus.

Der VGH sah dies anders: Das Interesse an dem Schutz der Bevölkerung und der Eindämmung des Corona-Virus rechtfertigt die Einschränkung des Rechts auf informationelle Selbstbestimmung. Die Nachverfolgbarkeit von Infektionsketten sei dafür ein wichtiges Instrument. Dass Kontaktdaten besonders sensible Daten sind, wollte der VGH auch nicht so ganz glauben. Jedenfalls sei die Verarbeitung aber von der baden-württembergischen Corona-Schutzverordnung gedeckt, deren Wirksamkeit der VGH nicht bezweifelte. Ein Verstoß gegen die DSGVO liegt danach ebenfalls nicht vor.

Ähnlich wie das OVG Münster für das nordrhein-westfälische Pendant der Corona-Verordnung (OVG Münster, Beschluss vom 23.06.2020 – 13 B 695/20) und das OVG Berlin-Brandenburg für das Land Brandburg (OVG Berlin-Brandenburg, Beschluss vom 27.05.2020 – OVG 11 S 43/20), entscheid der VGH Baden-Württemberg damit, dass wir uns an die „neue Normalität“ der Kontaktdatenangabe beim Restaurantbesuch fürs Erste gewöhnen müssen. Für diejenigen, die dies stört, hatte der VGH aber auch eine Lösung bereit: Restaurantbesuche sind freiwillig, wem die Datenangabe nicht passt, soll zu Hause bleiben.

Zu guter Letzt

Auch in diesem Monat gibt es einige interessante Entscheidungen ausländischer Datenschutzbehörden, die teils zu hohen Bußgeldern für die Verantwortlichen führten. Das Unternehmen Google traf es dabei gleich zweimal, wobei es in einem Fall mit einem überraschend niedrigen Bußgeld davonkam. Besonders fleißig war im Übrigen die spanische Datenschutzbehörde. Ihre Bußgelder trafen in diesem Monat vor allem spanische Telekommunikationsunternehmen.

- **Belgien**

Die belgische Datenschutzbehörde verhängte gegen Google ein Bußgeld in Höhe von 600.000 Euro, weil das Unternehmen das „Recht auf Vergessenwerden“ eines Betroffenen nicht ausreichend würdigte. Der Betroffene war eine Person des öffentlichen Lebens in Belgien und beantragte bei Google die Löschung einzelner konkreter Suchergebnisse, die mit seinem Namen automatisch in der Suchmaschine verknüpft wurden. Dabei handelte es sich zum einen um Informationen über seine vermeintliche politische Orientierung und zum anderen um Informationen über eine Beschwerde wegen Belästigung, die zwar zunächst gegen den Betroffenen verfolgt, aber bereits einige Jahre vor Stellung des Antrages abgewiesen wurde. In der Weigerung seitens Google, einen der entsprechenden Inhalte zu entfernen, erkannte die

Datenschutzbehörde letztlich einen Verstoß gegen das „Recht auf Vergessenwerden“, das sich aus Art. 17 Abs. 2 DSGVO ergibt.

- **Griechenland**

In Griechenland wurde gegen eine Kandidatin für eine anstehende Kommunalwahl ein Bußgeld in Höhe von 2.500 Euro verhängt. Die Politikerin versendete SMS-Nachrichten zwecks Wahlwerbung an zahlreiche Personen, ohne vorher je mit ihnen in Kontakt gestanden oder geschweige denn eine Einwilligung für die Nutzung ihrer Handynummer erhalten zu haben. Da der Politikerin auch kein überwiegendes berechtigtes Interesse zur Seite stand, war diese Verwendung der fremden Handynummern rechtswidrig.

- **Niederlande**

In den Niederlanden hat die Datenschutzbehörde ein Bußgeld in Höhe von 830.000 Euro gegen eine Kreditregistrierungsstelle verhängt. Grund dafür war, dass diese den digitalen Zugang zu den über die betroffenen Personen erhobenen Daten nur gegen Zahlung einer Gebühr vorsah und den freien Zugang per Post auf einmal pro Jahr beschränkte. Die Datenschutzbehörde war der Ansicht, dass der digitale Zugang zu den personenbezogenen Daten frei sein müsse. Die Behörde begründete die Höhe des Bußgeldes damit, dass die Kreditregistrierungsstelle durch den gebührengebundenen Zugang der Daten die Betroffenen dazu bewegt, die kostenlose Auskunft per Post zu wählen, die jedoch nur einmal pro Jahr erfolgen soll. Diese Umstände führen in den Augen der Behörde zu einer zusätzlichen Barriere und letztlich zur Entmutigung des Betroffenen in der Durchsetzung seiner Rechte. Die Entscheidung ist bemerkenswert und von hoher praktischer Relevanz. Bei Erfüllung der Betroffenenrechte sind auch die deutschen Aufsichtsbehörden streng. Die unzureichende Erfüllung dieser Rechte (in jeglicher Hinsicht) stellt in der Praxis einen der größten Stolpersteine für Unternehmen dar.

- **Spanien**

Die spanische Datenschutzbehörde belegte das Telekommunikationsunternehmen XFERA MOVILES zum wiederholten Male mit einem Bußgeld. Grund dafür war diesmal, dass das Unternehmen aufgrund eines Fehlers bei der Rechnungsstellung das Konto eines Dritten mit der Rechnung eines

Kunden belastete. Dies hatte zur Folge, dass der Kontoinhaber des belasteten Kontos sämtliche persönlichen Daten des Kunden (Name, Adresse, Ausweis- und Telefonnummer) einsehen konnte. Die Datenschutzbehörde war wegen dieses Vorkommnisses der Ansicht, dass XFERA MOVILES nicht in der Lage sei, ausreichende Sicherheit für personenbezogene Daten zu gewährleisten. Sie sah in dem Verhalten einen Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit der Datenverarbeitung aus Art. 5 Abs. 1 Buchstabe f DSGVO und verhängte ein Bußgeld in Höhe von (lediglich) 70.000 Euro.

Auch im Übrigen war die Behörde fleißig:

- Bußgeld in Höhe von 70.000 Euro gegen das Unternehmen Telefónica Móviles España. Das Unternehmen hatte ohne Zustimmung des Betroffenen die Übertragung seines Telefonanschlusses von einem anderen Anbieter vorgenommen.

- Bußgeld gegen Telefónica Móviles España in Höhe von 70.000 Euro. Diesmal hatte das Unternehmen einer Person fälschlicherweise die Nutzung zweier Telefonanschlüsse eines anderen Kunden in Rechnung gestellt.

- Auch bei der Telefongesellschaft Orange stellte die Datenschutzbehörde einen Verstoß gegen Art. 6 Abs. 1 DSGVO fest. Die Behörde war der Ansicht, dass das Unternehmen nicht die nötigen Mindestanstrengungen unternommen habe, um die Identität seiner Kunden festzustellen. Verhängt wurde ein Bußgeldin Höhe von 80.000 Euro.

- Ferner stellte die Datenschutzbehörde auch einen DSGVO-Verstoß bei der spanischen Airline Iberia fest. Diese weigerte sich gegenüber einem Kunden, die Aufzeichnungen mehrerer Telefongespräche herauszugeben. Die Datenschutzbehörde erkannte in diesem Verhalten einen Verstoß gegen das Auskunftsrecht des Betroffenen aus Art. 15 DSGVO und sanktionierte dieses Verhalten mit einem Bußgeld in Höhe von 40.000 Euro.

- Auch ein Verstoß, der im Zusammenhang mit der Cookie-Nutzung steht, wurde geahndet. Dem Betreiber von drei

Websites wurde ein Bußgeld in Höhe von 6.000 Euro auferlegt, weil er die Nutzer der Websites nicht ausreichend über die Verwendung von Cookies informierte. Der Betreiber verstieß somit in den Augen der Datenschutzbehörde gegen die Informationspflicht, die sich aus Art. 22 Abs. 2 DSGVO ergibt.

- **Ungarn**

In Ungarn wurde ein Bußgeld gegen Google in Höhe von 10.000 Forint verhängt. Das Unternehmen unterließ die beantragte Auskunft über die durch Google AdWords gespeicherten personenbezogenen Daten eines Betroffenen. Google begründete dies damit, dass es nicht wüsste, welche Abteilung für die Erteilung der Auskunft zuständig sei. Nach Art. 12 Abs. 3 DSGVO steht dem Betroffenen allerdings unverzüglich, jedenfalls aber innerhalb eines Monats, eine solche Auskunft zu. Ausgehend von der auffallend geringen Höhe des Bußgeldes (umgerechnet nur 29 (!) Euro) stufte die Datenschutzbehörde die Nichteinhaltung der Frist scheinbar als einen nicht gravierenden datenschutzrechtlichen Verstoß ein.

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