LOSCHELDER

Newsletter Datenschutzrecht
Mai 2023

Sehr geehrte Damen und Herren,

pünktlich zum 5. Geburtstag der DSGVO sehen wir aktuell eine Entscheidungsflut des EuGH in Sachen Datenschutz. Höchstrichterliche Konkretisierung und Präzisierung der auslegungsbedürftigen DSGVO ist weiterhin heiß ersehnt – aber bringen die EuGH-Entscheidungen wirklich die so dringende Klarheit und Rechtssicherheit für die Praxis?

Von erheblicher Relevanz sind die Entscheidungen allemal, insbesondere mit Blick auf die Reichweite des Auskunftsrechts und auf Schadensersatzforderungen betroffener Personen. Wir haben Ihnen eine Übersicht über die für uns wichtigsten Entscheidungen und Aussagen zusammengestellt und einige der Entscheidungen detaillierter aufbereitet.

Wir freuen uns über Ihr Interesse!

Inhalt

Alles neu macht der Mai: Entscheidungswelle beim EuGH

Am 4. Mai und in den Tagen davor hat der EuGH mehrere datenschutzrechtlich höchst relevante Entscheidungen bzw. Schlussanträge veröffentlicht. Es geht unter anderem erneut um die Reichweite des Auskunftsrechts und Schadensersatzansprüche bei DSGVO-Verstößen, um den Adressaten von Bußgeldentscheidungen und vieles mehr. Wir haben Ihnen eine substantielle Übersicht erstellt mit den nach unserer Auswertung wichtigsten Aussagen.

Angesichts der kürzlich veröffentlichten Entscheidungswelle wird deutlich, dass die Relevanz des Datenschutzrechts weiter steigt. Der EuGH schafft in diesem Bereich durch seine Urteile mehr Rechtssicherheit, die seit nunmehr fünf Jahren sehnlich erwartet wird.

Die Kernaussagen der Urteile und Schlussanträge der letzten Wochen haben wir im Folgenden zusammengefasst. Bitte beachten Sie, dass der EuGH den Schlussanträgen nicht folgen muss, auch wenn dies statistisch gesehen meist der Fall ist.

Auskunftsrecht nach Art. 15 DSGVO

Zum Auskunftsrecht: Die Herausgabe einer Übersicht der verarbeiteten Daten genügt, um den Anspruch auf Kopie zu erfüllen.

- Eine „Kopie“ im Sinne des Art. 15 Abs. 3 DSGVO meint eine „originalgetreue und verständliche Reproduktion“ (Rn. 45) der personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Auch eine Übersicht, in der die Daten zusammengetragen werden, reicht grundsätzlich aus.
- Reicht dies ausnahmsweise nicht aus, damit die betroffene Person vollständig die Richtigkeit ihrer Daten überprüfen kann, kann sie Kopien von ganzen Dokumenten oder Datenbankauszügen verlangen. Dabei sind jedoch insbesondere Urheberrechte oder Geschäftsgeheimnisse anderer Personen zu berücksichtigen, die darin enthalten sein können.

- Auch, wenn die Kopien gem. Art. 15 Abs. 3 S. 3 DSGVO auf elektronischem Wege beantragt werden, bleibt der Umfang der herauszugebenden Daten der gleiche.
  EuGH, Urteil vom 04.05.2023, Rs. C-487/21 – Österreichische Datenschutzbehörde

Zweck und Motivation des Herausverlangens von Kopien nach Art. 15 Abs. 3 DSGVO unerheblich; Entgelte können für weitere Kopien zulässig sein

- Grundsätzlich ist nach Ansicht des Generalanwalts die Motivation der betroffenen Person unerheblich für ihr Recht auf Herausgabe einer Kopie.
- Verfolgt die Person das Ziel, mit den Kopien beispielsweise arzthaftungsrechtliche Ansprüche zu belegen, besteht trotzdem eine Herausgabepflicht.
- Die erste Kopie ist gem. Art. 15 Abs. 3 DSGVO unentgeltlich herauszugeben. Dies kann aber durch eine nationale Regelung im Einklang mit Art. 23 DSGVO eingeschränkt werden. Vor allem muss das Entgelt „strikt auf die tatsächlich anfallenden Kosten beschränkt sein“ (Rn. 71)
  Schlussanträge vom 20.04.2023 zur Rs. C-307/22

<u>Schadensersatz Betroffener</u>

Schadensersatz ist nur bei tatsächlich eingetretenem Schaden zu leisten; das Gewicht des Schadens ist allerdings unerheblich

- Der bloße Verstoß gegen die DSGVO begründet für sich noch keinen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO. Es muss beim Betroffenen tatsächlich ein Schaden eingetreten sein.
- Allerdings ist das Gewicht des Schadens unerheblich. Auch für Bagatellschäden ist Ersatz zu leisten.
  EuGH, Urteil vom 04.05.2023, Rs. C-300/21 – Österreichische Post

Befürchtung eines Missbrauchs von Daten nach DSGVO-Verstoß soll einen ersatzfähigen Schaden darstellen können

- Ein immaterieller Schaden der betroffenen Person kann auch in der bloßen Befürchtung des Missbrauchs ihrer Daten bestehen.
- Die Möglichkeit eines Missbrauchs muss die betroffene Person allerdings nachweisen ebenso wie die Tatsache, dass sie „individuell einen realen und sicheren emotionalen Schaden erlitten hat“ (Rn. 82).
  Schlussanträge vom 27.04.2023 zur Rs. C-340/21 – Natsionalna agentsia

Verantwortlicher soll Datensicherheit nachweisen müssen (Rechenschaftspflicht)

- Eine Datenpanne i.S.d. Art. 4 Nr. 12 DSGVO impliziert nicht, dass die Datensicherheit unzureichend war.
- Der Verantwortliche trägt im Rahmen einer Schadensersatzklage (Art. 82 DSGVO) die Darlegungs- und Beweislast, dass die von ihm ergriffenen Maßnahmen i.S.d. Art. 32 DSGVO geeignet waren, da er i.d.R. als einziger die Mittel für einen solchen Nachweis besitzt. Die Bestimmung der zulässigen Beweismittel ist mangels unionsrechtlicher Vorschriften Sache der Mitgliedstaaten (Verfahrensautonomie). Auch ein gerichtliches Sachverständigengutachten kann daher nach nationalem Recht ein zulässiges Beweismittel darstellen.
  Schlussanträge vom 27.04.2023 zur Rs. C-340/21

Haftungsfreistellung nur, wenn keinerlei Verantwortlichkeit für eingetretenen Schaden besteht

- Der Verantwortliche wird nicht allein deswegen von der Haftung nach Art. 82 DSGVO befreit, weil ein Dritter den Verstoß gegen die DSGVO, der den fraglichen Schaden verursacht hat, begangen hat (Hackerangriff).
- Vielmehr muss der Verantwortliche beweisen, dass er in keinerlei Hinsicht für den Verstoß verantwortlich ist.
  Schlussanträge vom 27.04.2023 zur Rs. C-340/21

Adressat von Bußgeldern

Unternehmen können Adressaten von Bußgeldern sein

- Was zwischen den deutschen Aufsichtsbehörden und Gerichten umstritten war, will der Generalanwalt beim EuGH zugunsten des LG Bonn entscheiden: Unternehmen können nach der DSGVO und ungeachtet des OWiG Adressaten (natürliche Personen in erster Linie) von Bußgeldern sein.
- Die OWiG-Vorgaben können konkretisierend herangezogen werden, aber nur, wenn dies die Durchsetzung der DSGVO nicht beeinträchtigt.
- Bußgelder setzen auch nach der DSGVO einen schuldhaften Verstoß voraus.
- Die Anwendung des deutschen Ordnungswidrigkeitenrechts darf nicht dazu führen, dass schuldhaftes Verhalten von Mitarbeitern dem Unternehmen nicht zugerechnet wird. Der Generalanwalt tendiert zu einer unspezifischen, weiten Auslegung, nach der DSGVO-Verstöße von Mitarbeitern regelmäßig und quasi „generell" dem Unternehmen zuzurechnen sind.
  Schlussanträge vom 27.04.2023 zur Rs. C-807/21 – Deutsche Wohnen SE

Bußgelder setzen Verschulden voraus

- Ein Bußgeld darf nur verhangen werden, wenn ein DSGVO-Verstoß vorsätzlich oder fahrlässig begangen wurde.
- Allerdings kann ein Verantwortlicher auch für einen verschuldeten Verstoß seines Auftragsverarbeiters bebußt werden.
  Schlussanträge vom 04.05.2023 zur Rs. C-683/21 – Nacionalinis visuoménes

Beweisverwertungsverbot bei DSGVO-Verstoß?

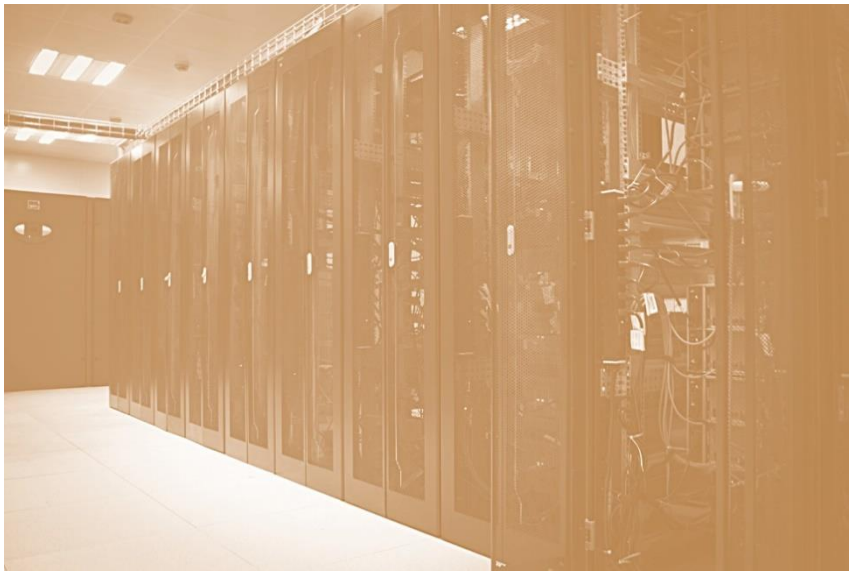
Rechtmäßigkeit der Datenverarbeitung trotz Verstoß gegen Art. 26, 30 DSGVO: Derartige Verstöße führen nicht zu einem Verwertungsverbot.

- Liegt ein Verstoß gegen die Pflicht zum Abschluss einer Vereinbarung über die gemeinsame Verantwortlichkeit (Art. 26 DSGVO) vor oder wird kein ordnungsgemäßes Verarbeitungsverzeichnis geführt (Art. 30 DSGVO), führt das allein noch nicht zur Unrechtmäßigkeit der Datenverarbeitung (wohl aber zu einem Verstoß gegen die DSGVO).
- Die hierbei verarbeiteten Daten dürfen trotzdem in einem gerichtlichen Verfahren berücksichtigt werden. Das gilt auch, wenn die betroffene Person nicht ausdrücklich ihre Einwilligung dazu erteilt hat. Es besteht hier also kein Beweisverwertungsverbot.
  EuGH, Urteil vom 04.05.2023, Rs. C-60/22 – Bundesrepublik Deutschland

Welche Daten sind personenbezogen?

Pseudonymisierte Daten sind nur für den Akteur personenbezogen, der die dahinterstehenden Personen identifizieren kann

- Daten können pseudonymisiert werden, sind aber auch dann noch – im Gegensatz zu anonymisierten Daten – personenbezogen.
- Pseudonymisierte Daten sind aber nur für den Akteur personenbezogen, der die Möglichkeit hat, den Personenbezug wiederherzustellen.
- Durch die Übermittlung können diese Daten für den Empfänger anonym werden, insbesondere, wenn der Empfänger nicht über die zusätzlichen Informationen wie die Zuordnung einer Kennnummer zu einem Namen verfügt und sich diese auch nicht mit verhältnismäßigem Aufwand beschaffen kann.
  EuG, Urteil vom 26.04.2023, Rs. T-557/20 – SRB/EDSB



Kein Strafschadensersatz: Der bloße DSGVO-Verstoß begründet noch keinen Schadensersatzanspruch

Welche Voraussetzungen vorliegen müssen, damit betroffenen Personen bei Verletzung der DSGVO ein Schadensersatzanspruch zusteht, wurde nun durch ein Urteil des EuGH klargestellt. Für Verantwortliche ist dies Fluch und Segen zugleich: Ein Verstoß gegen die DSGVO führt für sich genommen noch nicht zum Anspruch auf Schadensersatz. Aber: Auch Bagatellschäden sind zu ersetzen.

Kürzlich veröffentlichte der EuGH sein Urteil zur Auslegung des datenschutzrechtlichen Schadensersatzanspruches (Art. 82 DSGVO). Dem Vorabentscheidungsverfahren (Rs. C-300/21) lag ein Rechtsstreit vor dem Obersten Gerichtshof (OGH) in Österreich zugrunde. In der Sache ging es darum, dass die Österreichische Post AG Informationen über politische Interessen der Bevölkerung gesammelt und diese mit einem Algorithmus ausgewertet hat, um im Ergebnis bestimmten Personen eine gewisse Affinität zu einer politischen Partei zusagen zu können.

Der Kläger im Ausgangsverfahren fühlte sich beleidigt und bloßgestellt, weil ihm im Rahmen dieser Auswertung eine Affinität zu einer bestimmten politischen Partei zugeordnet wurde, ohne dass er im Voraus der Verarbeitung seiner Daten zugestimmt hatte. Seiner Klage auf Unterlassung der Verarbeitung wurde vom Landesgericht Wien (Österreich) stattgegeben. Der daneben geltend gemachte Anspruch auf Ersatz seines immateriellen Schadens aus Art. 82

DSGVO wurde abgelehnt, was auch in der Berufungsinstanz bestätigt wurde. Das wurde damit begründet, dass der immaterielle Schaden nach österreichischem Schadensrecht eine gewisse Erheblichkeit aufweisen müsse, die bei den dargelegten negativen Gefühlen nicht vorläge.

Im Rahmen der Revision vor dem OGH legte dieser dem EuGH mehrere Fragen zur Auslegung von Art. 82 DSGVO vor. Die Schlussanträge hierzu haben wir bereits in der Newsletter-Ausgabe von November 2022 erläutert.

In seinem Urteil folgt der EuGH den Schlussanträgen im Wesentlichen:

1. **Ein bloßer DSGVO-Verstoß genügt nicht**: Für einen Schadensersatzanspruch reicht nicht schon die bloße Verletzung von DSGVO-Vorschriften aus. Vielmehr muss tatsächlich ein materieller oder immaterieller Schaden beim Betroffenen entstanden und dargelegt sein und dieser auch kausal auf der Verletzung der DSGVO beruhen. Das ergibt sich schon aus dem Wortlaut von Art. 82 Abs. 1 DSGVO, der die Verletzung der DSGVO und einen Schaden als eigenständige Begrifflichkeiten nennt. Etwas Anderes folgt auch nicht aus den Erwägungsgründen zur DSGVO.

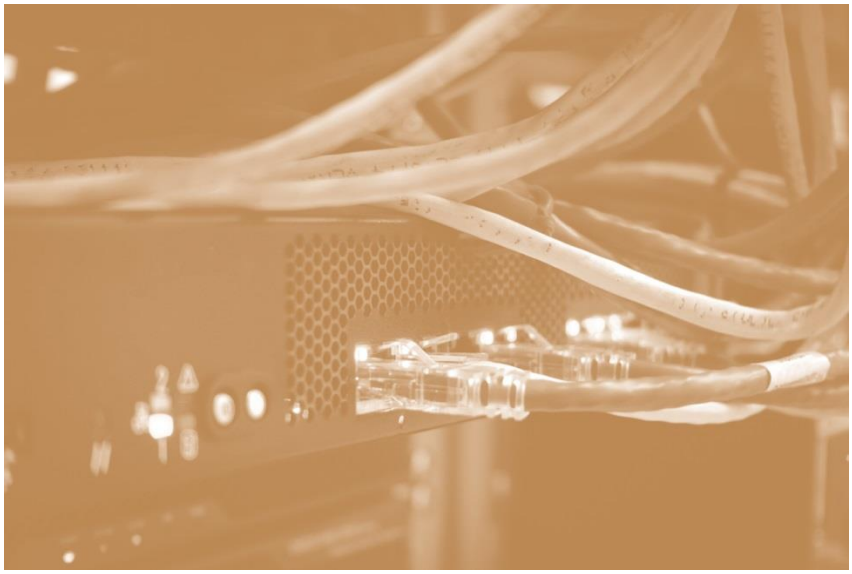
2. **Auch Bagatellschäden:** Der Schadensersatz darf allerdings nicht davon abhängig gemacht werden, dass der Schaden eine gewisse Erheblichkeitsschwelle überschritten haben muss. Der Anspruchsteller muss lediglich nachweisen, dass überhaupt ein Schaden entstanden ist. Dies steht im Einklang mit dem weiten Verständnis des Schadensbegriffs in der DSGVO und ihrem Ziel, ein gleichmäßiges und hohes Schutzniveau in allen Mitgliedstaaten zu gewährleisten (Erwägungsgrund 10). Denn eine Bewertung der Erheblichkeit durch die nationalen Gerichte würde dazu führen, dass diese Schwelle unterschiedlich hoch angesetzt und die DSGVO eben nicht gleichmäßig angewendet wird.

3. **Schadenshöhe:** Die Festsetzung der konkreten Höhe des zu zahlenden Betrages bleibt jedoch Sache der nationalen Gerichte. Da die DSGVO keine Regeln zur Bemessung des Schadensersatzes nach Art. 82 DSGVO enthält, folgen die Gerichte dabei den jeweiligen nationalen Vorschriften. Es

gelten die allgemeinen Prinzipien für den Vollzug von Unionsrecht in den Mitgliedstaaten (Äquivalenz- und Effektivitätsgrundsatz).

Dass von einer DSGVO-Verletzung nicht sofort auf einen Schaden geschlossen werden kann, bringt mehr Rechtssicherheit und könnte der befürchteten Klagewelle entgegenstehen. Wirklich aufatmen können Verantwortliche aber nicht, da nach EuGH auch geringste immaterielle Schäden zu einem Ersatzanspruch führen. Im konkreten Fall wird eine sehr genaue Prüfung erforderlich werden, was passiert ist – und was vorgetragen wird. Denn der Anspruchsteller bleibt darlegungs- und beweisbelastet. Hier wird sich zeigen, ob künftig das bloße „Unwohlsein" als Schaden ausreicht. Nach der EuGH Rechtsprechung ist das zu befürchten.

Sicher ist: Nicht bei jeder Verletzung der DSGVO ist automatisch Schadensersatz zu leisten. Werden jedoch ein Schaden und auch alle übrigen Anspruchsvoraussetzungen nachgewiesen, muss unabhängig von der Erheblichkeit des Schadens gezahlt werden. Der EuGH widerspricht damit einiger nationaler Rechtsprechung (siehe unser Newsletter-Beitrag zur Entscheidung des OLG Frankfurt).



Hackerangriff: Haftung des Verantwortlichen entfällt nur im Ausnahmefall

Kommt es zu einem Datenleck oder Hackerangriff, können millionenfach personenbezogene Daten in die Hände Unbefugter gelangen, wie es im Juli 2019 bei der bulgarischen Nationalen Agentur für Einnahmen (NAP) erfolgte. Fraglich ist dann, ob und wie weit der datenschutzrechtlich Verantwortliche für einen entstandenen Schaden haftet. Der Generalanwalt beim EuGH legt einen weiten Maßstab an.

Wenn es zu einem unbefugten Zugang zu personenbezogenen Daten durch Dritte kommt, so haftet der Verantwortliche geschädigten Betroffenen nach den Maßstäben des Art. 82 DSGVO, auch für einen immateriellen Schaden in Form von Angst und Sorge wegen eines möglichen Datenmissbrauchs. Erforderlich ist, dass dieser Schaden tatsächlich nachgewiesen ist. An das Verschulden des Verantwortlichen will der Generalanwalt dabei keine hohen Anforderungen stellen und spricht gar von einem womöglich „vermuteten Verschulden", wobei unklar bleibt, ob dies tatsächlich der Fall sein soll (Rn. 73). Wir sehen für ein vermutetes Verschulden jedenfalls keinen Anhaltspunkt in Art. 82 DSGVO und auch der Generalanwalt äußert sich hier nicht klar (Generalanwalt Pitruzzella, Schlussanträge vom 27.04.2023 zur Rs. C-340/21).

Den Schlussanträgen zugrunde liegt der folgende Fall: Im Juli 2019 wurde in bulgarischen Medien bekannt gegeben, dass im Internet Steuer- und Sozialversicherungsdaten von Millionen bulgarischen Bürgern und Bürgerinnen im Internet veröffentlicht wurden. Diese hatte sich ein Unbefugter mittels eines Hackerangriffs auf das Informationssystem der Nationalen Agentur beschafft. In einer Klage gegen die Agentur verlangte die Klägerin Schadensersatz aufgrund der Angst und Befürchtung, zukünftig einen Datenmissbrauch zu erleiden. Im Rahmen dieser Klage legte das Gericht dem EuGH einige Vorlagefragen zur Klärung vor. Darunter fand sich auch die Frage, ob eine Befürchtung, in Zukunft einen Missbrauch von personenbezogenen Daten zu erleiden, einen immaterieller Schaden i.S.d. Art. 82 DSGVO darstellt und wer die Beweislast dafür trägt, dass geeignete Maßnahmen zum Schutz der personenbezogenen Daten getroffen wurden.

Schaden: Die Befürchtung, dass ein Missbrauch von personenbezogenen Daten erfolgen wird, kann dann einen

immateriellen Schaden nach Art. 82 Abs. 1 DSGVO darstellen, wenn die betroffene Person nachweisen kann, dass sie tatsächlich einen realen und sicheren emotionalen Schaden erlitten hat. Es reiche demnach nicht aus, wenn die betroffene Person lediglich verärgert ist.

Mit dem Verlust der Daten und der damit vorliegenden Datenpanne lag auch ein tatbestandlicher DSGVO-Verstoß vor. Fraglich war allerdings, ob der Verantwortliche diesen auch zu verschulden hatte.

Zur Frage, ob ein **Haftungsausschluss** in Betracht kommt, wenn der Datenverstoß von einem Dritten ausging, führt der Generalanwalt aus, dass dies für sich genommen keinen solchen Ausschluss begründen kann. Hierzu muss der Verantwortliche vielmehr nachweisen, dass er in keinerlei Hinsicht für den Verstoß verantwortlich ist. Im Kern kommt es damit darauf an, ob der Verantwortliche die Daten angemessen gesichert hat:

Bei angemessener Datensicherheit i.S.d. Art. 24, 32 DSGVO hat der Verantwortliche Schäden eines Hackerangriffs nicht zu verschulden und muss keinen DSGVO-Schadensersatz zahlen.

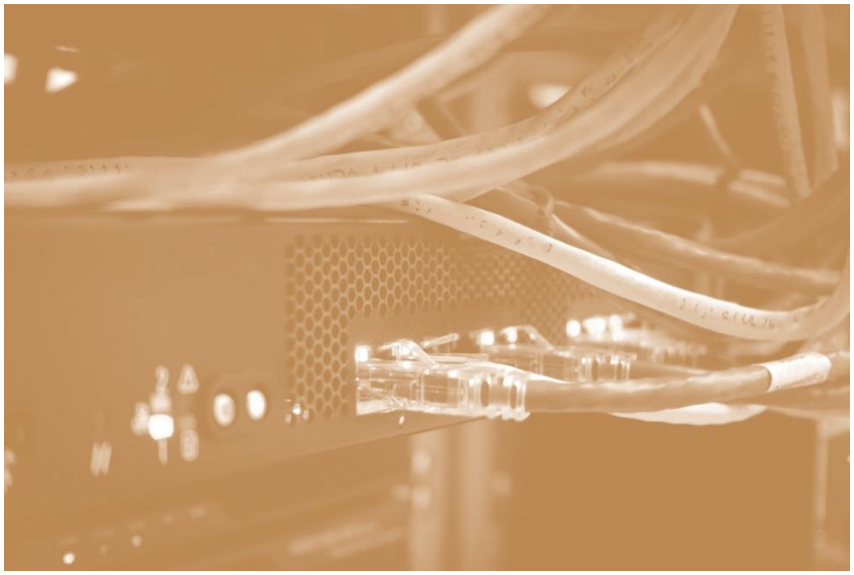
Wann aber liegt eine angemessene Datensicherheit vor?

Der Generalanwalt stellt diesbezüglich fest, dass allein das Vorliegen einer Verletzung des Schutzes von personenbezogenen Daten nicht ausreicht, um festzustellen, ob die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten ungeeignet waren. Hierzu muss vielmehr eine Prüfung des Einzelfalles stattfinden, in der die konkreten Maßnahmen, deren Umsetzung unter Berücksichtigung der technischen Möglichkeiten und die Interessen der Betroffenen zu beachten sind.

Weiter stellt der Generalanwalt fest, dass die Beweislast, ob die ergriffenen Maßnahmen geeignet waren, beim Verantwortlichen liegt. Dies folgt vor allem aus dem Umstand, dass es dem Betroffenen aufgrund des Informationsdefizits nicht möglich sei, die Ungeeignetheit nachzuweisen. Die zulässigen Beweismittel und deren Beweiskraft sind von den nationalen Gerichten zu bestimmen. Im deutschen Recht wird hier das Institut der sekundären Beweislast zur Anwendung kommen können: Der Betroffene weist die Anknüpfungstatsachen nach – der Verantwortliche und potentielle Anspruchsgegner muss sich dann entlasten.

Es ist offen, ob der EuGH der Entscheidung folgt. Sie hat das Potential zur erheblichen Sicherheit für die Unternehmen, die Opfer von Hackerangriffen geworden sind. Allerdings bringt sie auch klare Lasten mit sich: Der Verantwortliche muss letztlich darlegen, dass er angemessene technische und organisatorische Maßnahmen implementiert hatte und es dennoch zu dem Angriff kam. Das erfordert eine umfassende Dokumentation (und natürlich entsprechende Vorarbeit in puncto Datensicherheit).

Letztere, die IT-Sicherheit, wird ohnehin zunehmend wichtig und zur Managementaufgabe: Der Cyber-Vorstand muss seiner neuen Rolle gerecht werden. Mehr dazu lesen Sie, unabhängig von der vorstehenden EuGH-Rechtsprechung, unter https://www.deutscheranwaltspiegel.de/anwaltspiegel/cybersecurity/cybersecurity-ist-c-level-aufgabe-31306/ und https://www.boersen-zeitung.de/recht-kapitalmarkt/was-der-cyber-vorstand-leisten-sollte



EuGH zum Auskunftsrecht: Was ist als Kopie herauszugeben?

Das Auskunftsrecht nach Art. 15 DSGVO umfasst auch die Überlassung von Kopien. Umstritten ist, wie umfangreich dieser Anspruch auf Überlassung von Kopien wirklich ist. Der EuGH hatte zu prüfen, ob die

Überlassung einer aggregierten Darstellung ausreicht und hat dies für möglich erachtet.

Die viel diskutierte Frage, wie weit das Recht betroffener Personen auf Erhalt einer Kopie aus Art. 15 Abs. 3 DSGVO tatsächlich geht, wurde in einem am 4. Mai 2023 veröffentlichten Urteil vom EuGH (Rs. C-487/21) beantwortet. Das Urteil erging im Rahmen eines Vorabentscheidungsersuchens des österreichischen Bundesverwaltungsgerichts von August 2021. Die Schlussanträge hierzu besprachen wir bereits in unserem Newsletter im Februar 2023.

Die Vorlagefragen

Vom vorlegenden Gericht wurde gefragt, was genau unter einer „Kopie" im Sinne von Art. 15 Abs. 3 DSGVO zu verstehen ist und ob es für die Erfüllung des Anspruchs ausreicht, die konkreten Daten des Anspruchstellers in einer zusammenfassenden Übersicht zur Verfügung zu stellen. Im Ausgangsrechtsstreit verlangte der Kläger stattdessen eine Kopie sämtlicher Dokumente wie E-Mails und Datenbankenauszüge, die neben seinen Daten auch weitergehende Informationen über den Kontext enthielten.

Entscheidung des EuGH

Der EuGH kam zu dem Ergebnis, dass betroffene Personen nach Art. 15 Abs. 3 DSGVO grundsätzlich das Recht haben, eine originalgetreue und verständliche Reproduktion der sie betreffenden personenbezogenen Daten zu erhalten. Dies kann jedoch nicht über das hinausgehen, was auch im Rahmen der Auskunft an sich (Art. 15 Abs. 1 DSGVO) zu übermitteln ist. Das bedeutet, dass gerade keine Kopien ganzer Dokumente, die nicht ausschließlich Daten der betroffenen Person enthalten, herauszugeben sind. Stattdessen genügt es grundsätzlich, die konkreten Einzeldaten der Person in einer Tabelle oder sonstigen Übersicht zusammenzutragen. Kurzum: Die Übermittlung in aggregierter Form ist ausreichend, wenn damit dem Zweck des Rechts auf Kopie, die Auskunft nach Art. 15 Abs. 1 DSGVO verständlich zu machen, genüge getan ist.

Zu beachten ist, dass die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form übermittelt werden müssen (Transparenzgrundsatz). Dies soll gewährleisten, dass die Rechte auf Berichtigung, Löschung oder Einschränkung der

Verarbeitung auch wirksam ausgeübt werden können. Denn ohne die Verständlichkeit der Daten lässt sich auch nicht die Rechtmäßigkeit der Verarbeitung überprüfen. Es kann für die wirksame Ausübung der Betroffenenrechte daher unerlässlich sein, auch Kontextinformationen zu kennen. Dies ist der Fall, wenn Daten aus anderen Daten generiert wurden oder Daten gerade auf einer fehlenden Angabe beruhen (sog. freie Felder). Ausnahmsweise kann dann eine Kopie von Auszügen von Dokumenten, von ganzen Dokumenten oder von Datenbankauszügen verlangt werden, die Informationen über den Kontext enthalten. Dabei ist jedoch Rücksicht auf die Rechte und Freiheiten anderer Personen zu nehmen, auch auf Geschäftsgeheimnisse und Urheberrechte.

Zum Begriff der „Informationen“ in Art. 15 Abs. 3 S. 3 DSGVO führt der EuGH aus, dass damit nichts Anderes gemeint sein kann, als die nach Art. 15 Abs. 3 Satz 1 DSGVO zu übermittelnde Kopie. Das hat zur Folge, dass der Umfang des Anspruchs nicht nur aufgrund der Form der Antragstellung unterschiedlich ausfallen kann. Auch nach elektronischer Antragstellung gelten demnach die obigen Ausführungen und die Kopien müssen keine weiterführenden Informationen wie zum Beispiel Metadaten enthalten (sofern diese nicht schon in der Auskunft nach Art. 15 Abs. 1 DSGVO enthalten und dann auch unterlegt sein müssen, etwa Informationen über ein spezifisches Nutzungsverhalten).

Im Ergebnis entspricht dieses Urteil den bereits erwähnten Schlussanträgen. Es ist durchaus geeignet, den Verantwortlichen, die die Kopien herauszugeben haben, Rechtssicherheit zu verschaffen. Trotzdem wird es vom Einzelfall abhängig bleiben, was wirklich für das Verständnis der betroffenen Person relevant und somit auch herauszugeben ist.

Die Herausgabe von Patientenakten über Art. 15 DSGVO für Ansprüche außerhalb des Datenschutzrechts

Darf ein Patient eine Kopie der Patientenakte vom behandelnden Arzt verlangen, wenn ich diese zur Überprüfung arzthaftungsrechtlicher Ansprüche benötige? Darf der Arzt in diesem Fall ein Entgelt dafür verlangen? Mit diesen Fragen hat sich der Generalanwalt Emiliou beim EuGH in aktuellen Schlussanträgen auseinandergesetzt: Auskunft ist unabhängig von den Absichten der betroffenen Person zu erteilen, eine Kostenerstattung über nationale Vorschriften soll aber möglich sein.

Der Anspruch auf Auskunft über die Verarbeitung personenbezogener Daten sowie der damit einhergehende Anspruch auf Herausgabe einer Kopie dieser Daten (Art. 15 Abs. 1, 3 DSGVO) werden im Datenschutzrecht weitreichend diskutiert. Mit solchen Kopien können die betroffenen Personen die Richtigkeit der Verarbeitung ihrer personenbezogenen Daten überprüfen und mit dieser Kenntnis bei gegebenem Anlass ihr Recht auf Berichtigung, Löschung oder Einschränkung der Datenverarbeitung (Art. 16 ff. DSGVO) geltend machen. Dies ist auch der in Erwägungsgrund 63 zur DSGVO beschriebene Zweck des Auskunfts- und Kopieanspruchs.

Verwendung von Kopien zu datenschutzfremden Zwecken

Die aufgrund von Art. 15 Abs. 3 DSGVO herauszugebenden Kopien werden in der Praxis jedoch nicht ausschließlich zu diesen datenschutzrechtlichen Zwecken verwendet. Das liegt daran, dass für den Anspruch – bis auf eine tatsächlich erfolgte Datenverarbeitung – keine weiteren Voraussetzungen erfüllt sein müssen und die betroffene Person ohne großen Aufwand Zugang zu den Kopien erhalten kann. Die erhaltenen Informationen können beispielsweise in Zivilprozessen zur Stärkung der eigenen Position verwendet werden, um Ansprüche, die nichts mit datenschutzrechtlichen Betroffenenrechten zu tun haben müssen, besser untermauern zu können. Ob dies zu einem „discovery-Ansatz" im deutschen Zivilprozess führt, haben wir in der letzten Ausgabe der RDi näher beleuchtet (bei Interesse fragen Sie uns gerne nach dem Aufsatz) und auch in unserem Blog Digitalisierung & Recht näher erläutert.

Da der Verantwortliche die Kopien nach Art. 12 DSGVO grundsätzlich unentgeltlich herauszugeben hat, bestehen seitens der Betroffenen keine Hürden, ihr Recht auch zu diesen – datenschutzfremden – Zwecken geltend zu machen. Dies kann aber, je nach Datenmenge und Auffindbarkeit der Daten, zu einem großen Aufwand bei den Verantwortlichen führen. Die DSGVO ermöglicht in Art. 23 DSGVO jedoch, unter gewissen Voraussetzungen unter anderem die Rechte aus Art. 15 DSGVO und damit auch den Grundsatz der Unentgeltlichkeit im nationalen Recht einzuschränken (sog. Öffnungsklausel).

In einem anhängigen Vorabentscheidungsverfahren vor dem EuGH (Rs. C-307/22), zu dem nun die Schlussanträge des Generalanwalts vorliegen, geht es darum, ob trotz Verfolgung datenschutzfremder Zwecke eine Datenkopie gem. Art. 15 Abs. 3 DSGVO zur Verfügung gestellt werden muss. Konkret forderte ein Patient von seinem Zahnarzt die unentgeltliche Herausgabe der Patientenakte, um einen vermuteten Behandlungsfehler belegen und einen daraus resultierenden Arzthaftungsanspruch begründen zu können. In dem zugrundeliegenden Verfahren vor dem Bundesgerichtshof (BGH) ist der Arzt der Auffassung, nur gegen ein Entgelt zur Herausgabe der Akte verpflichtet zu sein. Eine entsprechende nationale Regelung zur Kostenerstattung bei Herausgabe der Patientenakte findet sich in § 630g Abs. 2 Satz 2 BGB. Dem EuGH wurde deshalb auch die Frage zur Vorabentscheidung vorgelegt, ob eine solche vor Inkrafttreten

der DSGVO erlassene nationale Vorschrift eine unzulässige Beschränkung des Rechts auf Kopie nach Art. 15 Abs. 3 DSGVO darstellt. Schließlich steht zur Frage, wie umfangreich eine etwaig herauszugebende Kopie sein muss, wie bereits zuvor in diesem Newsletter besprochen.

Die Ansichten des Generalanwalts

In den Schlussanträgen vertritt der Generalanwalt Emiliou die Ansicht, dass die Pflicht zur Auskunft und zur Herausgabe von Kopien grundsätzlich unabhängig von den Absichten der betroffenen Person ist. Eine Patientenakte ist danach auch dann herauszugeben, wenn der Patient nicht die Überprüfung der Rechtmäßigkeit der Datenverarbeitung anstrebt.

Dies ist folgerichtig – der Auskunftsanspruch ist bedingungslos. Er gilt allerdings nicht grenzenlos:

Eine **Kostenregelung** im nationalen Recht, wie § 630g Abs. 2 Satz 2 BGB, ist nach seiner Auffassung eine zulässige Einschränkung des Auskunftsrechts, sofern die Anforderungen von Art. 23 DSGVO eingehalten werden. Insbesondere muss die nationale Vorschrift den Wesensgehalt der Grundrechte und Grundfreiheiten achten sowie notwendig und verhältnismäßig sein. Die erhobenen Kosten müssen dafür „strikt auf die tatsächlich anfallenden Kosten beschränkt" sein, womit z.B. Materialkosten und Arbeitszeit erstattungsfähig werden.

Hinsichtlich des **Umfangs der herauszugebenden** Kopie schließt sich Emiliou den Schlussanträgen des Generalanwalts Pitruzzella und damit einem weiteren EuGH-Verfahren an, in welchem es speziell um diese Frage der Reichweite des Kopieanspruchs geht (Rs. C-487/21; siehe dazu oben in diesem Newsletter). Wesentlich ist, dass durch die Kopie die Verständlichkeit der verarbeiteten Daten für die betroffene Person gewährleistet wird. Dafür kann es ausreichen, die Daten in einer Übersicht zusammenzustellen (aggregierte Daten). Es kann aber auch erforderlich sein, ganze Dokumente zur Verfügung zu stellen, die den Kontext der Datenverarbeitung erläutern.

Sollte der EuGH mit seinem Urteil den Schlussanträgen folgen, würde dies für die Praxis bedeuten, dass die Herausgabe von Kopien verarbeiteter personenbezogener Daten nicht pauschal verweigert werden kann, weil diese nicht zur Überprüfung der Richtigkeit der Datenverarbeitung dienen sollen. Jedoch kann eine Erstattung der

tatsächlich anfallenden Kosten verlangt werden, sofern diese bei dem Verpflichteten tatsächlich angefallen sind. Und auch der Umfang ist begrenzt: Es besteht kein allgemeines Recht auf Herausgabe der gesamten Patientenakte mit sämtlichen Dokumenten. Zu überlassen sind nur die Dokumente oder Auszüge daraus, die wirklich die Auskunft nach Art. 15 Abs. 1 DSGVO erläutern und für ihr Verständnis benötigt werden. Umfangreich sind Kopien danach weiterhin in vielen Fällen, jedoch seltener uferlos. Das endgültige Urteil bleibt abzuwarten, wobei der EuGH in aller Regel den Schlussanträgen folgt.

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

Philipp Schoel
+49(0)221 65065-200
philipp.schoel@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