Auswirkung der aktuellen EuGH-Rechtsprechung zu Art. 82 DSGVO auf die Cyber-Versicherung

Der EuGH hat in drei kürzlich ergangenen Urteilen (C-687/21, C-340/21 und C-456/22) seine Rechtsprechung zur datenschutzrechtlichen Verantwortlichkeit von Unternehmen für die eigene IT- und Datensicherheit sowie zu den Voraussetzungen der Anerkennung eines immateriellen Schadenersatzes gem. Art. 82 DSGVO konkretisiert. Das Gericht schafft damit weiter Klarheit hinsichtlich der Frage, wann Betroffene bei Abhandenkommen von Daten einen Anspruch auf Ersatz von immateriellen Schäden gegen Unternehmen haben. Damit wird der Trend des EuGH fortgesetzt, die Haftung von Unternehmen zu verschärfen, so dass zukünftig vermehrt mit Inanspruchnahmen zu rechnen ist. Dies wird auch Einfluss auf die Cyber-Versicherung haben, da Sachverhalte, in denen Unternehmen von Kunden auf Schadenersatz gem. Art. 82 DSGVO in Anspruch genommen werden, grundsätzlich unter die Deckung von Cyber-Policen fallen. Der Beitrag fasst die EuGH-Urteile C-687/21, C-340/21 sowie C-456/22 kurz zusammen, erläutert die Voraussetzungen eines Schmerzensgeldanspruchs gem. Art. 82 DSGVO und schließt mit einem Blick auf die Versicherbarkeit solcher Ansprüche in der Cyber-Versicherung.

EuGH, Urt. v. 15.01.2024, Az. C-687/21 – Kein Schmerzensgeld ohne fremde Kenntnisnahme

Ein Verbraucher kaufte bei einem Elektrofachhändler ein Haushaltsgerät. An der Warenausgabe wurde das Gerät mitsamt den Kauf- und Kreditvertragsunterlagen aber versehentlich einem anderen sich vordrängelnden Kunden ausgehändigt. Aufgrund der Unterlagen kannte der Drängler nun die Anschrift, den Arbeitgeber und die Einkünfte des Käufers. Einem Mitarbeiter des Elektronikfachhändlers fiel der Irrtum auf und nach kurzer Zeit wurden dem wahren Käufer das Gerät sowie die Unterlagen ausgehändigt. Der Kunde hat daraufhin Klage auf Ersatz des immateriellen Schadens erhoben, den er aufgrund des Irrtums der Angestellten und des daraus resultierenden Risikos des Verlusts der Kontrolle über seine personenbezogenen Daten erlitten habe.

Der EuGH verneinte einen Anspruch auf Schmerzensgeld gem. Art. 82 DSGVO. Ein immaterieller Schaden liegt laut EuGH nicht schon dann vor, wenn eine Person, deren personenbezogene Daten an einen unbefugten Dritten weitergegeben wurden, der diese aber erwiesenermaßen nicht zur Kenntnis genommen hat, dennoch befürchtet, dass die Daten kopiert wurden und in Zukunft weitergegeben oder gar missbraucht werden könnten. Ein lediglich ungutes Gefühl hinsichtlich seiner Daten begründet somit noch keinen Anspruch auf immateriellen Schadenersatz, insbesondere dann nicht, wenn die Daten von keinem Unbefugten zur Kenntnis genommen wurden.

EuGH, Urt. v. 14.12.2023, Az. C-340/21 – Schmerzensgeld bei Angst vor Datenmissbrauch

Anders verhielt es sich in einem Sachverhalt, in dem eine bulgarische Behörde Opfer eines Hackerangriffs wurde, bei dem Steuer- und Sozialversicherungsdaten von mehr als 6 Millionen Betroffenen exfiltriert und im Internet veröffentlicht wurden. Eine hiervon Betroffene verklagte die Behörde auf Ersatz ihres immateriellen Schadens, weil sie einen Missbrauch ihrer Daten durch Dritte befürchtete.

Der EuGH bejahte in diesem Fall eine Schadenersatzpflicht. Allein die begründete Angst eines künftigen Datenmissbrauchs reicht danach aus, um einen Schmerzensgeldanspruch anzunehmen. Die Behörde hat es unterlassen, geeignete technische und organisatorische Maßnahmen zu treffen, um eine angemessene Sicherheit der Verarbeitung der personenbezogenen Daten sicherzustellen. Es besteht allerdings kein Automatismus, dass Schutzmaßnahmen stets als ungeeignet oder unzureichend anzusehen sind, wenn es zu einem erfolgreichen unbefugten Zugang gekommen ist. Die Behörde hätte sich jedoch nur entlasten können, wenn sie nachgewiesen hätte, dass die getroffenen Maßnahmen zur Abwehr von Hackerangriffen geeignet waren und sie in keinerlei Hinsicht für den Schaden verantwortlich ist.

EuGH, Urt. v. 14.12.2023, Az. C-456/22 – Keine Bagatellgrenze bei Schmerzensgeld

Erwähnenswert ist zudem ein Urteil des EuGH, dem ein Sachverhalt zugrunde lag, in dem die Namen zweier Personen von einer Gemeinde in Baden-Württemberg veröffentlicht wurden. Die Gemeinde hatte ohne rechtliche Grundlage auf ihrer Website die Tagesordnung einer Gemeinderatssitzung veröffentlicht, in der die Namen der Kläger genannt waren, sowie ein Verwaltungsgerichtsurteil, in dessen Rubrum die Namen sowie die Anschrift der Kläger enthalten waren. Obwohl der Eintrag nur kurze Zeit später wieder gelöscht wurde, machten die Betroffenen Schadenersatz nach Art. 82 DSGVO aufgrund der unzulässigen Veröffentlichung ihrer personenbezogenen Daten geltend.

Der EuGH bejahte einen Anspruch gem. Art. 82 DSGVO. Obwohl es sich nur um eine Bagatelle handelte, hätte die Veröffentlichung personenbezogener Daten im Internet und der daraus resultierende kurzzeitige Verlust der Hoheit über die Daten den betroffenen Personen einen immateriellen Schaden im Sinne von Art. 82 DSGVO zufügen können. Die betroffenen Personen müssen lediglich den Nachweis erbringen, dass sie tatsächlich einen solchen Schaden – so geringfügig er auch sein mag – erlitten haben.

Es besteht gem. dem EuGH somit keine Bagatellgrenze für einen Schaden im Sinne des Art. 82 DSGVO und das Urteil stärkt die Rechte von Betroffenen auf Schadenersatz für immaterielle Schäden.

Voraussetzungen eines Schmerzensgeldanspruchs gem. Art. 82 DSGVO

Den Urteilen des EuGH ist gemein, dass es stets um die Frage ging, ob die Betroffenen einen Anspruch aus Art. 82 DSGVO haben. Art. 82 DSGVO stellt eine eigenständige, unmittelbar geltende, deliktsrechtliche Anspruchsgrundlage dar, die zum einen den Zweck hat, einen Ausgleich für durch Datenschutzrechtsverletzungen erlittene materielle und immaterielle Schäden zu schaffen und zum anderen Datenschutzrechtsverletzungen zu sanktionieren, um weitere Verstöße zu verhindern.

Voraussetzung für einen Anspruch aus Art. 82 DSGVO ist zunächst, dass ein Verstoß gegen eine Bestimmung der DSGVO vorliegt. Zudem muss der Verantwortliche den Datenschutzverstoß fahrlässig oder vorsätzlich verschuldet haben. Das Verschulden wird grundsätzlich vermutet. Um sich zu entlasten, muss der Verantwortliche daher nachweisen, für das schadenauslösende Ereignis nicht verantwortlich gewesen zu sein, indem er geeignete technische und organisatorische Maßnahmen getroffen hat, um eine angemessene Sicherheit bei der Verarbeitung der personenbezogenen Daten sicherzustellen. Kann das von einem Datenleck oder einer Exfiltration betroffene Unternehmen z.B. nachweisen, dass alles Zumutbare getan wurde, um dem Abhandenkommen der Daten vorzubeugen, ist eine Entlastung ggf. möglich.

Elementarer Kern eines begründeten Schadenersatzanspruches nach Art. 82 DSGVO ist nach ständiger Rechtsprechung insbesondere der Eintritt eines kausalen Schadens. Dies können zum einen materielle Schäden sein, die finanziell konkret beziffert werden (z.B. Vermögensverluste durch die Nutzung der Zahlungsdaten des Betroffenen). Zum anderen kommt auch der Ersatz von immateriellen Schäden (= Schmerzensgeld) in Betracht. Um einen Schmerzensgeldanspruch zu begründen, muss nach Ansicht der herrschenden Meinung dem Betroffenen ein spürbarer Nachteil entstanden sein, der aus einer objektiv nachvollziehbaren, mit gewissem Gewicht erfolgten Beeinträchtigung von persönlichkeitsbezogenen Belangen resultiert.

Versicherbarkeit in der Cyber-Versicherung

„Erfreulich ist, dass für Sachverhalte, in denen Unternehmen von Kunden auf Schadenersatz gem. Art. 82 DSGVO in Anspruch genommen werden, grundsätzlich Deckung im Rahmen von Cyber-Versicherungen besteht. Der Anwendungsbereich der Cyber-Versicherung ist in aller Regel eröffnet, da ein sog. deckungsauslösendes Ereignis in Form einer Verletzung datenschutzrechtlicher Bestimmungen vorliegt," beruhigt Dr. Marcel Straub, Head of Legal bei Finlex. „Als Daten gelten hierbei in vielen Bedingungswerken auch physische Dokumente bzw. nicht-elektronische Daten, so dass auch im Sachverhalt des Elektrofachhändlers (Az. C-687/21), bei welchem Kauf- und Kreditvertragsunterlagen versehentlich einem anderen Kunden ausgehändigt wurden, ein deckungsauslösendes Ereignis anzunehmen wäre," ergänzt der Syndikusrechtsanwalt.

Liegt ein deckungsauslösendes Ereignis vor, ist der Haftpflichtteil der Police ansteuerbar. Der Versicherungsschutz umfasst hierbei zunächst die Prüfung der Haftpflichtfrage durch den Versicherer. Auf Grundlage der Einschätzung gewährt der Versicherer sodann Versicherungsschutz für die gerichtliche und außergerichtliche Abwehr von unbegründeten Ansprüchen oder stellt das versicherte Unternehmen von begründeten Ansprüchen frei.

„Für die vorliegenden Fälle bedeutet dies, dass ein Versicherer in allen drei EuGH-Fällen zum einen die angefallenen angemessenen Abwehrkosten hätte tragen müssen. Zum anderen wäre vom Versicherungsschutz grundsätzlich auch umfasst, dass ein Versicherer den vom Unternehmen an die Kunden zu leistenden Schadenersatz tragen müsste. In den Fällen Az. C-340/21 und Az. C-456/22 bestünde daher Versicherungsschutz sowohl für die Kosten der erfolglosen Abwehr der geltend gemachten Ansprüche als auch für die zu leistenden Schadenersatzansprüche gem. Art. 82 DSGVO.", fasst Dr. Straub zusammen.

Ausblick

Die Urteile erweitern die bestehende Rechtsprechung zu Art. 82 DSGVO und präzisieren die bereits erkennbare Linie des EuGH. Durch die Betonung der Notwendigkeit einer konkreten und individuellen Bewertung von Sicherheitsmaßnahmen sowie die Verantwortung von Datenverarbeitern und die Verneinung einer Bagatellgrenze für immaterielle Schäden stärkt der EuGH weiter die Rechte von betroffenen Personen bei Datenschutzverletzungen.

Dr. Straub: „Von den mehr als 200 Cyber-Claims, die wir mit der Finlex Claims-Abteilung in den letzten zwei Jahren begleitet haben, waren bislang nur sehr wenige Ansprüche gegen Unternehmen auf einen Schadenersatz aus Art. 82 DSGVO gerichtet. Aufgrund der neuerlichen Rechtsprechung ist zukünftig jedoch vermehrt mit dahingehenden Inanspruchnahmen zu rechnen. Unternehmen sind daher gut beraten – auch im Hinblick auf das Kostenrisiko wegen Ansprüchen aus Art. 82 DSGVO – eine Cyber-Police abzuschließen. Selbst wenn sich ein etwaiger Anspruch auf Schadenersatz gem. Art. 82 DSGVO für den einzelnen Betroffenen in der Regel lediglich im drei- oder vierstelligen

Bereich bewegt, droht bei einem Sachverhalt mit einer Vielzahl an Betroffenen ein Millionenschaden. Geht man beispielsweise davon aus, dass einem mittelständischen Unternehmen 10.000 Kundendaten entwendet werden und jedem Betroffenen 500 Euro Schmerzensgeld zustehen, würde sich die Gesamtsumme möglicher Schmerzensgeldansprüchen ohne Rechtsanwalts- und Gerichtskosten bereits auf 5 Mio. Euro summieren. Unternehmen ist daher dringend geraten, ihre IT und die Kundendaten zu schützen. Darüber hinaus sollte unbedingt das Risikomanagement geschärft werden und im Hinblick auf die Beweislast eine belastbare Dokumentation über getroffene Maßnahmen etabliert werden. Zudem sollte sich jedes Unternehmen ernsthaft darüber Gedanken machen, eine Cyber-Versicherung abzuschließen, um das Kostenrisiko zu minimieren und um im Fall der Fälle einen Spezialisten an seiner Seite zu haben."

Pressekontakt

Finlex GmbH

Denise Jetzki | Head of Marketing & Communication
E-Mail: marketing@finlex.de
Telefon: +49 (0) 69 / 8700 142-00

finlex.io