LOSCHELDER

Newsletter Datenschutzrecht

Januar 2021

Sehr geehrte Damen und Herren,

wir wünschen Ihnen ein erfolgreiches und gesundes neues Jahr 2021! Im Datenschutzrecht haben die ersten Wochen des neuen Jahres schon einiges Berichtenswertes mit sich gebracht, über das wir in diesem Newsletter gewohnt praxisnah, knapp und verständlich informieren.

Im neuen Jahr dürfen wir einige Rechtsänderungen im Umfeld der Datennutzung und Digitalisierung erwarten: Erstmals steht ein Vertragsrecht für digitale Produkte vor der Tür, am 13.01.2021 wurde der Regierungsentwurf für entsprechende Änderungen des BGB veröffentlicht. Und auf EU-Ebene wird ein Data Governance Act diskutiert, der einige grundlegende Ideen für die künftige Gestaltung der digitalen Welt mit sich bringt. Grund genug, in diesem Newsletter auch diese Grundsatzthemen anzusprechen und Ihnen einen Überblick auf dem aktuellen Stand zu präsentieren.

Wir beginnen das neue Jahr mit der Fortsetzung unserer Veranstaltungsreihe „Forum Digitalisierung", angesichts der aktuellen Situation virtuell: Drei aktuelle und hoch brisante Themen rund um die Digitalisierung von Geschäftsprozessen diskutieren wir mit Ihnen beim Lunch@Loschelder:

Digitalisierung I: Nur noch ohne US-Tools?
Datenschutzrechtliche Unsicherheiten nach dem Urteil des EuGH zum EU-U.S.-Privacy Shield: Unter welchen Bedingungen können Angebote von US-Dienstleistern rechtskonform genutzt werden?
Mittwoch, den 10.02.2021: 12.00 bis 12.30 Uhr
Dr. Kristina Schreiber / Dr. Simon Kohm

Digitalisierung II: Apps und Services aus „Standardbausteinen"
Was ist urheberrechtlich zu beachten, insbesondere bei Nutzung von Open Source-Elementen?
Mittwoch, den 10.03.2021: 12.00 bis 12.30 Uhr
Dr. Patrick Pommerening / Dr. Hans-Georg Schreier, LL.M.

Digitalisierung III: Neues für Verträge über digitale Inhalte und Dienste
Die größte Reform des BGB seit dem Schuldrechts-modernisierungsgesetz? Wir geben einen Überblick über die anstehenden Änderungen durch die neuen EU-Vorgaben, die zum 01.07.2021 umzusetzen sind.
Mittwoch, den 14.04.2021: 12.00 bis 12.30 Uhr
Dr. Kristina Schreiber / Dr. Hans-Georg Schreier, LL.M.

Wir freuen uns über Ihre Anmeldung unter webinare@loschelder.de – die Veranstaltungen sind selbstverständlich kostenlos.

Inhalt

Twitter im Visier der Aufsichtsbehörden. Oder: Wenn zwei sich streiten…

Ein Datenleck bei Twitter sorgt derzeit für Streit zwischen den Datenschutzbehörden in Europa: Viele, darunter auch deutsche Behörden, sind mit der Handhabung des Vorfalls durch die zuständige irische Datenschutzaufsichtsbehörde (DPC) nicht einverstanden und legten gegen deren Entscheidung auf EU-Ebene Einspruch ein. Nun hat der Zusammenschluss der europäischen Datenschutzbehörden, der Europäische Datenschutzausschuss (EDSA) den Konflikt vorerst durch eine Entscheidung beendet – die in der Sache allerdings überwiegend enttäuscht. Das Twitter in Aussicht gestellte Bußgeld aber wird die DPC anheben, von 150.000 – 300.000 Euro auf 450.000 Euro.

Der Twitter-Konzern hat ebenso wie die anderen Giganten der Social Media Welt einen europäischen Ableger mit Sitz in Irland. Bei diesem wurde Ende 2018 ein Datenleck aufgedeckt: Durch einen Programmierungsfehler wurden in bestimmten Fällen Tweets öffentlich sichtbar, auch wenn der Account-Inhaber seine Tweets auf „privat" gestellt hatte. Nachdem das Leck dem Konzern bekannt wurde, meldete der irische Twitter-Ableger dies bei der irischen Datenschutzaufsichtsbehörde, der Data Protection Commission (DPC) in Dublin. Diese startete prompt eine Untersuchung der Angelegenheit, dessen Ergebnis inklusive eines Entwurfs zum Bescheid über die Datenschutzverstöße des Konzerns Mitte 2020 den anderen europäischen Datenschutz-aufsichtsbehörden von der DPC zur Kommentierung vorlegt wurde.

Kommentiert wurde der vorlegte Entscheidungsentwurf vielfach: Datenschutzaufsichtsbehörden aus acht Ländern meldeten sich mit Einsprüchen nach Art. 60 Abs. 4 DSGVO beim EDSA, darunter auch mehrere deutsche Behörden. Das Verfahren nach Art. 60 Abs. 4 DSGVO dient der Kohärenz der Anwendung und Auslegung der DSGVO durch die verschiedenen nationalen Datenschutz-aufsichtsbehörden. Können sich die Behörden untereinander nicht einigen, entscheidet der EDSA, um eine einheitliche Auslegung und Anwendung der DSGVO über die nationalen Grenzen hinweg sicherzustellen.

Die Aufsichtsbehörden übten reichlich Kritik an der Einschätzung des Sachverhalts durch die DPC: Neben der Zuständigkeit der DPC

wurde in Frage gestellt, ob deren Einschätzung, der europäische Ableger von Twitter, „Twitter International“, sei alleiniger Verantwortlicher für die Datenverarbeitung in Europa, richtig sei. Zu groß seien die organisatorischen, technischen und sonstigen Überlappungen mit der Konzernzentrale in den USA, weshalb die beiden zumindest gemeinsame Verantwortliche seien. Auch die Beurteilung der DPC, inwieweit das Verhalten von Twitter eine Verletzung der DSGVO-Vorgaben darstelle, wurde von vielen der kritisierenden Aufsichtsbehörden anders gesehen: Sie sahen deutlich mehr und auch andere Vorschriften verletzt als die DPC. Schließlich wurden auch die von der DCP verhängten Konsequenzen für den Konzern kritisiert. Vor allem sei das Bußgeld falsch bemessen worden und damit zu niedrig angesichts der Ausmaße des Datenlecks.

… entscheidet der EDSA …

: Verantwortliche – dies ist in Home-Office-Situationen regelmäßig der Arbeitgeber – haben mittels technischer und organisatorischer Maßnahmen (Art. 25 Abs. 1 DSGVO) sicherzustellen, dass Einblicke in die Privatsphäre der Betroffenen nicht möglich sind (z.B. durch Ausrichtung der Kamera oder durch Einblendung eines virtuellen Hintergrunds). Alternativ kann in solche Einblicke in die Privatsphäre eingewilligt werden (Art. 26 Abs. 2 DSGVO). In jedem Fall muss aber darauf geachtet werden, dass der Betroffene durch den Verantwortlichen über die datenschutzrechtlichen Risiken aufgeklärt wird, die sich aus einer Videokonferenz in den privaten Räumen ergeben.

Da die DPC diese Kritik zurückwies, musste der EDSA nach Art. 65 Abs. 1 DSGVO über den Konflikt entscheiden. Die Entscheidung fiel mit dem Beschluss 01/2020 im November 2020 (die englische Fassung ist hier abrufbar). Bemerkenswert ist der Beschluss schon deshalb, weil er seit dem Inkrafttreten der DSGVO den ersten verbindlichen Beschluss nach Art. 65 Abs. 1 DSGVO über Meinungsverschiedenheiten von nationalen Aufsichtsbehörden in einem Kohärenzverfahren darstellt.

Der Clou an der Sache ist, dass nach der DSGVO und der Einschätzung des EDSA nur die Einsprüche berücksichtigt werden müssen, die den Anforderungen des Art. 60 Abs. 4 DSGVO entsprechend „maßgeblich und begründet“ sind. Das heißt, auch wenn die Kritik einer anderen Aufsichtsbehörde angebracht und

richtig ist, liegt kein Einspruch im Sinne des Art. 60 Abs. 4 DSGVO vor, wenn der Hinweis auf die Konsequenzen der kritisierten Entscheidung für die Rechte und Freiheiten der Betroffenen fehlt.

… oder auch nicht!

Diese formalen Anforderungen hielten die überwiegenden Rügen der Datenschutzaufsichtsbehörden nach Ansicht des EDSA nicht ein. Zu einem Großteil der Kritikpunkte und der darin aufgeworfenen Fragen nahm der EDSA daher keine Stellung, weil nach seiner Analyse kein „maßgeblicher und begründeter" Einspruch i.S.d. DSGVO vorlag. Nicht weiter diskutiert wurden deshalb die Fragen um die Verantwortlichenstellung des europäischen Twitter-Ablegers und einiger der nach Ansicht der Aufsichtsbehörden vorliegenden Verstöße gegen die DSGVO.

Ebenfalls enttäuschend dürfte sein, dass der EDSA auch dort, wo es einen ausreichenden Einspruch sah, keine inhaltliche Entscheidung treffen konnte, weil die von der DPC gelieferten Informationen nicht ausreichend waren, um den Sachverhalt richtig bewerten zu können. Hier wurde die DPC zwar gerügt, in Zukunft detaillierter zu arbeiten. Zur Klärung des Sachverhaltes wurde aber ohne eine wirkliche Einschätzung des EDSA nicht beigetragen.

Eine Entscheidung fällte der EDSA lediglich über die Grundlage der Bußgeldberechnung und der daraus resultierenden Höhe des geplanten Bußgelds. Bei dieser legte die DPC nicht den richtigen Maßstab an; vor allem hatte sie die Schwere und Reichweite des Datenschutzverstoßes durch den Programmierfehler nicht ausreichend berücksichtigt. Der EDSA verlangte, dass in einer erneuten Abwägung ein höheres Bußgeld verhängt wird.

Immerhin: Die DPC veröffentlichte Anfang Dezember ihre überarbeitete Entscheidung gegenüber dem europäischen Twitter-Ableger (abrufbar hier in englischer Sprache). Das Bußgeld wurde in dieser von den zunächst geplanten 150.000 – 300.000 Euro auf 450.000 Euro angehoben.

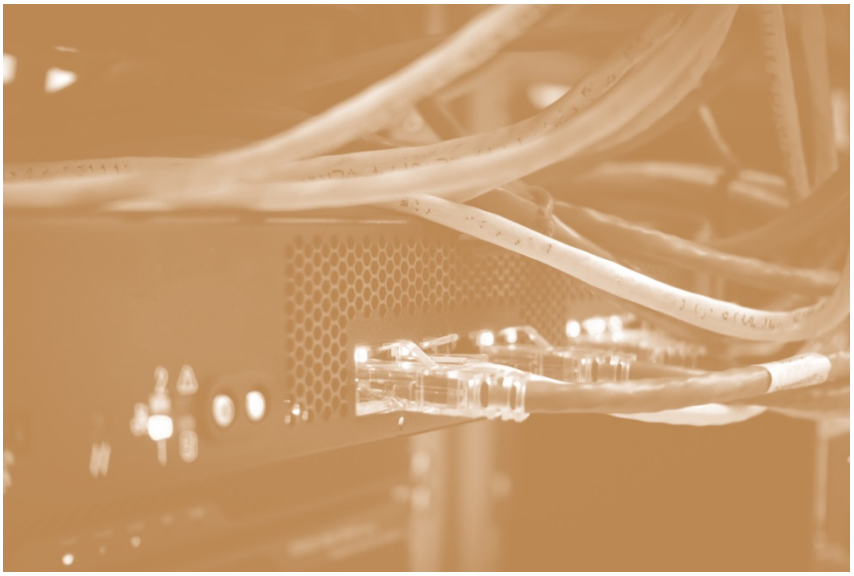
Der Brexit und der Datenschutz: UK ist ein Drittland

Am 31.12.2020 ist das Vereinigte Königreich endgültig aus der Europäischen Union ausgetreten. Auch die Übergangsphase ist nun vorbei. In letzter Minute konnten sich EU und UK über einen „Deal" einigen. Auch das Datenschutzrecht ist in diesem berücksichtigt. Bringt dies die erhoffte Entwarnung für die weitere Übermittlung von Daten in das Vereinigte Königreich?

Im Handels- und Kooperationsabkommen zwischen der EU und UK findet sich auf Seite 406 f. eine „Übergangsbestimmung für die Übermittlung von personenbezogenen Daten an das Vereinigte Königreich" (Artikel FINPROV.10A). Nach dieser gilt das Vereinigte Königreich für die nächsten vier Monate nicht als Drittland, die Frist kann um weitere zwei Monate verlängert werden. Geplant ist, dass die EU-Kommission während dieser Zeit einen Angemessenheitsbeschluss i.S.d. Art. 45 DSGVO erlässt, der das Vereinigte Königreich als sicheres Drittland ausweist und den Austausch personenbezogener Daten somit erheblich erleichtert.

Unternehmen können damit zunächst auch dann aufatmen und personenbezogene Daten weiterhin mit Unternehmen im Vereinigten Königreich austauschen, wenn sie keine vorsorglichen Maßnahmen getroffen haben. Dies entspricht nach einer Stellungnahme der Datenschutzkonferenz vom 28.12.2020 auch der Position der deutschen Aufsichtsbehörden.

Aufgrund der Unsicherheiten bis zur letzten Minute haben in der Praxis viele Unternehmen mit EU-Standardvertragsklauseln den weiteren Datentransfer in das Vereinigte Königreich geregelt. Die Absicherung des Datentransfers mit den EU-Standardvertragsklauseln einschließlich der nach der Rechtsprechung des EuGH notwendigen individuellen Prüfung ist auch unter Berücksichtigung des Handels- und Kooperationsabkommens die rechtssicherere Lösung: Dogmatisch wird nämlich bereits höchst streitig diskutiert, ob die Datenschutzgrundverordnung und das EU-Recht insgesamt eine solche Fiktion überhaupt ermöglichen – ein sehr berechtigter Einwand. Zudem haben beide Seiten das vertragliche Recht, der Verlängerung zu widersprechen. Damit könnte das Vereinigte Königreich binnen kürzester Zeit auch vor Ablauf der beschriebenen 4 bzw. 6 Monate zum Drittland werden.



Ein neues digitales Vertragsrecht

Das BGB wird um einen neuen Abschnitt erweitert: Im allgemeinen Schuldrecht wird es künftig gesonderte Regelungen für digitale Produkte geben, die von Unternehmern an Verbraucher (B2C) vertrieben werden. Es steht eine kleine Revolution des Vertragsrechts vor der Tür, die für die Wirtschaft einen ganz erheblichen Erfüllungsaufwand mit sich bringt.

Am 13.01.2021 veröffentlichte das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) den Regierungsentwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RegE).

Der Gesetzentwurf sieht einen neuen Titel 2a „Verträge über digitale Produkte“ im „Recht der Schuldverhältnisse“ vor. Die neuen Vorgaben für Verbraucherverträge über digitale Produkte werden unabhängig vom Vertragstyp gelten. Hinzu kommen einzelne Sonderregelungen im besonderen Teil, etwa zum Kauf- und Mietvertragsrecht.

Die wichtigsten Neuerungen im Schnelldurchlauf:

- **Anwendungsbereich**: Die Neuregelungen sollen unmittelbar nur für Verbraucherverträge gelten. Sachlich ist der Anwendungsbereich aber sehr weit: Alle digitalen Dienstleistungen und Inhalte („digitale Produkte“) fallen darunter sowie digitale Elemente von Paket- und kombinierten Verträgen (wenn etwa das Fernsehgerät gekoppelt mit einem Streamingangebot vertrieben wird).

- **Gegenleistung**: Erfasst sind „Verträge“, der Gesetzentwurf versteht dies aber denkbar weit. Grundsätzlich muss es also zu einem Leistungsaustausch zwischen Unternehmer und Verbraucher kommen. Hier kann die Gegenleistung des Verbrauchers für das digitale Produkt auch die Preisgabe personenbezogener Daten sein. Zum anderen tendieren die Entwurfsverfasser dahin, schon die Einwilligung auf einer Website in das Werbetracking als ausreichend für eine auf den Vertragsschluss gerichtete Willenserklärung anzusehen. Wird also bald jeder Websitebesuch einen Vertrag mit den Besuchern begründen (mit den weitreichenden Vorgaben der

neuen Regelungen), wenn ein personenbezogenes Werbetracking erfolgt?

- **Updatepflicht**: Digitale Produkte müssen künftig aktualisiert werden, solange der Vertrag läuft und auch darüber hinaus, solange der Verbraucher eine weitere Aktualisierung „vernünftigerweise" erwarten darf. Möglicherweise werden Unternehmensentscheidungen wie die Einstellungen der Aktualisierungen etwa für ältere Windowsversionen damit künftig nicht mehr vereinbar sein.

- **Mängelbegriff und Folgeansprüche**: Der Mängelbegriff wird ausgedehnt und digitale Produkte damit schneller zum Gewährleistungsfall. Besonders hervorzuheben: „Objektiv" mangelfrei sein soll ein digitales Produkt nach den Neuregelungen nur, wenn es den „objektiven Anforderungen" entspricht, also etwa eine „übliche" Beschaffenheit aufweist. Will der Unternehmer davon abweichen, muss er den Verbraucher gesondert und explizit darauf hinweisen und sich die Abweichung aktiv bestätigen lassen. Das „Kennen" eines Mangels als Ausschlussgrund für die Gewährleistung wir damit ganz erheblich beschränkt.

- **Änderungsrechte**: Die Rechte von Unternehmern, digitale Produkte zu ändern und sich derartige Rechte im Vertrag vorzubehalten, werden künftig eingeschränkt. Zum einen gibt es Änderungsrechte nur, wenn diese rechtskonform im Vertrag vorgesehen sind. Zum anderen werden die Fälle zunehmen, in denen eine Änderung nicht durgesetzt werden kann und daher mehrere Produktversionen im Markt gehalten werden müssen.

- **Folgen datenschutzrechtlicher Erklärungen des Verbrauchers**: Für den Datenschutzrechtler besonders spannend ist eine eher unternehmensfreundliche Neuregelung. Widerruft ein Verbraucher eine gegebene Einwilligung oder widerspricht der Datenverarbeitung, kann der Unternehmer den Verbrauchervertrag fristlos kündigen, wenn ihm die weitere Fortsetzung des Vertrags nicht zugemutet werden kann. Mit dem Kopplungsverbot des Art. 7 Abs. 4 DSGVO und dem „freien" Widerrufs- und Widerspruchsrecht ist dies wohl dort in Einklang zu bringen, wo der Verbraucher personenbezogene Daten als

Gegenleistung, „Bezahlung“ hingegeben hat. Hier wird es indes in den kommenden Monaten noch einigen Diskussionsbedarf geben.

- **Weiterverwendung nicht personenbezogener Daten nach Vertragsbeendigung**: Unternehmer werden künftig in der Weiterverwendung von nicht personenbezogenen Daten nach Vertragsbeendigung erheblich eingeschränkt. Umso sorgfältiger wird künftig zu prüfen sein, wie Verträge gestaltet und Daten erhoben werden, um auch die Entwicklung neuer Geschäftsmodelle nicht weiter zu beschränken, als zwingend notwendig.

Unternehmen müssen die absehbaren Neuregelungen zügig analysieren und den Umstellungsbedarf ermitteln, insbesondere hinsichtlich Produktgestaltung, der Einführung notwendiger Prozesse etwa für die künftigen Updatepflichten einschließlich erweiterter Informationspflichten und – last but not least – der Anpassung der Verträge.

Auch wenn die Neuregelungen unmittelbar nur den B2C-Rechtsverkehr betreffen, werden sie ganz erheblichen Einfluss auf den rein unternehmerischen Rechtsverkehr haben. Zum einen dann, wenn die Produkte sowohl Verbrauchern- als auch Unternehmern angeboten werden, zum anderen aufgrund absehbarer Ausstrahlwirkungen der Neuregelungen auch auf den B2B-Bereich. Nicht zuletzt basieren zahlreiche B2B-Geschäftsmodelle mittelbar auf Datenerhebungen (anonymisiert oder personenbeziehbar) bei Verbrauchern. Änderungen im B2C-Bereich schlagen dann unmittelbar auf den B2B-Bereich durch.

Ein ausführlicher Überblick hierzu wird in Kürze in der ZdiW, der seit diesem Jahr neu erscheinenden Zeitschrift für das Recht der digitalen Wirtschaft erscheinen. Sprechen Sie uns bei Interesse gerne hierauf an (kristina.schreiber@loschelder.de).

EU-Datenstrategie: Der Data Governance Act

Die EU-Kommission hat im November 2020 eine neue Gesetzesinitiative auf den Weg gebracht, den sogenannten Data Governance Act (DGA). Die EU-Kommission erhofft sich, dass der DGA dazu beitragen wird, das enorme Potential wertvoller, aber bisher zum Großteil ungenutzter, Datenbestände nutzbar zu machen. Die Verordnung soll Impulse setzen, die den Zugang zu den Datenbeständen sowie die gemeinsame Nutzung von Daten erleichtert und rechtssicherer macht. Wie und wo genau, haben wir für Sie hier zusammengefasst.

Was ist das Ziel der Verordnung?

Der Data Governance Act ist Teil der Anfang 2020 veröffentlichen europäischen Datenstrategie. Hinter ihm verbergen sich Regelungen und Mechanismen für den Umgang mit Daten. Er soll dazu beitragen, dass personenbezogene und nicht personenbezogene Daten effizienter verwendet werden. Die EU-Kommission beabsichtigt, mit dem DGA einen „Datenbinnenmarkt" innerhalb der EU zu verwirklichen (zum Ganzen DGA-Entwurf der Kommission, COM(2020) 767 final). Dafür enthält der DGA Instrumente, die einen rechtsicheren und einfachen Datenaustausch ermöglichen und die gemeinsame Nutzung von Daten stärken. Ohne den Austausch vorhandener oder neu generierter Daten kann das enorme gesellschaftliche und wirtschaftliche Potential, das vor allem in Bereichen wie der

technologischen Entwicklung (z.B. dem maschinellen Lernen), einer nachhaltigen Steuerung des Verkehrs, der Digitalisierung von Bildungsinhalten/-methoden oder der Schaffung gesamtheitlicher digitaler Entwicklungskonzepte (z.B. für Städte als sog. „Smart Citys“) liegt, nicht effektiv genutzt werden.

In ihrem Vorschlag betont die EU-Kommission, dass die Impulse des DGA nicht zulasten des hohen Datenschutzniveaus in der EU gehen sollen. Die Rechtsvorschriften sollen vielmehr ineinandergreifen und die bereits bestehenden Vorschriften ergänzen. Der DGA begegnet damit der enormen Herausforderung, Datennutzungspotentiale zu heben und Rechtssicherheiten abzubauen, zugleich aber das Schutzniveau der DSGVO zu halten.

Wie soll es umgesetzt werden?

Die EU-Kommission hat im DGA-Entwurf im Wesentlichen drei Instrument zur Realisierung ihrer Ziele vorgeschlagen:

- **Weiterverwendung von Datenbeständen, die sich in öffentlicher Hand befinden:** Öffentliche Stellen sind im Besitz großer Datenmengen. Der DGA soll die Richtlinie über offene Daten ergänzen, indem auch die Weiterverwendung besonders geschützter Daten aus der Hand öffentlicher Stellen erlaubt sein soll, wenn der Schutz von Privatsphäre und Geheimhaltungsinteressen sichergestellt ist.

- **Stärkung des Datenaltruismus:** Organisationen, die Daten zu Gemeinwohlzwecken nutzen, sollen unterstützt werden. Dafür soll die Möglichkeit der freiwilligen Bereitstellung von Daten durch Einzelpersonen oder Unternehmen für das Allgemeinwohl transparenter und rechtssicherer gestaltet werden. Unter dem Stichwort „Datenaltruismus“ wird schon seit längerer Zeit diskutiert, wie die durchaus bestehende Bereitschaft von Bürgern/-innen, personenbezogene Daten für altruistische Zwecke bereitzustellen, in einen rechtlichen Rahmen gefasst werden kann. Die EU-Kommission schlägt dafür im DGA zwei Instrumente vor:

    - Das Vertrauen von Bürger/-innen und Unternehmen in gemeinwohlorientierte Organisationen soll über eine Art „Gütesiegel“ gestärkt werden („in der Union anerkannte datenaltruistische Organisation“).

- Für die gemeinwohlorientierte Arbeit soll ein gemeinsames europäisches Einwilligungsformular als ein rechtssicheres Dokument für das Sammeln von Datenspenden bereitgestellt werden.

Ob diese Maßnahmen den gewünschten Effekt – insbesondere den erhofften Vertrauensvorschuss – haben werden, wird kontrovers diskutiert.

- **Förderung der gemeinsamen Nutzung von Daten:** Es soll ein Anmeldeverfahren für Anbieter eingerichtet werden, die anderen Akteuren eine transparente und gemeinsame Nutzung von Daten ermöglichen. Diese Anbieter zeichnen sich dadurch aus, dass sie als vertrauenswürdige, unabhängige Dienstleister gemeinsam genutzte Daten zusammenführen und die Weiterverarbeitung organisieren (sog. „Datenintermediäre bzw. Datenvermittler"). Anbieter, die u.a. den verarbeiteten Daten neutral gegenüberstehen müssen und kein eigenes Interesse an der Verarbeitung haben dürfen, sollen sich in ein öffentliches, von den Mitgliedstaaten einzuführendes Register eintragen können.

Wie geht es weiter?

Nachdem der Vorschlag der Europäischen Kommission dem Europäischen Parlament und dem Rat der Europäischen Kommission vorgelegt wurde, durchläuft der Vorschlag nun das ordentliche Gesetzgebungsverfahren. Bis zum 1. Februar 2021 können bei der EU-Kommission noch Stellungnahmen zum Vorschlag des DGA eingereicht werden. Bis Parlament und Rat gemeinsam über die Annahme des Vorschlags entscheiden werden, wird noch einiges an legislativer Arbeit erwartet und bis zum Inkrafttreten des DGA daher noch einige Zeit vergehen. Für die Weiterentwicklung von Geschäftsmodellen macht es aber schon heute Sinn, die geplanten Neuregelungen im Blick zu halten.

Zu guter Letzt

Auch zum neuen Jahr gibt es einige berichtenswerte Bußgelder – allen voran 10,4 Mio. Euro gegen „notebooksbilliger.de“. Verhängt wurde es von der niedersächsischen Aufsichtsbehörde, weil eine unzulässige Videoüberwachung erfolgt sei. Die Entscheidung ist nicht nur wegen der Höhe des Bußgeldes höchst interessant, sondern auch, weil die Behördenmitarbeiter während einer Ermittlungszeit von mehreren Jahren wohl kein einziges Mal vor Ort die Videoüberwachung in Augenschein genommen haben. Und jenseits der Bußgelder gibt es noch lesenswerte Anmerkungen zu WhatsApp und Zoom.

- **Zoom unterstützt den datenschutzkonformen Einsatz**

  Der Videokonferenz-Dienst war zu Beginn der Corona-Pandemie nicht nur unter Datenschützern in Verruf geraten. Der Vorwurf undurchsichtiger und (zu) umfassender Datenverarbeitungsvorgänge sowie zwangsweiser und intransparenter Datenübermittlungen an Dritte, u.a. Facebook, standen im Raum und unterlagen einer breiten Berichterstattung durch die Medien. Deutlich intensiver, als viele andere Anbieter, besserte Zoom seine Dienste daraufhin nach. Auch die Datenschutzaufsichtsbehörden erkannten dies an, etwa aus Baden-Württemberg wurde ausdrücklich auf die Verbesserungen hingewiesen. Nun folgte jüngst ein weiterer Schritt von Zoom in Sachen Datenschutz, der Unternehmen

bei dem datenschutzkonformen Einsatz des Dienstes eine hilfreiche Stütze bietet: Zoom veröffentlichte jüngst eine „Datenschutz-Checkliste“ für Zoom-Nutzer, orientiert an den Vorgaben der DSK.

- **WhatsApp einmal mehr in der Kritik**

  Hohe Wellen schlug in den vergangenen Tagen die Ankündigung von WhatsApp, ab Anfang Februar Kunden von der weiteren Nutzung des Messenger Dienstes auszuschließen, wenn diese bis dahin die aktualisierten Nutzungsbestimmungen nicht akzeptiert hätten. Im Ausgangspunkt ist ein solches Vorgehen üblich und auch grundsätzlich nachvollziehbar, um Vertragsbedingungen umfassend erneuern zu können.

  Das Problem: Kritiker sahen in den neuen Nutzungsbedingungen die zwangsweise „Einwilligung“ in die umfassende Datenübermittlung an Facebook – damit etwa Facebook künftig auf die WhatsApp-Kommunikation zugeschnittene Werbung anzeigen kann.

  Die Kritik, so WhatsApp, sei unbegründet. Dennoch: Die öffentliche Kritik hat bewirkt, dass WhatsApp die Zustimmungsfrist nun verschiebt – bis Mai sollen die Bedenken ausgeräumt und klargestellt sein.

  Jedenfalls melden alternative Messenger-Dienste erhebliche Kundenzuwächse aus den vergangenen Tagen. Für etliche WhatsApp-Nutzer war die Ankündigung wohl die Motivation, zu datenschutzfreundlicheren Messenger-Diensten zu wechseln.

- **10,4 Mio. Euro Bußgeld aus Niedersachsen für unzulässige Videoüberwachung**

  Ein weiteres Millionenbußgeld erfuhr in den vergangenen Tagen Beachtung: Das Unternehmen Notebooksbilliger.de soll über mindestens zwei Jahre Beschäftigte per Video überwacht haben, ohne dass dafür eine Rechtsgrundlage vorlag. Die unzulässig angebrachten Kameras hätten unter anderem Arbeitsplätze, Verkaufsräume, Lager und Aufenthaltsbereiche gefilmt (Pressemitteilung der LfD

Niedersachsen vom 08.01.2021). Angesichts erheblicher Jahresumsätze liegt das Bußgeld bei etwa 1%.

Notebooksbilliger.de veröffentlichte eine eigene Darstellung der Angelegenheit. Auffällig ist, dass danach die Behördenmitarbeiter die Videoüberwachungsanlage zu keinem Zeitpunkt in Augenschein genommen hätten. Aus der reinen Dokumentation aber sei der Sachverhalt deutlich weniger klar zu erkennen, als dies vor Ort möglich sei.

Notebooksbilliger.de kündigte an, das Bußgeld gerichtlich überprüfen zu lassen. Der Fall wird weitere grundlegende Fragen einer ersten gerichtlichen Klärung zuführen, neben den materiellen Themen rund um die Videoüberwachung, insbesondere auch die Untersuchungs- und Sachverhaltsaufklärungspflichten der Aufsichtsbehörden und – zum zweiten Mal – die Angemessen- und Verhältnismäßigkeit des Bußgeldbemessungskonzepts der DSK. Letzteres stand auch im 1&1-Verfahren bereits auf dem Prüfstand, das LG Bonn hatte die Berechnungsweise überzeugend kritisiert und das vom BfDI gegen 1&1 verhängte Bußgeld von gut 9 Mio. Euro auf 900.000 Euro reduziert.

Bemerkenswert ist schließlich auch: Es ist einer der ersten Fälle, in denen die LfD Niedersachsen den Namen des Bußgeldadressaten veröffentlicht. Darauf war bisher aus guten Gründen verzichtet worden; die öffentliche Berichterstattung greift zusätzlich und gesondert aufgrund der Öffentlichkeitswirksamkeit in die Rechte des betroffenen Unternehmens ein.

- **Polen: Über 450.000 Euro für mangelnde Monitoring-prozesse**

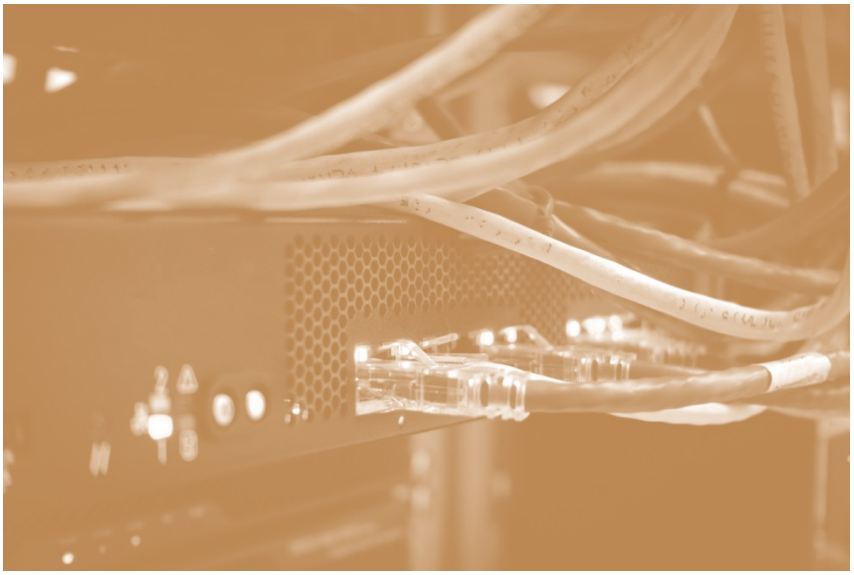
  Die polnische Aufsichtsbehörde (UODO) hat ein erhebliches Bußgeld gegen ein Unternehmen wegen des Vorwurfs verhängt, dass dieses Unternehmen keine internen Richtlinien und Monitoringprozesse zur Überprüfung implementiert hat, ob die umgesetzten technischen und organisatorischen Maßnahmen auch nach einiger Zeit noch angemessen sind oder Änderungen erforderlich werden. Das Bußgeld führt überaus deutlich vor Augen, wie bedeutsam die

Implementierung eines Datenschutz-Managements im Unternehmen ist.

- **Spanien: Unzureichende Datenschutzhinweise**

  In Spanien wurden zwei Bußgelder in Höhe von 2 und 3 Millionen Euro wegen zahlreicher Informationsmängel in Datenschutzhinweisen verhängt. Anlass der behördlichen Untersuchung waren mehrere Beschwerden, die gegen kommerzielle Werbemaßnahmen (SMS, Anruf oder E-Mail) des betroffenen Unternehmens eingereicht worden waren. Die spanische Aufsichtsbehörde entschied zum einen, dass die Datenschutzhinweise des Unternehmens zu unpräzise formuliert waren und zu ungenaue Begriffe verwendet wurden. Darin sah die Behörde einen Verstoß gegen den Transparenzgrundsatz der DSGVO, der das Unternehmen zwei Millionen Euro kostet.

  Das zweite Bußgeld verhängte die Behörde wegen Verstoßes gegen den Art. 6 DSGVO, denn das Unternehmen hatte ihrer Ansicht nach ohne gültige Erlaubnisgrundlage personenbezogene Daten verarbeitet. Eingeholte Einwilligungen seien unwirksam, da insbesondere unzureichende Informationen in Bezug auf die Art der verarbeiteten Daten vorhanden waren. Besonders hervor hob die Aufsichtsbehörde zahlreiche Informationsmängel in Bezug auf Profiling-Maßnahmen, die das Unternehmen auch zu kommerziellen Zwecken nutzte.



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