LOSCHELDER

Newsletter Datenschutzrecht

Juni 2022

Sehr geehrte Damen und Herren,

von wegen Sommerloch: Wir melden wir uns mit einem für die Praxis höchst relevanten Thema: Der Europäische Datenschutzausschuss (EDSA) hat seine Leitlinien zur Bußgeldbemessung veröffentlicht. In unserem ersten Beitrag erläutern wir, ob jetzt niedrigere oder gar höhere Strafen bei einem Verstoß gegen Datenschutzvorschriften zu erwarten sind.

Außerdem informiert Sie unser Juni-Newsletter über erste aufsichtsbehördliche Prüfungen von Facebook-Fanpages, interessante Neuigkeiten zum Auskunftsrecht aus Luxemburg und den jüngst verabschiedeten Data Governance Act, bevor wir – wie gewohnt – im zu guter Letzt wichtige und erstaunliche Bußgeldentscheidungen erläutern.

Wir freuen uns über Ihr Interesse!

Inhalt

Neue Leitlinien des EDSA zur Berechnung von Bußgeldern

Der Europäische Datenschutzausschuss (EDSA) veröffentlichte am 12.05.2022 eine gemeinsame Methodik zur Berechnung von Bußgeldern bei Verstößen gegen die DSGVO. Das Konzept des EDSA soll zu einer weitgehenden Harmonisierung und Transparenz bei der Sanktionierungspraxis führen. Die neuen Leitlinien sollen auch das umstrittene (nationale) Bußgeldbemessungskonzept der deutschen Datenschutzkonferenz (DSK) von Oktober 2019 ablösen. Drohen jetzt höhere Bußgelder oder verringern die Leitlinien das Risiko?

Die Leitlinien des EDSA sehen eine fünfstufige Berechnungsmethodik für die Verhängung von Bußgeldern bei Verstößen nach der DSGVO vor:

1. Identifikation der unzulässigen Verarbeitungen und Prüfung, ob ein oder mehrere zu ahndende Verstöße vorliegen.

2. Einstufung der Schwere des Verstoßes bzw. der Verstöße nach Qualität und Dauer, der Kategorien betroffener Daten sowie anhand des Vorsatz- oder Fahrlässigkeitsgrades und Identifikation des Umsatzes der Unternehmensgruppe als Faktor für die Verhängung einer wirksamen, abschreckenden und verhältnismäßigen Geldbuße

    - Ausgangsbetrag: Bei der Berechnung der Geldbuße für Verstöße mit geringer Schwere liegt der Ausgangsbetrag für die weitere Berechnung auf einen Wert zwischen 0 und 10%, bei mittelschweren Verstößen zwischen 10% und 20% und bei schweren Verstößen zwischen 20% und 100% der in Art. 83 DSGVO geregelten Höchstbeträge (also bis zu 10 bzw. 20 Mio. Euro oder 2% bzw. 4% des Jahresumsatzes, je nachdem, welcher Betrag höher ist).

    - Korrektur: Abhängig davon, wie hoch der Umsatz eines Unternehmens ist, wird der Ausgangsbetrag korrigiert. Er beträgt 0,2% bis 50% des Ausgangsbetrags, je nach Jahresumsatz. Dieses Ergebnis wird „Grundbetrag“ genannt.

Durch die Korrektur wird der für kleinere Unternehmen ungleich abschreckendere Bußgeldrahmen der DSGVO korrigiert. Zur Erinnerung: Ein Bußgeld darf nach Art. 83 Abs. 5 DSGVO bis zu 10 bzw. 20 Mio. Euro oder 2% bzw. 4% des Jahresumsatzes betragen, je nachdem, welcher Betrag höher ist. Das bedeutet für ein kleines Unternehmen mit 500.000 Euro Jahresumsatz theoretisch, dass es ein Bußgeld bis zu 20 Mio. Euro erwarten kann, während ein Unternehmen mit einem Jahresumsatz von 500 Mio. Euro auch ein Bußgeld von maximal 20 Mio. Euro zu erwarten hat (4% von 500 Mio. = 20 Mio.). Diese Ungleichheit korrigiert das Bußgeldkonzept, indem von dem zunächst nur anhand der Schwere des Verstoßes errechneten Grundbetrag nochmal ein gewisser Prozentsatz abgezogen wird, abhängig davon, wie groß der Umsatz eines Unternehmens ist.

3. Identifikation von erschwerenden oder mildernden Umständen, auch im Zusammenhang mit dem früheren oder gegenwärtigen Verhalten des Verantwortlichen (z.B. Kooperation, Transparenz, ergriffene Gegenmaßnahmen), die den Grundbetrag aus Schritt 2 erhöhen oder verringern. Diese Erhöhungen oder Ermäßigungen werden nicht durch Prozentsätze im Voraus festgelegt, sondern die tatsächliche Bezifferung der Geldbuße wird von der Abwägung aller gesammelten Umstände des Einzelfalls abhängig gemacht. In den Beispielen des EDSA können so Erhöhungen oder Ermäßigungen nochmal im Bereich von 30-40% vorgenommen werden, ohne dass der EDSA auch noch größere Anpassungen ausschließen würde.

4. Ermittlung der gesetzlichen Höchstwerte, die keinesfalls überschritten werden dürfen

5. Einzelfallanalyse mit Verhältnismäßigkeitsprüfung

Zusammengefasst wird für die Berechnung eines Bußgeldes also zunächst ein Grundbetrag gebildet, der anhand der Schwere des Verstoßes und des Unternehmensumsatzes bestimmt wird (Schritte 1-2). Dieser Betrag kann anschließend aufgrund erschwerender oder mildernder Umstände angepasst werden (Schritt 3) und ist dann daraufhin zu überprüfen, dass die nach DSGVO festgelegten

Höchstwerte (10 bzw. 20 Mio. Euro oder – je nachdem, was höher ist – 2% bzw. 4% des Jahresgruppenumsatzes des vergangenen Jahres) nicht überschritten werden. Abschließend (Schritt 5) muss eine Einzelfallanalyse erfolgen, ob die erwogene Geldbuße verhältnismäßig ist.

Verbindlichkeit

Die EDSA Leitlinien sind weder für die nationalen Datenschutzaufsichtsbehörden, noch für Gerichte rechtsverbindlich. Sie dienen lediglich als Auslegungshilfe. In der Praxis haben die Leitlinien des EDSA allerdings erfahrungsgemäß erhebliche Auswirkungen auf Behördenentscheidungen.

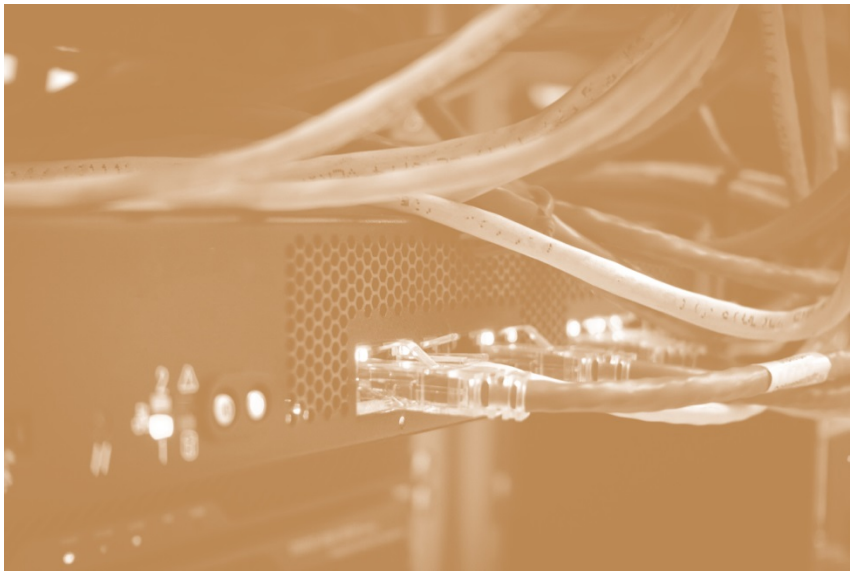
Drohen nun höhere oder geringere Bußgelder als nach dem Bemessungskonzept der DSK?

Einiges spricht dafür, dass die neuen Leitlinien das bisherige Bußgeldbemessungskonzept der DSK ersetzen. Dieses stand aufgrund seiner schematischen Herangehensweise ohnehin in der Kritik und hat ersten gerichtlichen Überprüfungen auch nicht standgehalten.

Müssen sich Unternehmen nun auf höhere oder niedrigere Strafen einstellen und inwiefern ist das Ganze kalkulierbar?

Der EDSA betont in der Einleitung des neuen Bußgeldkonzepts, dass die Bestimmung einer Geldbuße keine mathematische Aufgabe ist. Ganz vorhersehbar werden Geldbußen folglich auch in Zukunft nicht sein. Vergleicht man die Herangehensweise des EDSA-Konzeptes allerdings mit dem der DSK, fällt auf, dass die Grundbeträge für Bußgelder, die dann nochmals aufgrund erschwerender oder mildernder Umstände angepasst werden, erheblich geringer ausfallen. Ein Unternehmen mit einem Jahresumsatz von 500 Mio. Euro hätte bei einem schweren Verstoß nach dem DSK-Konzept einen Grundbetragsrahmen zwischen ca. 11,1 und 16,6 Mi. Euro zu befürchten. Nach dem EDSA-Konzept läge der Grundbetrag zwischen 2 und 10 Mio. Euro. Ein Unternehmen mit einem Jahresumsatz von 150 Mio. Euro hätte bei einem leichten Verstoß nach dem DSK-Konzept einen Grundbetragsrahmen von 416.000-1,664 Mio. Euro zu erwarten. Nach dem EDSA-Konzept läge der Rahmen für den Grundbetrag zwischen 0 und 400.000 Euro.

Anpassungen sind auch nach der Festlegung des Grundbetrags noch in beide Richtungen möglich (Schritt 3). Dennoch könnten die niedrigeren Grundbeträge nach dem EDSA-Konzept tendenziell auch zu niedrigeren Bußgeldern führen. Ob das am Ende allerdings so kommt und ob und wie die Regelungen des EDSA-Konzepts in der Praxis angewendet werden, bleibt abzuwarten. Bis zum 27. Juni können noch Stellungnahmen eingereicht werden und der EDSA daran anknüpfend noch Änderungen vornehmen.



Startschuss gefallen: Erste Prüfung von Facebook-Fanpages

Vielfach haben die Datenschutzaufsichtsbehörden in den letzten Monaten verlautbart, dass Facebook-Fanpages nicht datenschutzkonform betrieben werden könnten. Untersagungs- oder gar Bußgeldbescheide gab es jedoch keine. Zuletzt hatten die Behörden verkündet, nun erste Verfahren einleiten zu wollen, zunächst gegen öffentliche Stellen. Das ist jetzt der Fall: Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI) hat ein Verfahren gegen das Bundespresseamt (BPA) eröffnet, bezogen auf die vom BPA betriebene Facebook-Fanpage „Bundesregierung". Damit ist der Startschuss für eine Überprüfung öffentlicher und im Anschluss daran womöglich auch privater Facebook-Fanpages gefallen.

Die Datenschutzkonformität von Facebook-Fanpages bereitet den Aufsichtsbehörden schon seit längerer Zeit Schwierigkeiten. Im März dieses Jahrs stellte die „Taskforce Fanpages" in einem Kurzgutachten die regelmäßig fehlende Konformität solcher Seiten mit DSGVO und

TTDSG heraus (siehe dazu auch unser Newsletter vom Monat April 2022). Die Datenschutzkonferenz (DSK) beschloss daraufhin zu überprüfen, welche Landes- bzw. Bundesbehörden Facebook-Fanpages betreiben, um darauf hinzuwirken, dass diese Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können. Bei der aufsichtsbehördlichen Tätigkeit sollten dabei zunächst die von öffentlichen Stellen betriebenen Pages in den Blick genommen werden.

Die DSK forderte in ihrem Beschluss vom März 2022 von den jeweiligen Behörden insbesondere den Nachweis

- über den Abschluss einer Vereinbarung nach Art. 26 DSGVO über die gemeinsame Verantwortlichkeit mit Facebook
- ausreichende Informationen über die gemeinsamen Datenverarbeitungen gegenüber den die Fanpages Nutzenden gemäß Art. 13 DSGVO
- die Zulässigkeit zur Speicherung von Informationen in der Endeinrichtung des Endnutzers und der Zugriff auf diese Informationen gemäß § 25 TTDSG sowie
- die Zulässigkeit der Übertragung personenbezogener Daten in den Zugriffsbereich von Behörden in Drittstaaten.

Auch der BfDI hatte angekündigt, ab Januar 2022 die Nutzung von Facebook-Fanpages durch die in seinem Zuständigkeitsbereich liegenden Bundesbehörden auf ihre datenschutzrechtliche Zulässigkeit hin zu überprüfen. Hierzu ist nun der Startschuss gefallen, indem der BfDI, nach erfolglosen Gesprächen über die Zulässigkeit der vom BPA betriebenen Facebook-Fanpage „Bundesregierung“, ein Anhörungsschreiben an dieses versendete.

Die Anhörung durch den BfDI ist der erste Schritt in einem förmlichen Aufsichtsverfahren. Der Ausgang des Verfahrens bleibt abzuwarten. Nach den bisherigen Ausführungen der Aufsichtsbehörden dürfte allerdings einiges dafürsprechen, dass eine gerichtliche Prüfung folgen könnte.

Nach der bisherigen Kommunikation der Aufsichtsbehörden soll das Vorgehen gegen öffentliche Stellen der erste Schritt sein. Private Unternehmen, die Facebook-Präsenzen unterhalten, sind daher gut

damit beraten, die Überprüfung öffentlicher Facebook-Fanpages und das weitere Verhalten der Behörden zu beobachten. Einiges spricht dafür, dass die Prüfung Facebook-Fanpages privater Unternehmen oder auch entsprechenden Präsenzen in anderen sozialen Medien folgen dürfte. Wir halten Sie über die weitere Entwicklung auf dem Laufenden.

Extensives Auskunftsrecht: Angabe der Empfänger personenbezogener Daten

Das Auskunftsrecht Betroffener nach Art. 15 DSGVO ist in seiner praktischen Bedeutung das wichtigste Betroffenenrecht der DSGVO. Sein Umfang ist nach wie vor in etlichen Details unklar und umstritten. Erste Verfahren zur Klärung liegen beim EuGH. Von dort kommt nun auch ein erster Hinweis auf das Verständnis dieses Rechts: Werden personenbezogene Daten offengelegt, muss Betroffenen jeder Empfänger genannt werden. Nur, wenn diese Angabe aus tatsächlichen Gründen unmöglich ist, soll es ausreichen, die Kategorien von Empfängern zu nennen.

Derzeit liegen eine Reihe von datenschutzrechtlich relevanten Verfahren zur Vorabentscheidung beim EuGH. Dies ist für die Konkretisierung der vielen unbestimmten Rechtsbegriffe in der DSGVO von erheblicher Bedeutung. In einem aus Österreich zum EuGH gelangten Verfahren geht es um die Reichweite des Auskunftsrechts, konkret: Muss Betroffenen, die Auskunft verlangen, konkret dargelegt werden, welchen Dritten ihre Daten

offengelegt wurden oder reicht es, wenn die Kategorie der Empfänger genannt werden, gegenüber denen eine Offenlegung erfolgte?

Die Frage bezieht sich auf Art. 15 Abs. 1 lit. c DSGVO. Danach haben Betroffene das Recht auf Auskunft „die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden …". In der Praxis macht es ganz erhebliche Unterschiede, ob die Empfänger oder „nur" die Kategorien benannt werden; muss im ersten Fall doch eine womöglich umfassende Liste mit Einzelangaben zu den juristischen und natürlichen Personen angefertigt und überlassen werden, die Daten vom Betroffenen erhalten haben, während die Angabe der Kategorie von Empfängern (z.B. „Kunden", „Social Media Anbieter") mit deutlich weniger Aufwand und einem deutlich geringerem Risiko einer Verletzung von Rechten der Dritten erfolgen kann.

In Luxemburg hat nun der Generalanwalt am 09.06.2022 seine Position in den Schlussanträgen zum Verfahren veröffentlicht (C-154/21 – RW gegen Österreichische Post). Diese Schlussanträge binden das Gericht nicht. In den weit überwiegenden Fällen folg der EuGH aber den Schlussanträgen des Generalanwalts. Grund genug, schon diese in den Blick zu nehmen.

Und, um dies gleich vorweg zu nehmen: Der Generalanwalt vertritt eine weite Auslegung des Auskunftsrechts. Er stärkt die Rechte der Betroffenen und verschärft die auf den Unternehmen liegende Last, Auskunftsrechte ordnungsgemäß zu erfüllen. Nach seiner Auffassung müssen immer die einzelnen Empfänger genannt werden, wenn ein Betroffener dies wünscht. Davon abgesehen werden könne nur, wenn dies tatsächlich unmöglich ist oder das Auskunftsbegehren offensichtlich unbegründet oder exzessiv ist.

Tatsächlich unmöglich sei die Angabe etwa, wenn die Empfänger z. B. tatsächlich noch nicht identifiziert wurden, weil eine Offenlegung erst künftig erfolgen soll (es könne vom Verantwortlichen zweifellos nicht verlangt werden, dass er Informationen mitteilt, die noch nicht vorliegen). In diesem Fall müssten nur die Kategorien von Empfängern angegeben werden. Von offensichtlich unbegründeten oder exzessiven Anträgen kann nach der bisherigen Positionierung der Behörden und Gerichte nur

in absoluten Ausnahmefällen ausgegangen werden; die aktuellen Schlussanträge bringen dazu keine neuen Erkenntnisse.

Die wichtigsten Aussagen des Generalanwalts dazu in aller Kürze:

- Die Struktur des Auskunftsrechts lege es nahe, dass Betroffene ein Wahlrecht haben, ob sie die Empfänger erfahren wollen oder „nur" die Kategorien von Empfängern.

- Ein Recht, die individuellen Empfänger zu erfahren, würde auch dem Zweck des Auskunftsrechts am besten gerecht: Nach den Erwägungsgründen hätten Betroffene ein Anrecht darauf, zu erfahren, wer Empfänger ihrer personenbezogenen Daten sind (EG 63 DSGVO). Gerade dies würde ein hohes Datenschutzniveau gewährleisten.

- Würde es ausreichen, die Kategorien von Empfängern zu nennen, würde dies bedeuten, dass der betroffenen Person die Möglichkeit genommen würde, in vollem Umfang die Rechtmäßigkeit der vom Verantwortlichen vorgenommenen Verarbeitung und insbesondere die Rechtmäßigkeit der bereits erfolgten Offenlegungen von Daten überprüfen zu können. Die Information sei auch erforderlich, um weitere Rechte, etwa auf Berichtigung oder Löschung, wirksam geltend zu machen.

Für die Praxis bedeutet dies: Im Zweifel sind Auskünfte umfassender zu erteilen. Rechte Dritter (hier der Empfänger personenbezogener Daten) dürfen dabei aber nicht aus dem Blick geraten. Verantwortliche stehen daher einmal mehr der Herausforderung gegenüber, die korrekte Abwägung widerstreitender Interessen zu finden. In jedem Fall sollte geprüft werden, ob die Auskunftsprozesse anzupassen sind.

Data Governance-Act veröffentlicht

Die EU verwirklicht ihre Digitalstrategie in großen Schritten. Anfang Juni ist ein Element der sog. Datenstrategie, der Data Governance Act (DGA) im Amtsblatt veröffentlicht worden. Er tritt damit in wenigen Tagen in Kraft, seine einzelnen Rechte und Pflichten entfaltet er ab Herbst 2023 unmittelbar in allen EU-Mitgliedstaaten. Wir haben Ihnen zusammengestellt, was der DGA für die Datenwirtschaft in der EU bringt.

Wie effizient Daten in Europa für die Gesellschaft nutzbar gemacht werden können und ob die EU künftig eine führende Rolle in der Datenwirtschaft haben wird, hängt maßgeblich von einem konsistenten Rechtsrahmen ab, der Privatsphäre und Vertraulichkeit von Daten schützt, ohne ihr Potential ungenutzt zu lassen. Den Weg zu einer starken, florierenden europäischen Datenwirtschaft soll die Anfang 2020 veröffentlichte EU-Datenstrategie weisen. Wichtige Wegpunkte der Strategie sind der seit Februar 2022 im Entwurf vorliegende Data Act (DA) und eben der jüngst veröffentlichte Data Governance Act (DGA; ABl. EU L 152/1).

Als Verordnung (EU) 2022/868 wird der DGA ab dem 24.09.2023 unmittelbar in jedem Mitgliedsstaat der EU gelten. Ab diesem Zeitpunkt werden Unternehmen und öffentliche Stellen die neuen Rechte und Pflichten beachten müssen, die der DGA mit sich bringt. Öffentliche Stellen sollten sich frühzeitig auf die neuen Pflichten einstellen. Unternehmen ist zu raten, zu prüfen, inwiefern die

Neuregelungen zur Verbesserung ihrer Produkte oder Dienste beitragen können.

Die Verordnung besteht im Wesentlichen aus vier Elementen, die Folgendes mit sich bringen:

- **Breitere, sichere Weiterverwendung von Daten im Besitz öffentlicher Stellen** (Kapitel II, Art. 3 bis 9 DGA)

  Der DGA beinhaltet **keine Bereitstellungspflicht** hinsichtlich in öffentlicher Hand befindlicher Daten. Ob öffentliche Stellen die Weiterverwendung von Daten, die sich in ihrem Besitz befinden, erlauben können oder müssen, richtet sich nach dem Recht des jeweiligen Mitgliedsstaats.

  Stellt die öffentliche Hand jedoch Daten bestimmter Datenkategorien zur Weiterverwendung bereit, ist ab Herbst 2023 ein neuer rechtlicher Rahmen zu beachten, der eine faire und umfassende Nutzung dieser Daten für alle Interessierten absichern soll, zu kommerziellen und nichtkommerziellen Zwecken.

  Dafür gelten folgende Vorgaben:

  - **Ausschließlichkeitsvereinbarungen** können, wenn überhaupt, nur noch unter engen Voraussetzungen geschlossen werden, bestehende Ausschließlichkeitsvereinbarungen laufen aus.

  - Der DGA schreibt **Bedingungen für die Erlaubnis der Weiterverwendung** vor. Diese sollen sowohl die Interessierten, als auch die von den Daten betroffenen Personen schützen.

    So sollen etwa technische Maßnahmen absichern, dass Daten weiterhin geschützt sind. Darüber hinaus unterliegen Weiterverwender **Mitteilungs-, Unterrichtungs- und Unterstützungspflichten** im Hinblick auf Datenschutzverletzungen und unbefugte Weiterverwendung nicht personenbezogener Daten. Die Rechte des geistigen Eigentums und die Vertraulichkeit der Daten sind jederzeit zu wahren. Alle Bedingungen müssen bei einer **zentralen Informationsstelle** abrufbar sein.

- Öffentliche Stellen dürfen für die Erlaubnis der Weiterverwendung der Daten (nur) **kostenorientierte Gebühren** erheben.

- **Förderung des Datenaustauschs durch Datenvermittlungsdienste** (Kapitel III, Art. 10 bis 15 DGA)

  Konzipiert als neues Geschäftsmodell sollen Datenvermittlungsdienste eine Umgebung bieten, in der Unternehmen und Einzelpersonen – jeweils als Dateninhaber oder als Datennutzer – einfach und sicher Daten miteinander austauschen können.

  Anbieter von Datenvermittlungsdiensten werden nach **Anmeldung in einem Register** eingetragen, dass sie als „in der Union anerkannter Anbieter von Datenvermittlungsdiensten" kenntlich macht. Dieses „Siegel" soll Vertrauen in diese Dienste schaffen, Interoperabilität fördern und zur freiwilligen gemeinsamen Datennutzung anregen. Der DGA normiert die Voraussetzungen, unter denen Datenvermittlungsdienste als solche anerkannt werden können. Eines der wesentlichsten Merkmale ist dabei die Neutralität in Bezug auf die vermittelten Daten – der Datenmittler darf mithin weder im Lager der Dateninhaber, noch der Datennutzer stehen.

  Datenvermittlungsdienste können unterschiedliche Gestalten haben. Sie können dem zwei- oder mehrseitigen Austausch von Daten dienen, als Plattformen oder als Datenbanken ausgestaltet sein oder die Akteure auf andere Art und Weise miteinander vernetzen, etwa Datenmarktplätze. Auch öffentliche Stellen können Datenvermittlungsdienste anbieten. Keine Datenvermittlungsdienste werden angeboten, wenn lediglich technische Werkzeuge bereitgestellt werden (z.B. Cloud-Speicher, Analysedienste), ohne dass darauf abgezielt wird, eine geschäftliche Beziehung zwischen Dateninhaber und Datennutzer herzustellen.

- **„Siegel des Vertrauens" für datenaltruistische Organisationen** (Kapitel IV, Art. 16 bis 25 DGA)

  Datenanalysen zu altruistischen Zwecken, etwa im Bereich medizinischer Forschung, bringen ein ganz erhebliches Potential. Indes fehlt es nach Ansicht der Kommission oft noch

an dem nötigen Vertrauen, dass die in Betracht kommende Einrichtung tatsächlich datenaltruistisch handelt. Folge ist, dass diesen weit weniger Daten bereitgestellt werden, als dies bei einem größeren Vertrauen der Fall wäre.

Der DGA bringt hier ein „Siegel" für derartige altruistische Datenorganisationen; die Mitgliedstaaten können allerdings frei entscheiden, ob sie dieses anbieten. Mit dem Siegel soll mehr Vertrauen geschaffen werden, um Unternehmen und Einzelpersonen zu mehr Datenspenden zu mobilisieren. Erfüllt eine Organisation die Eintragungsanforderungen und wahrt das Verfahren, wird sie – wenn die Mitgliedstaaten dieses einrichten – in ein nationales **Register** der anerkannten datenaltruistischen Organisationen eingetragen.

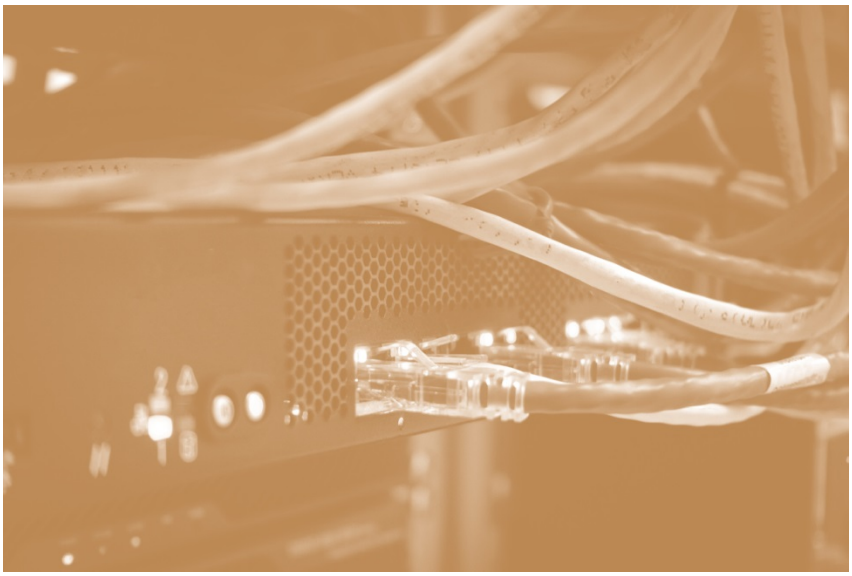
„Datenaltruistisch" handelt, wer freiwillig gemeinsam Daten auf Grundlage einer Einwilligung (bzgl. personenbezogener Daten) bzw. einer Erlaubnis (bzgl. nicht personenbezogener Daten), für Ziele von allgemeinem Interesse, beispielsweise der Gesundheitsfürsorge, der Bekämpfung des Klimawandels oder der Verbesserung der Mobilität, nutzt, ohne dafür ein Entgelt zu fordern oder zu erhalten (ausgenommen ist eine kostenorientierte Entschädigung).

Anerkannte datenaltruistische Organisationen müssen Transparenz- und Dokumentationsanforderungen erfüllen. Zum Schutz der Rechte und Interessen betroffener Personen und Dateninhaber sind sie u.a. verpflichtet, bestimmte Informationen bereitzustellen und ein angemessenes Sicherheitsniveau sicherzustellen. Künftig wird die Erhebung von Daten zu datenaltruistischen Zwecken durch ein einheitliches, europäisches **Einwilligungsformular für Datenaltruismus** erleichtert, welches die Kommission veröffentlichen wird.

- **Einrichtung eines Europäischen Dateninnovationsrat** (Kapitel VI, Art. 29 bis 30)

  Eine Expertengruppe aus Vertretern der unter dem DGA zuständigen und weiteren EU-Behörden wird als Europäischer Dateninnovationsrat beratend und unterstützend tätig sein, um die weitere Entwicklung der Data Governance voranzutreiben.

Auf den ersten Blick erscheint der DGA – jedenfalls im operativen Geschäft – unscheinbar. Die vorstehenden Regelungen enthalten indes ein erhebliches Potential, um die Datenwirtschaft in der EU anzukurbeln. Öffentliche Stellen sollten die neuen Pflichten im Blick haben und sich an die Implementierung begeben. Unternehmen dagegen sollten wachsamer analysieren, wo sie die Neuregelungen in ihrem Geschäft nutzen können, etwa durch die Nutzung von Daten öffentlicher Stellen oder erweiterte Analyseoptionen bei Einbindung von Datenmittlern.



Zu guter Letzt

Auch im letzten Monat gab es wieder einige spannende Entscheidungen zum Datenschutz: Allen voran eine der spanischen Datenschutzbehörde über ein 10-Millionen-Euro-Bußgeld für Google wegen der unbefugten Weitergabe von Daten an Dritte. Das Fahrtenvermittlungsunternehmen Uber musste über 4 Millionen Euro wegen DSGVO-Verstößen in 1,5 Millionen Fällen zahlen. Die italienische Datenschutzbehörde stellte außerdem fest, dass auch für die Verarbeitung unzugänglicher, verschlüsselter Daten auf den Servern von Unternehmen eine ausreichende Rechtsgrundlage vorhanden sein müsse.

- **Spanien: 10 Millionen Euro Bußgeld für Google**

Die spanische Datenschutzbehörde (AEPD) hat gegen Google LLC ein Bußgeld in Höhe von zehn Millionen Euro verhängt, da Daten an

Dritte ohne Rechtsgrundlage durch das Unternehmen weitergegeben wurden. Die AEPD sah darin einen Verstoß gegen die Art. 6 und Art. 17 DSGVO.

Die Daten über von Bürgern gestellte Anträge auf Entfernung von Inhalten wurden einschließlich ihrer Identifizierung, ihrer E-Mail-Adresse, der angegebenen Gründe und der URL von Google an das sog. Lumen-Projekt übermittelt. Dieses Projekt sammelt Löschanträge und veröffentlicht diese. Dem Nutzer der Google-Formulare wurde keine Möglichkeit gegeben, Widerspruch gegen die Übermittlung zu erheben. Es fehlt zudem an einer hinreichenden Transparenz im Lumen-Projekt.

Zusätzlich zum Bußgeld wurde Google aufgefordert, die Übermittlung von Daten an das Lumen-Projekt sowie die Möglichkeiten zur Ausübung von Betroffenenrechten mit der DSGVO in Einklang zu bringen.

- **Spanien: Unzulässige Löschung des Videomaterial einer Überwachungskamera bringen 170.000 Euro Bußgeld für MERCADONA S.A.**

Die spanische Datenschutzbehörde verhängte gegen Spaniens größte Supermarktkette MERCADONA S.A. ein Bußgeld über 170.000 Euro. Grund für die Entscheidung war, dass ein Kunde einen Unfall in einer Filiale erlitten hatte und für die Geltendmachung von Schadensersatzansprüchen die Bereitstellung des Videomaterials bei der betreffenden Filiale anforderte.

Nachdem die Supermarktkette monatelang nicht auf das Auskunftsersuchen reagierte, wandte sich die betroffene Person an den Datenschutzbeauftragten. Der behördliche Datenschutzbeauftragte stellte fest, dass das Videomaterial bereits vernichtet worden war.

Darin lag nach Ansicht der Aufsichtsbehörde ein Verstoß gegen die Art. 12 und Art. 15 DSGVO, da das Auskunftsersuchen der betroffenen Person nicht beantwortet wurde. Weiter wurde gegen Art. 6 DSGVO verstoßen, da die Löschung des Videomaterials ohne Rechtsgrundlage erfolgte.

Der Fall zeigt: Auch eine Löschung personenbezogener Daten kann DSGVO-widrig sein.

- **Italien: Datenschutzverstoß kostet das Unternehmen Uber rund 4 Mio. Euro**

Dem Fahrtenvermittlungsunternehmen Uber wurde von der italienischen Datenschutzbehörde ein Bußgeld von 4.240.000 Euro aufgrund von Verstößen in Bezug auf die Verarbeitung von Daten von 1.500.000 Betroffenen in Italien erteilt.

Die italienische Datenschutzbehörde leitete eine Untersuchung gegen die gemeinsamen Verantwortlichen Uber B.V. und Uber Technologies Inc. ein. Diese ergab eine Vielzahl von Verstößen gegen die DSGVO durch die Unternehmen, darunter eine unzureichende Datenschutzerklärung, die Verarbeitung personenbezogener Daten ohne die erforderliche Zustimmung der Betroffenen sowie das Versäumnis, Meldepflichten ggü. der Datenschutzbehörde zu erfüllen. Bei den verarbeiteten Daten handelte es sich um Personen- und Kontaktdaten, Zugangsdaten zur App, Standortdaten und Beziehungen zu anderen betroffenen Personen.

Zudem wurden die Daten von etwa 1.379.000 betroffenen Personen eingeholt und für die Erstellung eines „Betrugsrisiko"-Profils verarbeitet. Dabei wurde den Betroffenen eine qualitative Bewertung (z. B. "niedrig") und ein numerischer Parameter von 1 bis 100 zugewiesen.

Uber B.V. und Uber Technologies Inc. wurden anteilig mit einem Bußgeld von jeweils ca. 2 Mio. Euro belegt. Schwer gewichtet wurde hier vor allem die große Betroffenenzahl.

- **Italien: Volle Geltung der DSGVO auch für verschlüsselte Daten**

Die italienische Datenschutzbehörde verhängte gegen ISWEB eine Geldstrafe in Höhe von 40.000 Euro: Die Aufsichtsbehörde stellte verschiedene Verstöße gegen die DSGVO fest. Die Verteidigung von ISWEB, sie verarbeite nur verschlüsselte Daten ohne über den Schlüssel zu verfügen, ließ die Behörde nicht gelten. Auch für verschlüsselte Daten gelte die DSGVO in vollem Umfang, selbst dann, wenn das verarbeitende Unternehmen nicht selbst über den Schlüssel verfüge.

ISWEB stellt Krankenhäusern eine Webanwendung, mit welcher Mitteilungen von Mitarbeitern gesammelt und verwaltet werden können, zur Verfügung. ISWEB beauftragte jedoch ohne das Wissen

der Krankenhäuser das Unternehmen Seeweb mit dem Hosting dieser Anwendung. Es fehlte an einer Genehmigung für die Beauftragung des Unterauftragsverarbeiters. Ferner lag kein Auftragsverarbeitungsvertrag zwischen ISWEB und Seeweb vor.

ISWEB machte geltend, dass der Gegenstand seines Vertrags mit den Krankenhäusern nicht die Verarbeitung der Meldungen, sondern allein die Bereitstellung der technischen Infrastruktur sei und weder ISWEB noch Seeweb zusätzliche Daten verarbeiteten. Da die Meldungen verschlüsselt werden und ausschließlich durch das Krankenhaus entschlüsselt werden können, sei der Zugang zu den Daten für sie nicht möglich. ISWEB stellte sich somit auf den Standpunkt, dass eine besondere oder allgemeine Genehmigung der Krankenhäuser nicht erforderlich gewesen sei und Seeweb nicht die gleichen Datenschutzgarantien hätten auferlegt werden müssen wie ISWEB im Verhältnis zu den Krankenhäusern ergaben.

Die Datenschutzbehörde ordnete das Vorgehen als Verstoß gegen die Regelungen zur Beauftragung von Unterauftragnehmern und gegen die Pflichten zum Abschluss eines Auftragsverarbeitungsvertrags ein. Die Datenschutzbehörde argumentierte, dass der Anbieter von Hosting-Diensten, selbst ohne direkten Zugang auf die Daten der Plattform, diese im System abspeichert. Daraus ergebe sich die Verpflichtung, die Voraussetzungen für eine rechtmäßige Verarbeitung der Daten durch den Unterauftragnehmer zu schaffen.

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