LOSCHELDER

Newsletter Datenschutzrecht

April 2022

Sehr geehrte Damen und Herren,

unser aktueller Newsletter bringt einige (verspätete) datenschutzrechtliche Ostereier: Facebook steht wieder einmal in der Kritik und auch die Datenverarbeitung auf Bewertungsportalen hat es erneut ins Rampenlicht geschafft. Die dazu ergangene BGH-Entscheidung ist aber nicht nur für Portalbetreiber interessant: Das Gericht beschäftigt sich intensiv mit der Reichweite des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und damit mit der in der Praxis vielbeschworenen Datenverarbeitung aus überwiegendem berechtigten Interesse. Aus den zunehmenden, datenschutzrechtlich interessanten Verfahren vor dem EuGH haben wir für Sie aktuelle Schlussanträge ausgewertet, die für die zentralen Grundsätze der Zweckbindung und Speicherbegrenzung praktisch höchst relevant sind. Kurz vor Redaktionsschluss hat der EuGH zudem eine Pressemitteilung veröffentlicht: auch Verbraucherschutzverbände dürfen jetzt die Einhaltung der DSGVO mithilfe von Klagen durchsetzen – ohne dazu von einem Verbraucher beauftragt worden zu sein. Und schließlich wagen wir einen Ausblick auf den nun im Entwurf vorliegenden Data Act, ein „Datengesetz“ mit weitreichenden Auswirkungen für das Datengeschäft. Der Newsletter schließt wie immer mit einigen spannenden Bußgeldern der letzten Wochen und einem DSK-Beschluss zum „Gastzugang“ in Online-Shops.

Zudem noch ein Hinweis in eigener Sache: Wir laden Sie herzlich ein zu unserem kostenfreien Lunch@Loschelder-Webinar zum Thema:

Datenhandel: Wie können Unternehmen Daten monetarisieren?

Daten werden für neue Geschäftsmodelle immer wichtiger. Aber wie können Unternehmen Daten rechtskonform beziehen, wie rechtskonform an Dritte "verkaufen"? Welche rechtlichen Gestaltungsmöglichkeiten bestehen unter Einhaltung der mannigfaltigen Grenzen des Datenschutzrechts, Urheberrechts, allgemeinen Zivilrechts und der neuen Regeln aus Brüssel (insbesondere dem "Data Act")? In unserem Lunch@Loschelder-Webinar führen wir Sie kompakt durch die für die Praxis wichtigsten Regelungsfelder und zeigen typische Fallstricke bei der Produkt- und Vertragsgestaltung auf.

Mittwoch, 15. Juni 2022 (12 Uhr bis 12.30 Uhr)

Referenten: Dr. Kristina Schreiber / Dr. Patrick Pommerening

Anmeldung unter: webinare@loschelder.de

Inhalt

Facebook Fanpages – never ending story

Der Betrieb von Facebook Fanpages steht schon lange in der datenschutzrechtlichen Kritik, erst recht nach der EuGH-Entscheidung in Sachen Schrems II. Untersagt worden sind die entsprechenden Unternehmenspräsenzen bislang von den Aufsichtsbehörden indes nicht. Ein Kurzgutachten bringt nun neuen Schwung in die Sache, die Datenschutzaufsichtsbehörden wollen zeitnah „darauf hinwirken", dass Fanpages deaktiviert werden.

Im Fokus stehen sollen laut Beschluss der DSK, der mit einer Gegenstimme gefasst wurde, zunächst die Fanpages öffentlicher Stellen. Deaktiviert werden sollen diese, falls die Betreiber die „datenschutzrechtliche Konformität" nicht nachweisen können. Wie ein solcher Nachweis gelingen kann, konkretisieren die Aufsichtsbehörden nur ansatzweise. Im Fokus stehen folgende datenschutzrechtliche Aspekte:

- Vertrag über die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO mit Facebook: Facebook bietet eine solche automatisiert erstellte Vereinbarung an. Ob diese Regelung den Anforderungen des Art. 26 DSGVO genügt, wird nicht näher erläutert.

- Ausreichende Information der Nutzer der Fanpages nach Art. 13 DSGVO: Auch hier bleibt unklar, welche konkreten Anforderungen die Datenschutzaufsichtsbehörden stellen. In der Praxis ist die größte Hürde die Unkenntnis der Fanpagebetreiber, wie genau Facebook mit den Daten der Nutzer umgeht. Ob dies zu einer unzureichenden Transparenz auf Seiten der Fanpagebetreiber führt, bleibt offen.

- Endgerätezugriffe müssen im Einklang mit den Anforderungen des § 25 TTDSG gestaltet sein, regelmäßig also mit Einwilligung. Dies haben die Fanpagebetreiber naturgemäß jedoch nicht in der Hand, da Facebook die technische Kontrolle innehat.

- Last but not least steht die „US-Frage" im Fokus: Werden personenbezogene Daten entgegen den Anforderungen der Art. 44 ff. DSGVO von Facebook in die USA übertragen? Bislang ist nicht endgültig entschieden, ob Nutzer wirksam in den US-Transfer auch in einem Massengeschäft wie dem der

Facebook-Fanpages einwilligen können oder – so wohl die überwiegende Tendenz der Aufsichtsbehörden, die sicherlich streitbar ist – nicht.

Der DSK-Beschluss basiert auf einem Kurzgutachten der Taskforce Fanpages aus März 2022, das zu einem vernichtenden Ergebnis kommt: Fanpages können danach nicht im Einklang mit DSGVO und TTDSG betrieben werden.

Unternehmen müssen die weiteren Entwicklungen zu verfolgen. Zu erwarten ist, dass die Aufsichtsbehörden zunächst gegen öffentliche Stellen vorgehen, im Anschluss daran dann aber voraussichtlich auch gegen private Unternehmen. Unternehmen brauchen also insbesondere für ihre Fanpages eine „Exit-Strategie", die im Zweifel sehr kurzfristig umgesetzt werden kann.

Keine Pflicht zur Löschung von Daten auf Arztbewertungsportal: Oder auch die Reichweite berechtigter Interessen

Im Februar 2022 hat der BGH erneut einen Fall mit Bezug zum Arztsuche- und -bewertungsportal „Jameda" entschieden. Die klagende Augenärztin hatte keinen Erfolg mit ihrem Verlangen, dass ein ohne ihr Zutun erstelltes Profil zu ihrer Praxis auf der Plattform gelöscht wird. Die berechtigten Interessen von Portalbetreiber und Nutzern an einer möglichst vollständigen Übersicht rechtfertigten die Datenverarbeitung, der keine überwiegenden Interessen der Augenärztin entgegenstanden. Die Entscheidung ist aber nicht nur für Bewertungsportale von Relevanz: Das Gericht konkretisiert die Prüfung berechtigter Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO in einer für die Praxis überaus hilfreichen Art und Weise.

Die Beklagte in der dem Urteil des BGH vom 15.02.2022 zugrundeliegenden Sache betreibt das Arztsuche- und -bewertungsportal „Jameda". Auf dieser Webseite werden Profile zu Arztpraxen angezeigt. Diese enthalten einerseits Basisangaben wie Name, Fachrichtung und Praxisanschrift. Andererseits können Patienten zu diesen Ärzten ihre subjektiven Erfahrungen mit der Community teilen, indem sie die Ärzte benoten und Freitextbewertungen auf der Plattform abgeben. Jameda selbst erstellt diese Profile ohne Einwilligung der betroffenen Ärzte. Neben solchen Basisprofilen bietet Jameda ein Upgrade der Profile gegen Bezahlung für Premiumkunden an. Das ermöglicht es den Ärzten, das Profil um ein Bild und weitere Informationen zu ergänzen, eine bessere Auffindbarkeit über Google sowie das Erscheinen des Profils in einer Liste von Anzeigen, die auch als solche gekennzeichnet ist.

Nachdem die klagende Augenärztin in einer Bewertung als „arrogant, unfreundlich, unprofessionell" bezeichnet wurde, klagte sie auf die Löschung des für sie erstellten Jameda-Profils. Der BGH sah jedoch keinen Löschungsgrund nach der DSGVO und wies die Revision daher zurück. Mustergültig prüft der BGH dafür, ob die Erstellung und Unterhaltung des Basisprofils durch Jameda eine rechtmäßige Verarbeitung aus berechtigten Interessen gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO darstellt. Für die hier erforderliche Abwägung ist die Charta der Grundrechte der Europäischen Union (GRCh) maßgeblich. Für den Betrieb des Portals spräche Art. 11 Abs. 1 GRCh – die Meinungs- und Informationsfreiheit. Jameda stelle

eine grundsätzlich von der Rechtsordnung gebilligte und gesellschaftlich erwünschte Informationsquelle über Arztangebote und die Erfahrungen mit diesen dar. Zudem spricht für Jameda – und dies ist in der Praxis auch auf eine Vielzahl anderer Fälle übertragbar – die unternehmerische Freiheit (Art. 16 GRCh).

Dass personenbezogenen Daten – hier die Basisdaten der Ärzte – dort eingepflegt werden, sei auch „erforderlich", um diese Interessen der Plattformbetreiberin und der Nutzer zu erreichen. Ohne, dass die einzelnen Ärzte identifiziert und gefunden werden können und dabei eine möglichst umfassende Übersicht erstellt wird, könne der Zweck der Plattform nicht erreicht werden.

Aufseiten der Ärztin stritten hingegen der Schutz ihrer personenbezogenen Daten (Art. 8 GRCh), die Achtung ihres sozialen und beruflichen Geltungsanspruchs (Art. 7 GRCh) und ihre unternehmerische Freiheit (Art. 16 GRCh). Zwar könnten die Bewertungen auf der Plattform eine erhebliche Auswirkung auf den beruflichen und wirtschaftlichen Erfolg der Ärztin haben, jedoch sei ein jeder beruflich selbständig Tätiger der dauerhaften Beobachtung seiner Arbeit durch die Öffentlichkeit und möglicher Kritik ausgesetzt. Diese Situation werde nicht erst durch diese Plattform erzeugt. Das öffentliche Interesse an einer verbesserten Leistungstransparenz im Gesundheitswesen überwiege somit die Interessen der Ärztin. Die Erstellung und Unterhaltung eines Ärzteprofils mit Basisdaten sei somit rechtmäßig im Sinne der DSGVO. Auch hier ergeben sich für die Praxis wesentliche Hinweise: Berufsbezogene Daten stehen regelmäßig in der Öffentlichkeit und genießen im Rahmen von Abwägungen wie hier unter Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO tendenziell einen geringeren Schutz als private oder gar intime Angaben.

Im Rahmen dieser Abwägung war auch relevant, dass Jameda als „neutrale Informationsmittlerin" auftritt. Durch die Differenzierung zwischen Basis- und Premiumprofil wird kein unsachlicher Eindruck erweckt, Premiumkunden seien „die besseren Ärzte". Eine absolute Gleichbehandlung ist nicht erforderlich.

Zweckbindung und Speicherbegrenzung: Grundlegendes zu den maßgeblichen Grundsätzen

In einem aktuell vor dem EuGH anhängigen Verfahren hat sich jüngst der Generalanwalt zu den maßgeblichen Datenschutzgrundsätzen der Zweckbindung und Speicherbegrenzung geäußert. Die wesentlichsten Aussagen fassen wir Ihnen zusammen.

Ein Unternehmen („Digi“) kopiert Kundendaten im Rahmen der Behebung technischer Serverprobleme auf einen internen Datenträger und lässt sie auch nach Behebung des Problems dort gespeichert. Darin sahen die ungarischen Behörden einen Verstoß gegen Art. 5 DSGVO und verhängten ein Bußgeld. Digi klagte, worauf das entscheidende Gericht dem EuGH Fragen zur Auslegung der Grundsätze von Zweckbindung und Speicherbegrenzung aus Art. 5 Abs. 1 lit. b und lit. e DSGVO vorlegte. In diesem Verfahren wurden jetzt die Schlussanträge des Generalanwalts veröffentlicht. In den allermeisten Fällen folgt der EuGH den Schlussanträgen.

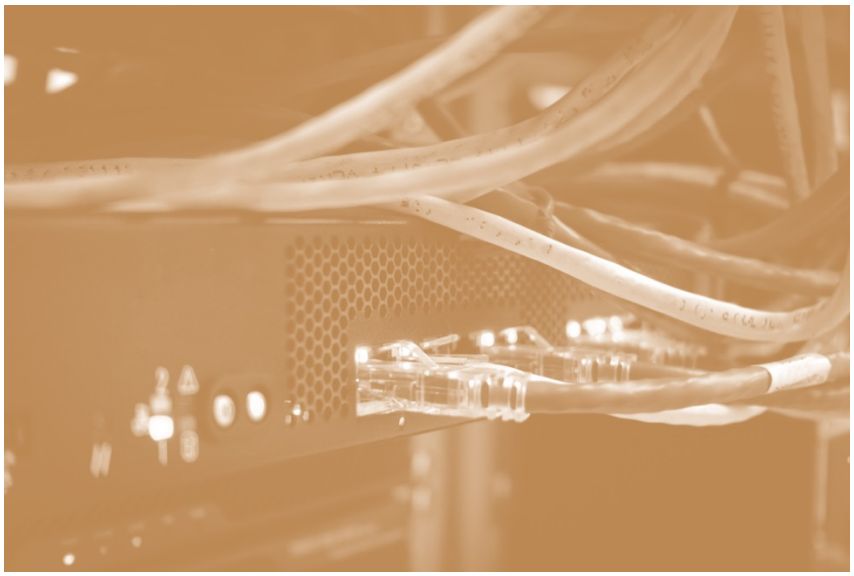
Der Generalanwalt stellt fest, dass es zwei verschiedene Aspekte zu betrachten gibt: In einem ersten Schritt die Frage der Rechtmäßigkeit der Speicherung der Daten in der „Testdatenbank“. Dabei gehe es um den Grundsatz der Zweckbindung. In einem zweiten Schritt dann die zeitliche Fortführung dieser Datenbank nach Behebung der technischen Störung, also die Frage, *wann* die Speicherung der Daten auf einem zusätzlichen Datenträger in zeitlicher Hinsicht nicht mehr

gerechtfertigt war. Hier greife ausschließlich der Grundsatz der Speicherbegrenzung.

Die Verarbeitung in der „Testdatenbank“ diente nach Ansicht des Generalanwalts ausschließlich dem spezifischen Zweck der vorübergehenden Sicherung der Abonnentendaten im Zusammenhang mit der Störungsbehebung und damit einem Zweck, der sich von dem der ursprünglichen Datenerhebung unterscheidet. Beide Zwecke seien aber i.S.d. Art. 6 Abs. 4 DSGVO miteinander kompatibel: Die Weiterverarbeitung diente gerade der Behebung einer technischen Störung und damit letztlich der Erbringung der eigentlichen Dienstleistung. Dies entspreche auch den legitimen Erwartungen der Abonnenten. Die Speicherung in der Testdatenbank verstößt damit im Ergebnis nach Ansicht des Generalanwalts nicht gegen den Grundsatz der Zweckbindung.

Kritik übt der Generalanwalt aber an der Dauer der Speicherung: Da der primäre Zweck hier in der Sicherung der Daten in Zusammenhang mit der Behebung der technischen Störung lag, verlor die Speicherung mit Behebung der Fehlfunktion ihre Legitimation. Nicht ganz unerheblich: Das Unternehmen hatte selbst eingestanden, die Datenbank nach Behebung des Fehlers versehentlich nicht gelöscht zu haben.

Für die Praxis hilft die Entscheidung: Testdatenbanken und anderweitige Sicherungskopien sind zulässig, solange sie für die Aufrechterhaltung oder Wiederherstellung der eigentlich geschuldeten Dienste benötigt werden. Ist dieser Zweck erreicht, müssen die (redundanten) Daten unverzüglich gelöscht werden.



Data Act: Von der Datenbereitstellung, fairen Vertragsregelungen und Interoperabilität

Ein Datengesetz: Die EU-Kommission hat Ende Februar 2022 den Entwurf eines „Data Act" vorgelegt. Dahinter verbirgt sich der Vorschlag für eine EU-Verordnung über harmonisierte Vorschriften für einen fairen Zugang zu Daten und deren Nutzung. Als EU-Verordnung werden die neuen Vorgaben nach Inkrafttreten in allen EU-Mitgliedstaaten unmittelbar gelten. Es wird also kein nationales Umsetzungsgesetz benötigt, Unternehmen und öffentliche Stellen werden die Vorschriften 12 Monate nach der Veröffentlichung im Amtsblatt ohne weiteres einhalten und umsetzen müssen.

Der Data Act soll künftig neue Maßstäbe für den Zugang zu, die Bereitstellung von und die Nutzung von in der EU erzeugten Daten setzen. Ziel ist es, zu einer fairen, innovativen und effizienten digitalen Wirtschaft in der EU beizutragen. Der Zugang zu vorhandenen (Industrie-)Daten soll erleichtert werden, Rechtssicherheit soll Vertrauen in die gemeinsame Nutzung von Daten fördern und der Abbau von technischen Hindernissen soll den Weg zu einer interoperablen und agilen Datenwirtschaft bereiten.

Die Regelungen sind umfangreich und weitreichend. Sie betreffen verschiedene Bereiche der digitalen Wirtschaft und eine Vielzahl unterschiedlicher Akteure, insbesondere Hersteller von smarten, vernetzten Produkten. Ihre Umsetzung wird erheblichen

Umsetzungsaufwand mit sich bringen, aber auch Chancen bieten, etwa neue Geschäftsmodelle ermöglichen.

Bis zum Inkrafttreten des Data Act werden noch einige Diskussionen geführt werden: Mit dem jetzt vorliegenden Entwurf ist der erste Schritt getan, die EU-Kommission hat ihre Position kundgetan. Es folgt nun das Verordnungsgebungsverfahren mit Einbindung von Rat und Parlament. Der Data Act war bereits vor Veröffentlichung seines ersten Entwurfs derart intensiv diskutiert, dass auch das nun anstehende Verordnungsgebungsverfahren kontrovers zu werden verspricht.

Umso bedeutender ist es angesichts dessen, schon von Beginn an die weitreichenden Vorschläge im Blick zu halten, auf die Weiterentwicklung Einfluss zu nehmen und Geschäftsmodelle frühzeitig auf das auszurichten, was aus Brüssel kommen dürfte.

Der Data Act umfasst 7 Fokusthemen mit den folgenden Schwerpunkten:

- **Zugangsrechte zu Daten: Nutzung der von einem Produkt oder Dienst erzeugten (Meta-)Informationen (Kapitel II – Art. 3 bis 7)**

  Bei der Nutzung eines vernetzten Produkts oder eines damit verbundenen Dienstes werden regelmäßig Daten erzeugt, gesammelt oder empfangen. Jedem Nutzer eines solchen Produkts oder Dienstes soll es künftig möglich sein, auf diese Daten zuzugreifen oder Zugang zu ihnen zu erhalten. Der Nutzer soll entscheiden können, ob und in welchem Umfang Dritte Zugang zu diesen Daten erhalten und zu welchen Zwecken und unter welchen Bedingungen sie diese nutzen dürfen.

  Kapitel II ist damit eines der Herzstücke des neuen Data Act und womöglich das weitreichendste Kapitel für alle Anbieter von vernetzten Produkten und Diensten: Anbieter müssen ihre Produkte für die Nutzer öffnen und u.a. Metadaten umfassend bereitstellen. Dies bringt nicht nur technische Herausforderungen mit sich, sondern wird auch ganz erhebliche kommerzielle Auswirkungen auf die Produktentwicklung haben.

- **Pflichten, Daten Dritten bereit zu stellen (Kapitel III – Art. 8 bis 12)**

  Wenn ein Gesetz den Zugang zu Daten normiert, wie etwa Kapitel II des Data Act, dann sind die Regelungen dieses Kapitels III ergänzend zu beachten: Die Bereitstellung von Daten an professionelle Datenempfänger (nicht die Produktnutzer) muss zu fairen Bedingungen und transparent erfolgen, eine etwaig verlangte Gegenleistung muss angemessen sein.

- **Pflichten, Daten öffentlichen Stellen bereit zu stellen (Kapitel V – Art. 14 bis 22)**

  Für die Bewältigung öffentlicher Notfälle und sogar – wenn es „anders nicht geht" – für die Erfüllung öffentlicher Aufgaben können künftig öffentliche Stellen bei Unternehmen Daten in verhältnismäßigem Umfang anfordern. Unternehmen müssen diese Daten dann entsprechend der Anforderung bereitstellen.

- **Vertragsgestaltung: Verbot missbräuchlicher Klauseln beim Zugang zu Daten und deren Durchsetzung und Mustervertragsklauseln der EU-Kommission (Kapitel IV – Art. 13 und Art. 34)**

  Vertragliche Vereinbarungen über den Zugang zu Daten und ihre Nutzung, die Haftung und Rechtsbehelfe bei der Verletzung oder Beendigung von Vereinbarungen sind zentral für die kommerzielle Bewertung von Datengeschäften. Bei Verträgen mit kleinen und mittleren Unternehmen werden diese Klauseln künftig besonders geprüft: Sind derartige Klauseln missbräuchlich, entfalten sie keine Wirksamkeit.

  Missbräuchlich ist insbesondere all das, was „in grober Weise" von der guten Geschäftspraxis abweicht, gegen Treu und Glauben und gegen die guten Sitten verstößt. Hierzu wird die EU-Kommission ergänzend Mustervertragsklauseln vorlegen.

- **Wechsel zwischen Datenverarbeitungsdiensten: Datenportabilität (Kapitel VI – Art. 23 bis 26)**

  Auch an einer weiteren Stelle sagt die EU-Kommission mit dem Data Act exklusiven Geschäftsvorteilen und LogIn-Effekten den Kampf an: Anbieter von

Datenverarbeitungsdiensten, also etwa Cloud-Anbieter, müssen künftig sicherstellen, dass Kunden zu einem anderen Datenverarbeitungsdienst wechseln können. Kommerzielle, technische, vertragliche und organisatorische Vorkehrungen, die die Kunden daran hindern, müssen beseitigt werden.

In der Praxis muss mithin insbesondere die Datenmigration danach deutlich und flächendeckend erleichtert werden. Der Data Act enthält dazu eine Reihe detaillierter Vorgaben. So müssen u.a. etwa Daten, Anwendungen und digitale Bestände migriert werden mit einer Übergangsfrist von maximal 30 Tagen, der Umstellungsprozess muss vom bisherigen Anbieter unterstützt und, soweit technisch machbar, abgeschlossen werden, die uneingeschränkte Kontinuität bei der Bereitstellung der betreffenden Funktionen oder Dienste muss gewährleistet werden. Welche Gegenleistung der migrierende bisherige Anbieter dafür verlangen darf, ist vom Data Act ebenfalls reguliert und wird perspektivisch auf Null abgesenkt.

- **Internationaler Transfer nicht-personenbezogener Daten (Kapitel VII – Art. 27)**

  Anbieter von Datenverarbeitungsdiensten haben auch für nicht-personenbezogene Daten künftig angemessene technische, rechtliche und organisatorische Maßnahmen zu treffen, um die internationale Übermittlung oder den staatlichen Zugriff auf in der Union gespeicherte Daten (von außerhalb) zu verhindern, wenn eine solche Übermittlung oder ein solcher Zugriff zu einem Konflikt mit dem Unionsrecht oder dem nationalen Recht des betreffenden Mitgliedstaats führen würde. Auch für nicht-personenbezogene Daten kommt damit eine (gegenüber der DSGVO abgeschwächte) Schutzpflicht der Daten bei Berührungen mit Gebieten außerhalb der EU zustande.

- **Interoperabilität (Kapitel VIII – Art. 28 bis 30)**

  Ein „Binnenmarkt der Daten“, das grundlegende Ziel der EU-Digitalstrategie, ist umso besser erreichbar, umso einfacher Daten gehandelt, ausgetauscht und gegenseitig genutzt werden können. Die Pflicht zur Herstellung einer verbesserten

Interoperabilität wird so zum Rückgrat der EU-Digitalstrategie.

Im Data Act markieren die Pflichten zur Verbesserung der Interoperabilität das letzte inhaltliche Kapitel. Es widmet sich drei wesentlichen Bereichen:

Betreiber von Datenräumen müssen grundlegende Interoperabilitätsanforderungen erfüllen, u.a. den Inhalt der Datensätze, Nutzungsbeschränkungen, Lizenzen etc. ausreichend beschreiben, damit der Empfänger die Daten finden, darauf zugreifen und sie nutzen kann.

Datenverarbeitungsdienste müssen bestimmte Spezifikationen einhalten und u.a. die Übertragbarkeit digitaler Bestände zwischen verschiedenen Datenverarbeitungsdiensten, die denselben Diensttyp abdecken, verbessern.

Intelligente Verträge (smart contracts) müssen ebenfalls bestimmte Anforderungen einhalten, u.a. so konzipiert sein, dass eine Manipulation durch Dritte ausgeschlossen ist oder eine Datenarchivierung der Transaktionsdaten, der Logik und des Codes des intelligenten Vertrags vorgesehen ist, um die Aufzeichnung der in der Vergangenheit an den Daten durchgeführten Operationen abzubilden.

Geltungsbereich und Verhältnis zu anderen Rechtsvorschriften

Gelten wird die Verordnung nach dem aktuellen Entwurf (Art. 1) für

- Hersteller und Nutzer von Produkten und Dienstleistungen, mit denen Daten erzeugt, bereitgestellt oder genutzt werden
- Dateninhaber und Datenempfänger in der EU
- Öffentliche Stellen, die Daten für die Wahrnehmung einer Aufgabe im öffentlichen Interesse benötigen und die Dateninhaber, die solche Daten zur Verfügung stellen können bzw. sollen
- Anbieter von Datenverarbeitungsdiensten in der EU

An verschiedenen Stellen privilegiert der Data Act KMU, also kleine und mittlere Unternehmen, etwa bei der Datenbereitstellung

(angemessene Gegenleistung nur bei reiner Kostendeckung) und den Vertragsklauseln (spezifische Missbrauchskontrolle).

Neben dem Data Act bleiben die DSGVO und ePrivacy-Richtlinie unberührt. Der Data Act ergänzt die bestehenden Regelungen, schränkt diese aber nicht ein und modifiziert sie auch nicht.

Durchsetzung und Bußgelder

Die Durchsetzung der neuen Verordnung ist von den Mitgliedstaaten jeweils einer oder mehreren Behörden aufzugeben, wobei die Überwachung mit Blick auf personenbezogene Daten den Datenschutzaufsichtsbehörden obliegen wird. Die betrauten Behörden müssen mit ausreichenden Instrumenten und Durchsetzungskraft ausgestattet werden.

Die Behörden werden auch als Beschwerdestelle dienen und sollen die Befugnis erhalten, von den jeweiligen Mitgliedstaaten noch festzulegende Bußgelder zu erlassen. Geht es um Verstöße gegen die Verarbeitung personenbezogener Daten, sollen die Bußgeldvorschriften der DSGVO Anwendung finden mit Bußgeldern von bis zu 4 % des Jahresgruppenumsatzes bzw. 20 Mio. Euro.

Ausblick

Der Entwurf des Data Act ist ein weiterer großer Wurf der EU-Kommission. Im Rahmen ihrer Digitalstrategie zielt diese darauf, die Maßstäbe zu setzen für die künftige Regulierung der „digital economy". Der Data Act reiht sich insofern ein in die wachsende Liste relevanter Entwürfe, insbesondere der KI-Verordnung, aber auch dem Data Markets Act oder dem Data Governance Act.

Mit dem Data Act steigt die EU nun erstmals in die Regulierung des eigentlichen Datengeschäfts ein und begrenzt ihre Vorgaben nicht, wie bisher, auf Spezialbereiche (KI), marktstarke Player wie Amazon, Apple, Google oder Facebook (Meta) und ähnliche Akteure (Digital Markets Act) oder die öffentliche Hand (Data Governance Act).

Der Data Act erstreckt sich als horizontale Regulierung auf alle Sektoren und alle Akteure im Datengeschäft. Er wird sich, so meine ganz subjektive Erwartung, zu der zentralen Regelung für alle digitalen Angebote neben dem Digitalen Vertragsrecht, der DSGVO und der ePrivacy-Regulierung entwickeln.

Vertiefungen zu den Regelungsbereichen des Data Act finden Sie in unserem Blog unter www.digitalisierungsrecht.eu.

Zu guter Letzt

Auch in den letzten Wochen wurden einige berichtenswerte Bußgelder in der EU verhängt: Ein Bußgeld in Millionenhöhe für ein polnisches Unternehmen wegen Unachtsamkeit beim Systemupdate, mehrere hunderttausend für den Brüsseler Flughafen wegen unzulässiger Temperaturkontrollen durch Wärmebildkameras und 20 Mio. Euro gegen Clearview AI wegen der unrechtmäßigen Verwendung tausender Gesichtsbilder zur Strafverfolgung. Für alle Online-Shops ist die neue DSK-Position zu beachten: Gastbestellungen müssen i.d.R. möglich sein.

- **Unzureichende Sicherheitsmaßnahmen in Polen: 1 Mio. Euro Bußgeld**

Fortum Marketing and Sales Polska S.A. („Fortum“) wurde mit einem Bußgeld in Höhe von ca. 1 Mio. Euro durch die polnische Datenschutzbehörde belastet, aufgrund fehlender angemessener technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit. Der eingebundene Auftragsverarbeiter erhielt ebenfalls ein Bußgeld (in Höhe von rund 55.000 Euro).

Bei einer Systemänderung wurde eine Kundendatenbank des Unternehmens Fortum und durch Unbefugte kopiert. Dies war möglich, da der Server nicht über ordnungsgemäß konfigurierte

Sicherheitsmaßnahmen verfügte. Bekannt wurde die Sicherheitslücke erst durch Internetnutzer, die ungesicherte Zugriffsmöglichkeiten meldeten.

- **Gesichtserkennung in der Strafverfolgung: 20 Mio. Euro für Clearview AI in Italien**

Die italienische Datenschutzbehörde belegte das Unternehmen Clearview AI mit einem Bußgeld von 20 Mio. Euro aufgrund einer Datenschutzverletzung beim Einsatz ihrer viel kritisierten Gesichtserkennungstechnologie. Die Software für Gesichtserkennung des Unternehmens, welche ihre Dienste unter anderem zur Strafverfolgung für Behörden der USA anbietet, war im Besitz von über 10 Milliarden Gesichtsbilder. Das Problem hieran: Clearview AI zog diese Bilder aus dem Internet, insbesondere aus Social Media Accounts.

Diese Vorgehensweise sei indes in der EU rechtswidrig und nicht mit der DSGVO in Einklang zu bringen, so die italienische Aufsichtsbehörde. Dies gilt auch dann, wenn eine Nutzung nur in den USA erfolgt: Die DSGVO greift, wenn Daten von EU-Bürger derart erhoben werden. Neben dem hohen Bußgeld ordnete die italienische Datenschutzbehörde die Löschung der entsprechenden Bilder an.

- **Unrechtmäßiger Einsatz von Wärmebildkameras kostet Flughafen in Belgien 100.000 Euro**

Die belgische Datenschutzbehörde verhängte ein Bußgeld in Höhe von 100.000 Euro gegen den Flughafen Brüssel-Süd-Charleroi wegen der Durchführung von Temperaturkontrollen mit Wärmebildkameras bei Fluggästen ohne gültige Rechtsgrundlage, ohne die gebotene Unterrichtung der betroffenen Personen und ohne eine angemessene Datenschutz-Folgenabschätzung. Bei allen Fluggästen, bei denen mittels der Kamera eine Temperatur von mehr als 38 °C festgestellt wurde, erfolgte erneut eine manuelle Messung der Temperatur. Passagiere, bei denen dadurch der Verdacht auf eine COVID-19-Infektion bestand, wurden aufgefordert, den Flughafen zu verlassen und durften nicht an Bord gehen.

- **Knapp 500.000 Euro wegen zu später Meldung einer Datenschutzverletzung (und unzureichender Datensicherheit)**

Die irische Datenschutzbehörde verhängte gegen die Bank of Ireland („BOI“) ein Bußgeld in Höhe von knapp 500.000 Euro, weil sie eine Datenschutzverletzung nicht rechtzeitig gemeldet und keine hinreichenden technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit personenbezogener Daten ergriffen hatte.

Ungenaue Kundendaten im Zentralen Kreditregister führten dazu, dass ein falsches Bild bezüglich der Finanzen und Kredite von Kunden der BOI entstand. Diese Fehlermeldung hätte unverzüglich erfolgen müssen, zudem versäumte die BOI es, angemessene Kontrollen zur Sicherung der Qualität und Validierungsverfahren einzusetzen.

- **Unzureichende Informationen der Klarna Bank: über 700.000 Euro in Schweden**

Die schwedische Datenschutzbehörde verhängte gegen die Klarna Bank ein Bußgeld in Höhe von rund 730.000 Euro, weil sie betroffene Personen nicht angemessen über ihre Verarbeitungstätigkeiten informiert hatte.

Klarna Bank hatte es beispielsweise versäumt, Informationen über die Länder außerhalb des EWR zur Verfügung zu stellen, in die personenbezogene Daten übermittelt werden. Zudem stellte Klarna Bank nur unvollständige Informationen über die Zeiträume, für die personenbezogene Daten aufbewahrt werden, und die Kriterien für deren Festlegung bereit.

- **Gastbestellungen im Online-Shop**

Die DSK hat sich in einem jüngst veröffentlichten Beschluss zur Gestaltung von Kundenkonten in Online-Shops geäußert: Nach ihrer Ansicht darf keine Registrierungspflicht bestehen, Kunden müssen auch über einen sog. Gastzugang Waren und Dienstleistungen bestellen können. Wenn Informationen aus einem Kundenkonto zu werblichen Zwecken verwendet werden sollen, ist dafür eine (gesonderte) Einwilligung notwendig.

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

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

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

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

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

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