LOSCHELDER

Newsletter Datenschutzrecht
September 2022

Sehr geehrte Damen und Herren,

diesen Monat haben wir Neuigkeiten rund um das Auskunftsrecht, das zunehmend auch die Gerichte beschäftigt. Wir haben für Sie praxisrelevante Entscheidungen des Finanzgerichts München und des Verfassungsgerichtshofs NRW aufbereitet.

Für Unruhe hat zudem in der Sommerpause einmal wieder der EuGH gesorgt. In einer aktuellen Entscheidung legte er ein sehr weites Verständnis „besonderer Datenkategorien" zugrunde, die für viel Unsicherheit sorgt. Lesen Sie in unserem heutigen Newsletter, was die Entscheidung für die Praxis bedeutet.

Zusätzlich: Muss Facebook einem Nutzer Schadensersatz leisten, dessen Post wegen Hassrede gelöscht wurde? Mit dieser Frage beschäftigte sich das OLG Frankfurt.

Schließen wollen wir – wie gewohnt – mit unserem „Zu guter Letzt" und spannenden wie kuriosen Bußgeldentscheidungen.

Wir freuen uns über Ihr Interesse!

Schließlich: Sie können der **Verwendung Ihrer Daten für diesen Newsletter-Versand jederzeit widersprechen,** indem Sie den Newsletter abbestellen. Bitte scrollen Sie dazu ans Ende dieser E-Mail.

Inhalt

FG München: kein Akteneinsichtsrecht nach Art. 15 DSGVO

DSGVO Auskunftsanspruch: keine Verfassungsbeschwerde vor dem VerfGH NRW

EuGH: problematische Aussagen zu sensiblen Daten

OLG Frankfurt: Schadensersatzanspruch nach Art. 82 DSGVO nur bei hinreichender Erheblichkeit

Zu guter Letzt

FG München: kein Akteneinsichtsrecht nach Art. 15 DSGVO

Das Finanzgericht München hatte jüngst zu der Frage zu entscheiden, in welchem Umfang der Auskunftsanspruch nach Art. 15 DSGVO Einsicht in umfangreiche Aktensammlungen, einschließlich Aktenvermerke, rechtliche Analysen etc., gewährt. Die Entscheidung verdeutlicht: Nicht immer sind umfangreiche Auskunftsersuchen gerechtfertigt.

Im Rahmen des Auskunftsanspruchs nach Art. 15 DSGVO stellt sich bei umfangreichen Aktensammlungen oftmals folgende Frage: Reicht der Anspruch soweit, dass von sämtlichen in der/den Akte/n enthaltenen Schriftstücken Kopien zu erstellen sind? Oder fallen nur einzelne Angaben in den Dokumenten als personenbezogene Daten in den Anwendungsbereich der DSGVO, sodass der Auskunftsanspruch entsprechend in seinem Umfang begrenzt ist?

Das FG München hatte nun bereits zum zweiten Mal die Gelegenheit, hierüber zu urteilen (FG München, Urteil vom 05.05.2022 – 15 K 194/20). Ein erstes Urteil des FG München hatte derselbe Kläger bereits im November 2021 errungen (FG München, Urteil vom 04.11.2021 – 15 K 118/20). In beiden Verfahren begehrte der Kläger Auskunft über die vom Finanzamt und dem Bayrischen Landesamt für Steuern verarbeiteten, den Kläger betreffenden personenbezogenen Daten und Einsicht in bzw. (Farb-)Kopie von sämtlichen Verfahrensakten und Schriftstücken. Während die streitgegenständlichen Akten im Verfahren gegen das Finanzamt vor allem das Besteuerungsverfahren betrafen, ging es in dem Verfahren gegen das Landesamt um die im Rahmen eines (Dienstaufsichts-) Beschwerdeverfahrens geführten Akten.

Kein umfassender Auskunftsanspruch gem. Art. 15 DSGVO

Eine Verwaltungsakte wird zur Dokumentation eines konkreten Verwaltungsverfahrens angelegt. Es liegt nahe, dass die in der Akte enthaltenen Dokumente und Schreiben Angaben zu Verfahrensbeteiligten enthalten, die als personenbezogene Daten zu qualifizieren sind. Das Finanzgericht München stellte sich die Frage, ob diese „naheliegende Vermutung“ ausreiche, um für sämtliche Dokumente wie Schriftwechsel, Aktenvermerke, rechtliche Stellungnahmen oder Analysen den erforderlichen Personenbezug

herzustellen, der für die Öffnung des Anwendungsbereichs der DSGVO erforderlich ist.

Diese Frage verneint das Gericht: Personenbezogene Daten seien Einzelangaben und nicht etwa Akten oder Aktensammlungen, so das Gericht und verweist dabei auf § 3 Abs. 1 BDSG a.F. sowie Erwägungsgrund 15 zur DSGVO.

Textpassagen oder ganze Schriftstücke als personenbezogene Daten?

Trotzdem können Textpassagen oder Volltexte einzelne Angaben (Tatsachen, Werturteile o.ä.) enthalten, die das Potential in sich tragen, *personenbezogene Daten* und damit Gegenstand eines Auskunftsanspruchs zu sein. Erst durch einen menschlichen Interpretationsakt, den das FG München als „Heben" bezeichnet, werde aus einem potentiellen ein tatsächliches personenbezogenes Datum. Die „bloße Veraktung" reiche hierfür nicht aus. Erst durch die beabsichtige Zuordnung unter einen „spezifischen, personenbezogenen (Feld-)Bezeichner" (auch Kategorie oder Kriterium) werde ein ausreichendes Maß an „Strukturiertheit" innerhalb der Dokumentation hergestellt, welche den Anwendungsbereich der DSGVO eröffne. Jedenfalls das Ergebnis des Verwaltungsverfahrens, die Verwaltungsentscheidung, enthalte personenbezogene Daten; durch Bekanntgabe der Entscheidungsbegründung werde der Auskunftsanspruch jedoch erfüllt.

In Abgrenzung dazu sind Einzelangaben, die strukturiert in Datenbanken abgelegt und spezifischen Kriterien (z.B. die Feldbezeichner „Geburtsdatum", „Adresse") zugeordnet werden, unmittelbar und direkt als personenbezogene Daten zu erkennen und dementsprechend vom Auskunftsanspruch umfasst.

Besonderheit: Immanente Zuordnung

Beachtlich ist, dass diese Rechtsgrundsätze lediglich für umfangreiche Akten gelten sollen. Diese kennzeichnet, dass in ihnen enthaltene Daten in der Vielzahl der Angaben nicht leicht wiederauffindbar sind. In anderen Fällen sei die Zuordnung zu einer konkreten Person dem Schriftstück immanent. Das sei in den vom EuGH in diesem Zusammenhang entschiedenen Fällen der Fall gewesen. Das gelte etwa für eine Sammlung mit wenigen Daten, die

umfassend strukturiert sind (vgl. EuGH, Urteil vom 10.07.2018 – C-25/17 – „Zeugen Jehovas“). Ebenso sind Korrekturanmerkungen zu einer Prüfungsarbeit in einem so engen persönlichen Bezug, dass die Zuordnung zum Bearbeiter immanent sei (EuGH, Urteil vom 20.12.2017 – C-434/16 –„Korrekturanmerkungen“).

Dass nicht alle Dokumente, die womöglich einer natürlichen Person zugeordnet werden könnten, personenbezogene Daten und damit vom Auskunftsanspruch umfasst sind, hatte auch schon der BGH im Versicherungskontext entschieden: Ausgenommen hatte das Gericht insbesondere interne Bewertungen von Ansprüchen eines Versicherten und zugehörige rechtliche Analysen vom Auskunftsanspruch (wir berichteten dazu in unserem Loschelder-Newsletter aus März 2022). Die Details der Reichweite des Auskunftsanspruchs sind indes nach wie vor umstritten. Einige Themen wird der EuGH in absehbarer Zukunft in anhängigen Vorabentscheidungsverfahren (etwa C-487/21) zu besprechen haben.

In der Praxis sollte man bei komplexen Auskunftsersuchen von Betroffenen durchaus prüfen, ob die Entscheidung des FG München fruchtbar gemacht werden kann, auch wenn es sich nicht um Verwaltungsakten handelt.

DSGVO Auskunftsanspruch: keine Verfassungsbeschwerde vor dem VerfGH NRW

Das Auskunftsrecht aus Art. 15 DSGVO wird in der gerichtlichen Praxis durchaus nicht grenzenlos gewährt, sodass Umfang und Grenzen dieses Anspruchs immer wieder Streitpunkt sind. Auch der Verfassungsgerichtshof NRW (VerfGH) setzte sich Ende Juni mit einer behaupteten fehlerhaften Anwendung des Auskunftsanspruchs und daraus vermeintlich folgender Verletzung des Rechts auf rechtliches Gehör aus Art. 4 Abs. 1 LV i. V. m. Art. 101 Abs. 1 Satz 2 GG auseinander.

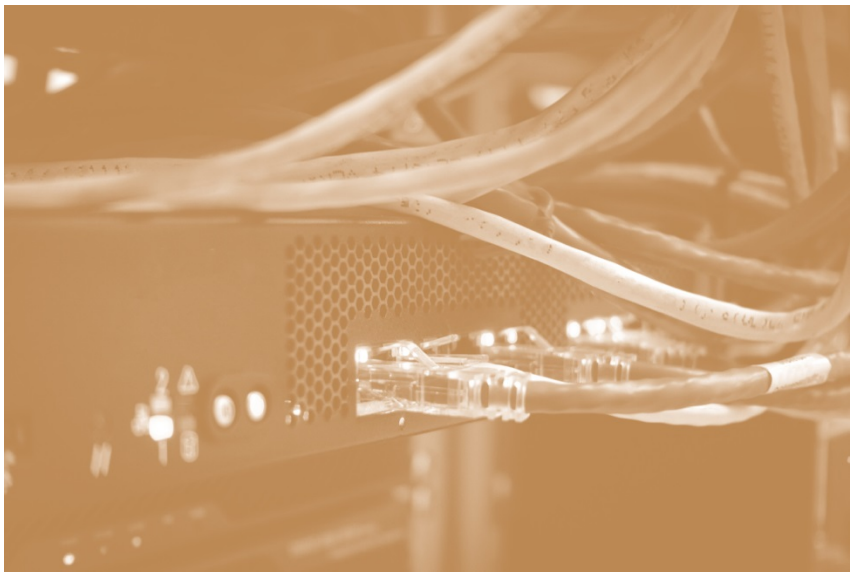
Die Verfassungsbeschwerde wurde von der Kammer mit ihrem Beschluss vom 21.06.2021 zurückgewiesen, weil sie nicht den Begründungsanforderungen genüge und damit unzulässig sei. Der Beschwerdeführer hatte sich mit einer Verfassungsbeschwerde gegen die Ablehnung eines Auskunftsanspruchs nach Art. 15 Abs. 3 DSGVO gewehrt. Das OLG Köln hatte zuvor einen solchen Anspruch aus Art. 15 Abs. 3 DSGVO mit der Begründung verneint, dass dieser nur dazu verpflichte, eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen, und nicht darüber hinaus wie gefordert die gesamte Gerichtsakte. Dieser Anspruch sei mit der Übersendung der verarbeiteten Stammdaten in Kopie erfüllt worden.

Der Beschwerdeführer sah sich deshalb durch das OLG in seinen Rechten aus Art. 15 Abs. 3 und 4 DSGVO verletzt. Dies habe der Beschwerdeführer in seiner Verfassungsbeschwerde jedoch nicht näher erläutert, geschweige denn sich damit umfassend auseinandergesetzt. Er habe lediglich unsubstantiiert vorgetragen, dass die Auffassung des Oberlandesgerichts, der datenschutzrechtliche Auskunfts- und Kopieanspruch nach Art. 15 Abs. 1 und 3 DSGVO beschränke sich auf die sog. Stammdaten des Betroffenen, nicht der überwiegend im Schrifttum und der instanzgerichtlichen Rechtsprechung vertretenen Ansicht entspreche. Damit gebe er jedoch nicht zu erkennen, inwiefern das Oberlandesgericht mit ihrer Auslegung des Art. 15 DSGVO Grundrechte außer Acht gelassen habe. Und nur solches spezifisches Verfassungsrecht prüft der Verfassungsgerichtshof.

Die Beschwerdebegründung gebe nach Auffassung des VerfGH NRW also nicht genügend Anlass für eine Vorlage an den Gerichtshof der Europäischen Union nach Art. 267 Abs. 3 AEUV und

damit auch nicht für eine Verletzung des Anspruchs auf den gesetzlichen Richter aus Art. 4 Abs. 1 Landesverfassung NRW (LV) i. V. m. Art. 101 Abs. 1 Satz 2 GG.

Der Beschluss des VerfGH NRW macht deutlich, dass der Verfassungsgerichtshof bei der Zulassung einer Verfassungsbeschwerde großen Wert darauf legt, dass die gerügte Grundrechtsverletzung umfassend als solche dargelegt wird. Es reicht auch im Kontext des Datenschutzes nicht aus, das verletzte Recht zu benennen. Vielmehr muss ausführlich begründet werden, warum seine Grundrechte bei der Anwendung des Art. 15 Abs. 3 und 4 DSGVO unberücksichtigt geblieben sind.



EuGH: problematische Aussagen zu sensiblen Daten

Das Verwaltungsgericht Vilnius in Litauen legte dem Europäischen Gerichtshof im Rahmen eines Vorabentscheidungsverfahrens zwei Fragen zum Verhältnis einiger litauischer Regelungen zur Korruptionsbekämpfung zu den Bestimmungen der DSGVO vor. Im Rahmen seines Urteils hat der Europäische Gerichtshof eine Aussage zur Reichweite des Art. 9 Abs. 1 DSGVO getroffen, der sensible Datenkategorien unter besonderen Schutz stellt. Der Europäische Gerichtshof legte den Anwendungsbereich der (immer wieder problematischen) Vorschrift weit aus und erregt damit die Gemüter in datenschutzrechtlichen Foren nachhaltig.

In dem Vorabentscheidungsverfahren ging es im Kern um die Frage, ob einige litauische Korruptionsbekämpfungsregeln wirksame rechtliche Verpflichtungen zur Datenverarbeitung nach Art. 6 Abs. 1 lit. c) DSGVO sind. Das war insbesondere unter Gesichtspunkten der Verhältnismäßigkeit problematisch. Die (sehr weitgehenden) Regelungen sehen vor, dass Daten von Personen, die mit der Verwaltung öffentlicher Mittel betraut sind, frei zugänglich ins Internet gestellt werden. Teil der erforderlichen Angaben sind unter anderem der Name, Arbeitgeber und die Funktion und Angaben über in den letzten zwölf Monaten durchgeführte Transaktionen im Wert von mindestens 3.000 Euro. Die Angaben müssen jeweils zur betroffenen Person selbst und in Bezug auf deren Lebensgefährten, Ehegatten oder Partner gemacht werden.

Der Europäische Gerichtshof (EuGH) hat diese Regelungen in seinem Urteil vom 01.08.2022 (C-184/20) als unverhältnismäßig beanstandet, sodass sie keine taugliche Rechtsgrundlage für Datenverarbeitungen nach Art. 6 Abs. 1 lit. c) DSGVO darstellen können.

Für das europäische Datenschutzrecht viel interessanter ist allerdings eine Aussage des EuGH zur Reichweite des Art. 9 Abs. 1 DSGVO. Auf die Frage hin, ob auch Informationen, die mittelbar Aufschluss über ein nach Art. 9 Abs. 1 DSGVO geschütztes Datum geben, bereits dem Schutz von Art. 9 Abs. 1 DSGVO unterliegen, führt der EuGH aus, dass es sich bereits bei diesen Informationen um besondere Kategorien personenbezogener Daten handele. Konkret ging es darum, ob die Angabe des Namens des Ehegatten, Partners oder Lebensgefährten, der – außer bei geschlechtsneutralen Namen – Aufschluss darüber gibt, ob die Personen in einer homo- oder

heterosexuellen Beziehung leben, ein sensibles Datum nach Art. 9 Abs. 1 DSGVO darstellt.

Diese Annahme und der damit einhergehende besondere Schutz von Informationen, die mittelbar auf sensible Daten nach Art. 9 Abs. 1 DSGVO schließen lassen, birgt eine gewisse Sprengkraft. Der Grund dafür ist, dass Art. 9 Abs. 1 DSGVO eine in der Praxis in vielen Fällen sehr schwer handhabbare Regelung darstellt, da sie die Verarbeitung sensibler Daten nur unter erschwerten Bedingungen zulässt. Das kann zu unterschiedlichen Widersprüchen führen.

Die Verarbeitung sensibler Daten ist nur auf der Grundlage eines Gesetzes zulässig, das spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht und aufgrund eines erheblichen öffentlichen Interesses erforderlich ist (Art. 9 Abs. 2 lit. g) DSGVO). Ausreichend ist also nicht jedes Gesetz, sondern nur besonders gestaltete Gesetze, was in der Praxis dazu führen kann, dass ein Verantwortlicher zwar aufgrund eines Gesetzes zur Verarbeitung sensibler Daten verpflichtet ist, die Verarbeitung aber nach der DSGVO dennoch nicht gestattet ist. Zwar genießt die DSGVO dann Vorrang gegenüber nationalen Gesetzen, aber der Verantwortliche bewegt sich hier auf einem schmalen Grat zwischen unterschiedlichen gesetzlichen Anforderungen (Pflicht zur Verarbeitung auf der einen, Verbot der Verarbeitung auf der anderen Seite). In beide Richtungen sieht er sich schnell dem Vorwurf eines Rechtsverstoßes ausgesetzt.

Weiter wird etwa im Zusammenhang mit Art. 9 Abs. 1 DSGVO immer wieder diskutiert, wie eigentlich die ungewollte Verarbeitung sensibler Daten gerechtfertigt werden kann. Beispielhaft ist wieder an die hier häufig erwähnte Rollstuhlfahrerin und/oder Brillenträgerin zu denken, die von einer Kamera gefilmt wird. Rollstuhl und Brille geben mittelbar Aufschluss über den Gesundheitszustand der Person und könnten daher grundsätzlich als besondere Kategorien personenbezogener Daten dargestellt werden. In diesem Fall wäre die Verarbeitung der Daten im Rahmen einer üblichen Videoüberwachung regelmäßig rechtswidrig. Dieses an sich vertretbare Ergebnis würde zu einer allgemeinen Unzulässigkeit der Videoüberwachung führen, da der Verantwortliche regelmäßig nicht vermeiden kann, dass auch Informationen über den Gesundheitszustand einer Person verarbeitet werden.

Solche und weitere Probleme potenzieren sich, wenn der EuGH den Begriff sensibler Daten nunmehr auf mittelbar sensible Informationen ausdehnt. Es bleibt daher zu hoffen, dass die Praxis die vorliegende Entscheidung mit Augenmaß heranzieht und sie nicht auf alle denkbaren Sachverhalte überträgt. Dadurch wäre die eigentliche Intention des Art. 9 Abs. 1 DSGVO, lediglich einen besonders sensiblen Bereich an Informationen zu schützen, konterkariert.

OLG Frankfurt: Schadensersatzanspruch nach Art. 82 DSGVO nur bei hinreichender Erheblichkeit

Das OLG Frankfurt befasste sich im Juni in einem Berufungsverfahren mit dem Facebook-Post eines Users, der gegen die Nutzungsbedingungen zur sogenannten Hassrede verstieß und Facebook damit zur Löschung des Posts sowie zur vorübergehenden Einschränkung von Funktionen des verantwortlichen Accounts veranlasste. Der Kläger hatte beim Landgericht Frankfurt erfolglos die erneute Freischaltung des Beitrags durch Facebook sowie Schadensersatz gem. Art. 82 DSGVO wegen Verstoßes gegen datenschutzrechtliche Bestimmungen verlangt.

Der umstrittene Post vom November 2018 nahm Bezug auf einen Artikel, der über die gewalttätige Auseinandersetzung zwischen zwei Afghanen in einer Flüchtlingsunterkunft berichtete. Der Kläger veröffentlichte in diesem Zusammenhang folgenden Kommentar:

„Solange diese sich gegenseitig abstechen ist es doch o.k. Ist jemand anderer Meinung? *Messer-Emoji*“.

Facebook hatte im April 2018 die Nutzungsbedingungen der Plattform geändert und darin die Veröffentlichung sogenannter „Hassrede“ verboten. Auch der Kläger hatte diesen geänderten Nutzungsbedingungen zugestimmt. Der Betreiber des sozialen Netzwerks war der Ansicht, dass der Post gegen die neuen Gemeinschaftsstandards verstieße und löschte diesen, ohne den Kläger vorher zu dem erhobenen Vorwurf anzuhören.

In einem Grundsatzurteil hatte der BGH vergangenen Sommer entschieden, dass Facebook vor der Löschung bestimmter Posts gewisse Regeln beachten müsse: Erforderlich sei dafür, dass der Nutzer über die Entfernung seines Beitrags informiert werde und ihm Gelegenheit zur Stellungnahme und Gegenäußerung eingeräumt werde. Mit der Entscheidung vom 30.06.2022 (16 U 229/20) knüpft das OLG Frankfurt am Main an diese Rechtsprechung an, urteilt aber nunmehr, dass die Anhörung eines Nutzers, dessen Post von Facebook gelöscht wurde, auch noch im gerichtlichen Verfahren nachgeholt werden könne.

Der Fehler einer unterlassenen Anhörung vor der Löschung eines Posts kann also im gerichtlichen Verfahren zur die Wiederfreischaltung geheilt werden. Mit der Berufung auf die unterlassene Anhörung allein kann der betroffene Nutzer also die Freigabe seines Posts nicht verlangen, soweit die nachgeholte Anhörung nicht zu einer veränderten Bewertung des Falls führt.

Ebenso weist das OLG einen Schadensersatzanspruch des Klägers aus Art. 82 DSGVO zurück, der einen Verstoß gegen Bestimmungen der DSGVO sowie einen materiellen oder immateriellen Schaden voraussetzt.

Zum einen sei die Zustimmung zu den Nutzungsbedingungen der Beklagten (Art. 6 Abs. 1 lit. a) DSGVO) nicht an die Erfüllung der vertraglichen Verpflichtungen durch die Beklagte geknüpft, sodass in der etwaigen Weiternutzung der bei der Beklagten vorhandenen Daten des Klägers während der teilweisen Sperrung des Kontos auch kein Verstoß gegen zwingende Vorgaben der DSGVO liege. Zum anderen stelle die temporäre Teilsperrung des Nutzerkontos des Klägers auch keine Verarbeitung von dessen Daten im Sinne von Art. 8 Nr. 2 DSGVO dar.

Das OLG äußert sich zudem umfassend zur Auslegung des Art. 82 DSGVO im Hinblick auf die Voraussetzung eines immateriellen Schadens. Ein Schadensersatzanspruch würde nicht bereits bei jeder individuell empfundenen Unannehmlichkeit oder bei Bagatellverstößen begründet; vielmehr müsse hierzu, auch angesichts des bestehenden Missbrauchsrisikos, eine gewisse Erheblichkeitsschwelle überschritten werden. Dies sei beispielsweise der Fall, wenn der datenschutzrechtliche Verstoß eine Vielzahl von Personen in gleicher Weise betrifft und damit Ausdruck einer im großen Stil betriebenen, bewussten Kommerzialisierung ist.

Anders müsse der hier gegebene Fall bewertet werden. Durch die Unterdrückung eines einzelnen Posts sei keine hinreichende Beeinträchtigung des Persönlichkeitsrechts gegeben. Vielmehr liege hier nur eine bagatellhafte Unannehmlichkeit vor, die einen Schadenersatzanspruch nach Art. 82 DSGVO nicht rechtfertigen könne. Darüber hinaus müsse auch berücksichtigt werden, dass die Löschung gerade vorgenommen wurde, um das Persönlichkeitsrecht anderer Nutzer gegen die veröffentlichte Hassrede zu schützen. Durch die Zuerkennung eines Schadensersatzanspruchs in einem solchen Fall würde zudem ein unangemessenes Spannungsfeld zwischen der Löschpflicht des Portalbetreibers einerseits und dem hiermit verbundenen Schadensersatzrisiko andererseits entstehen. Aus diesem Grund stehe dem Kläger hier kein Schadensersatzanspruch nach Art. 82 DSGVO zu.

Die Entscheidung des OLG Frankfurt unterstreicht, dass Schadensersatzansprüche nicht bei jeglichen, bagatellhaften Verstößen gegen das Datenschutzrecht drohen. Vielmehr löst erst die Überschreitung einer gewissen Erheblichkeitsschwelle, die über eine individuell empfundene Unannehmlichkeit hinausgeht, ein Schadensersatzanspruch nach Art. 82 DSGVO aus.

Zu guter Letzt

Auch diesen Monat haben wir wieder einige spannende Fälle für Sie. Das zweithöchste Bußgeld der Geschichte der DSGVO wurde einem Social-Media-Unternehmen auferlegt. Ein deutscher Automobilersteller muss wegen fehlender Datenschutzkennzeichnungen in Probefahrzeugen über eine Million Euro zahlen. Ein Hackerangriff auf eine Anwaltskanzlei kostete diese ein Bußgeld von 67.000 Euro. Google Workspace darf in einer dänischen Gemeinde nicht mehr verwendet werden. Und zuletzt wird ein Berliner E-Commerce-Konzern wegen eines Interessenskonflikts des Datenschutzbeauftragten in Höhe von 525.000 Euro zur Kasse gebeten. Diese Verstöße gegen die DSGVO haben wir Ihnen im Folgenden zusammengestellt.

- **Irland: Rekordbußgeld über 405 Millionen Euro für Instagram**

Grund für das Bußgeld in Rekordhöhe für das Social-Media-Unternehmen ist, dass jugendliche Nutzer nicht ausreichend Schutz erfahren hätten. Bis September 2019 war es Nutzern im Alter von 13 bis 17 Jahren möglich, nicht nur private, sondern auch Geschäftskonten zu eröffnen. Hierdurch wurden ihre Kontaktdaten (Telefonnummer, E-Mail-Adresse) standardmäßig für die Allgemeinheit sichtbar. Erst seit September 2019 sind nun alle Konten standardmäßig privat gestellt, wenn das Alter der Nutzer unter 18 Jahren liegt.

Hierin sah die irische Datenschutzbehörde einen schweren Verstoß gegen die Datenschutzgrundverordnung und belegte das Unternehmen mit dem Bußgeld in Höhe von 405 Millionen Euro. Damit wurde das zweithöchste Bußgeld der Geschichte der DSGVO verhängt und übertrifft dabei das Bußgeld gegen WhatsApp in Höhe von 225 Millionen Euro von vor einem Jahr, welches ebenfalls die Muttergesellschaft Meta Platforms betraf. Diese hat jedoch bereits angekündigt, Berufung gegen das hohe Bußgeld einzulegen.

- **Deutschland: 1,1 Millionen Euro Bußgeld für Volkswagen aufgrund fehlender Kennzeichnung von Kameraaufnahmen durch ein Probefahrzeug**

Der Verstoß gegen die DSGVO fiel auf, nachdem die österreichische Polizei ein Erprobungsfahrzeug des Unternehmens zur Verkehrskontrolle angehalten hatte. Die Beamten bemerkten dabei Kameras am Fahrzeug, welche eingesetzt wurden, um die Funktionsfähigkeit eines Fahrassistenzsystems zu testen. Zu diesem Zwecke wurde das Verkehrsgeschehen um den Wagen aufgezeichnet. Es fehlte jedoch an Hinweisschildern und vorgeschriebenen Informationen bezüglich der Aufnahmen, weshalb ein Verstoß gegen Art. 13 DSGVO vorlag. Weiter wurde gegen Art. 28 DSGVO wegen Fehlens eines Auftragsverarbeitungsvertrags zwischen Volkswagen und dem Unternehmen, welches für die Fahrt zuständig war, verstoßen. Es fand keine Datenschutz-Folgenabschätzung i. S. d. Art. 35 DSGVO statt, auch wurde Art. 32 DSGVO verletzt.

Nach Bekanntwerden der Verstöße wurden die Mängel durch Volkswagen unverzüglich behoben. Die Forschungsfahrten an sich waren datenschutzrechtlich zulässig, da die Verarbeitung der Optimierung eines Fahrassistenzsystem zur Verhinderung von Unfällen diene und demnach die Sicherheit im Straßenverkehr fördern soll. Die Landesbeauftrage für den Datenschutz (LfD) Niedersachsen verhängte daraufhin aufgrund grenzüberschreitender Verarbeitung personenbezogener Daten ein Bußgeld von 1.100.000 Euro.

- **Dänemark: Hackerangriff auf eine Anwaltskanzlei mit unzureichenden Sicherheitsmaßnahmen**

Nach einem Hackerangriff auf eine Kanzlei verschafften sich die Hacker Zugang zu deren Servern und verschlüsselten die darauf

gespeicherten personenbezogenen Daten. Es bestand so ein hohes Risiko, dass Unbefugte auf die Daten zugreifen könnten. Die Kanzlei informierte deshalb die Datenschutzbehörde bezüglich des Angriffs.

Die dänische Datenschutzbehörde stellte fest, dass durch die Anwaltskanzlei keine grundlegenden Sicherheitsmaßnahmen ergriffen wurden. Insbesondere unter dem Gesichtspunkt, dass ihre Verarbeitung eine besondere Kategorie von personenbezogenen Daten betraf. Die Datenschutzbehörde betonte, dass in solchen Fällen eine Datenverletzung mit großer Wahrscheinlichkeit ein hohes Risiko für die Rechte der betroffenen Personen mit sich bringen würde. Daher müssen in einem solchen Fall strenge Sicherheitsmaßnahmen ergriffen werden, um unbefugte Zugriffe zu verhindern.

Die Datenschutzbehörde zeigte die Kanzlei deshalb bei der Polizei an und schlug ein Bußgeld von 67.200 Euro (500.000 DKK) wegen der Verletzung des Art. 83 Abs. 2 DSGVO vor. In solchen Fällen verhängt nicht die dänische Datenschutzbehörde selbst das Bußgeld, sondern verweist sie an die Polizei. Diese untersucht dann, ob Gründe für eine Anklageerhebung vorliegen. Anschließend entscheidet ein Gericht über den Fall.

- **Dänemark: Die dänische Datenschutzbehörde verbietet die Nutzung von Google Workspace in der Gemeinde Helsingør**

Die dänische Datenschutzbehörde wies im September 2021 die Gemeinde Helsingør an, eine Risikobewertung der Verarbeitung personenbezogener Daten durch die Gemeinde in der Grundschule unter Verwendung von Google Chromebooks und Workspace durchzuführen.

Die erstellte Dokumentation und Risikobewertung der Gemeinde zeigte auf, dass die Verarbeitung der Daten in mehreren Punkten nicht den Anforderungen der DSGVO entspricht.

Zum einen hatte die Gemeinde einige spezifische Risiken in Bezug auf die Verarbeitungstätigkeiten nicht bewertet, die die Gemeinde als öffentliche Behörde durchführen darf. Darüber hinaus heißt es in der Vereinbarung mit dem Datenverarbeiter, dass Informationen in Situationen, in denen es um technische Unterstützung geht, in Drittländer übermittelt werden können, ohne dass das erforderliche Sicherheits- und Schutzniveau gewährleistet ist.

Aufgrund der Entscheidung vom September 2021, fasste die dänische Datenschutzbehörde nun einen neuen Beschluss und wies die Gemeinde Helsingør an, die Datenverarbeitung auszusetzen, solange Informationen ohne erforderliches Schutzniveau in Drittländer übermittelt werden. Zudem legte sie der Gemeinde ein allgemeines Verbot bezüglich der Verarbeitung personenbezogener Daten mit Google Workspace auf, bis eine angemessene Dokumentation und Folgenabschätzung durchgeführt und die Verarbeitungsvorgänge mit der DSGVO in Einklang gebracht wurden.

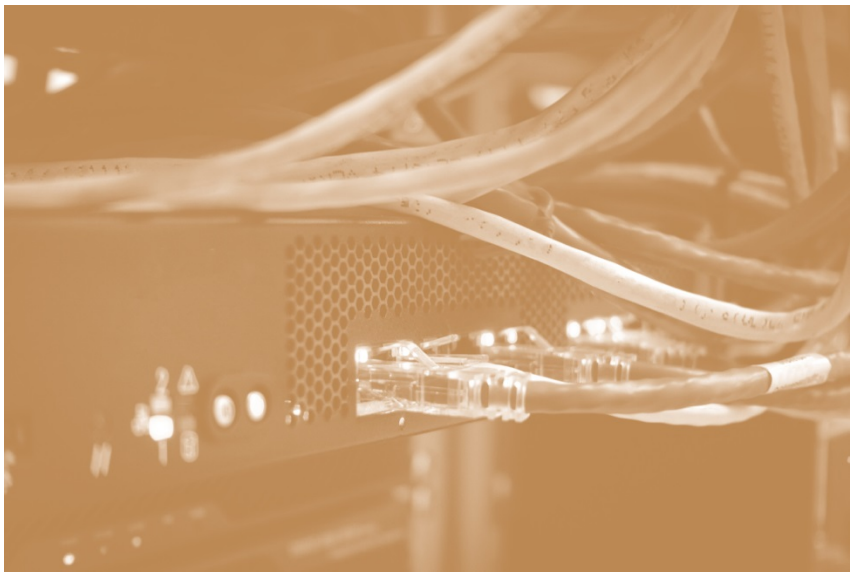
Die dänische Datenschutzbehörde stellt zudem fest, dass viele der spezifischen Schlussfolgerungen dieser Entscheidung wahrscheinlich auch für andere dänische Gemeinden gelten werden, welche dieselbe Datenverarbeiter-Konstruktion verwenden. Die dänische Datenschutzbehörde erwartet von diesen Gemeinden, dass sie auf der Grundlage dieser Entscheidung entsprechende Schritte unternehmen.

- **Berlin: 525.000 Euro Bußgeld für die Tochtergesellschaft eines Berliner E-Commerce-Konzerns wegen Interessenskonflikts des Datenschutzbeauftragten**

Gemäß Art. 38 Abs. 6 S. 2 DSGVO können als Datenschutzbeauftragte nur Personen fungieren, welche keinem Interessenskonflikt aufgrund anderer Aufgaben im Unternehmen unterliegen. Es soll somit keine Selbstüberwachung stattfinden. Der Datenschutzbeauftrage der Tochtergesellschaft des E-Commerce-Konzerns war jedoch zugleich Geschäftsführer zweier Dienstleistungsgesellschaften, welche personenbezogene Daten im Auftrag eben dieses Unternehmens verarbeiteten, in welchem er als Datenschutzbeauftragter tätig war. Er musste somit die Einhaltung des Datenschutzrechts jener Dienstleistungsgesellschaften überwachen, obwohl er deren Geschäftsführer ist und demnach von ihm selbst getroffene Entscheidungen kontrollieren.

Hierin lag laut der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) ein Interessenkonflikt und mithin ein Verstoß gegen die DSGVO. Aus diesem Grund erteilte die Aufsichtsbehörde im Jahr 2021 zunächst eine Verwarnung gegen das Unternehmen. Bei erneuter Überprüfung 2022 bestand der Verstoß jedoch weiterhin und es wurde ein Bußgeld in Höhe von 525.000 Euro verhängt. Das Urteil ist noch nicht rechtskräftig.

Das hohe Bußgeld rechtfertigte die BlnBDI zum einen mit dem dreistelligen Millionenumsatz des E-Commerce-Konzerns im vorherigen Geschäftsjahr und der bedeutsamen Rolle, welche dem Datenschutzbeauftragten als Ansprechpartner für eine Vielzahl an Beschäftigten und Kunden zukommt. Zudem hatte das Unternehmen trotz der Verwarnung zunächst keine Maßnahmen eingeleitet.



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