Uferlose Schadensersatzrisiken nach neuen EuGH-Entscheidungen?

Der EuGH hat in zwei Entscheidungen die Anforderungen an einen immateriellen Schadensersatz nach DSGVO-Verstoß konkretisiert. Hoch praxisrelevant sind dabei gerade die Anforderungen an Schadensersatzforderungen gegen die Opfer eines Hackerangriffs: Müssen Unternehmen auch dann noch Schadensersatz an betroffene Personen zahlen? In der Praxis wird bereits befürchtet, dass nun die Massenklagen anrollen. Aber ist das wirklich so? Eine genaue Betrachtung der beiden Urteile lohnt sich!

Kommt es nach einem schuldhaften DSGVO-Verstoß zu einem Vermögensschaden, liegen Schadensersatzansprüche auf der Hand. Was aber ist, wenn es an einem materiellen Schaden fehlt, die Betroffenen allerdings immaterielle Schäden beklagen? Wie intensiv muss die Beeinträchtigung sein, um einen Ausgleich in Geld zu erhalten – und wie ist die Beeinträchtigung nachzuweisen?

Insbesondere: Was gilt nach einem Hackerangriff, wenn Daten der Betroffenen unbefugt eingesehen, wurden? Muss das Opfer des Hackerangriffs wegen des Vorfalls an sich Schadensersatz leisten?

Der EuGH hat sich dieser Fragen angenommen. Im ersten Fall ging es um die bloße Befürchtung eines Datenmissbrauchs nach einem Hackerangriff (Rs. C-340/21), im zweiten Fall um die Namensnennung in öffentlichen Dokumenten (Rs. C-456/22).

Angst vor Datenmissbrauch und die Anforderungen an die Datensicherheit

Der Fall

Hacker haben auf das Computersystem der bulgarischen Behörde NAP zugegriffen. Laut Medienberichten wurde dabei personenbezogene Steuer- und Sozialversicherungsdaten von mehreren Millionen Personen abgegriffen und im Internet

veröffentlicht. Die Klägerin des Ausgangsverfahrens verlangte daraufhin von der NAP Schadensersatz aus Art. 82 DSGVO, wozu der EuGH im Rahmen eines Vorabentscheidungsverfahrens angerufen wurde. Zu den Schlussanträgen in diesem Verfahren berichteten wir in unserem Newsletter aus Mai 2023.

Die EuGH-Entscheidung

Die EuGH-Entscheidung erging am 14.12.2023 (Rs. C-340/21). Die für die Praxis wichtigsten Aussagen des EuGH betreffen die Anforderungen an die **angemessene Datensicherheit** und den **immateriellen Schadensnachweis**:

1. Ein (erfolgreicher) Hackerangriff alleine belegt nicht, dass das angegriffene Unternehmen keine ausreichenden technischen und organisatorischen Schutzmaßnahmen ergriffen hatte.

   Auch im neuen IT-Sicherheitsrecht, das bislang im Entwurf vorliegt, werden folgerichtig lediglich Risikomanagementmaßnahmen verlangt, die die Auswirkungen von Cyber-Attacken geringhalten. Vermieden werden können diese bisweilen selbst bei optimaler IT-Sicherheit nicht.

2. Allerdings trägt das angegriffene Unternehmen auch im Rahmen einer Schadensersatzklage die **Beweislast für angemessene Sicherheitsmaßnahmen**. Dieses muss sich entlasten und nicht der Kläger eine unzureichende Sicherheit nachweisen.

3. Ein immaterieller Schaden i.S.d. Art. 82 Abs. 1 DSGVO kann auch schon dann vorliegen, wenn die betroffene Person infolge eines Verstoßes gegen die DSGVO **die Befürchtung hat**, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten. Der Datenmissbrauch muss (noch) nicht stattgefunden haben. Allerdings muss die betroffene Person ihre **Befürchtung nachweisen**.

Voraussetzungen des immateriellen Schadensersatzes

Der Fall

Die Gemeinde Ummendorf hatte auf ihrer Internetseite für einen Zeitraum von drei Tagen ohne Einwilligung der Kläger deren

Namen sowie Anschrift im Zusammenhang mit der Tagesordnung einer Gemeinderatssitzung sowie eines Gerichtsurteils veröffentlicht. Die Kläger machten wegen der unzulässigen Offenlegung ihrer Daten immateriellen Schadensersatz geltend.

Das im Berufungsverfahren mit der Sache befasste Landgericht Ravensburg war sich unsicher, ob tatsächlich ein immaterieller Schaden entstanden ist. Daher bat das LG Ravensburg den EuGH um Auskunft im Rahmen eines Vorabentscheidungsverfahrens zu der Frage, ob die Annahme eines immateriellen Schades einen spürbaren Nachteil und eine objektiv nachvollziehbare Beeinträchtigung persönlichkeitsbezogener Belange erfordert oder ob bereits der kurzzeitige Verlust des Betroffenen über die Hoheit seiner Daten, der ohne spürbare und nachteilige Konsequenzen für den Betroffenen blieb, für die Annahme eines immateriellen Schadens genügt.

Die EuGH-Entscheidung

Das EuGH-Urteil vom 14.12.2023 in dieser Rechtssache C-456/22 ist weitreichend: Die Veröffentlichung der Daten im Internet sowie der daraus resultierende – kurzzeitige – Verlust der Datenhoheit kann zu einem immateriellen Schaden führen. Auch ein Bagatellschaden begründet einen Schadensersatzanspruch. Allerdings muss der Betroffene nachweisen, dass er tatsächlich einen Schaden erlitten hat, wie gering dieser auch sein mag.

Fazit

Der EuGH knüpft inhaltlich an vergangene Urteilen zum immateriellen Schadensersatz an. Bereits in den Verfahren Österreichische Post und Identitätsdiebstahl Rs. C-182/22 und C-189/2 hatte der EuGH klargestellt, dass zwar auch Bagatellschäden vom immateriellen Schadensersatz umfasst sind, jeder Schaden aber nachgewiesen werden muss. Der bloße DSGVO-Verstoß begründet noch keinen Schadensersatzanspruch (wir berichteten hier). Insofern bleibt der EuGH seiner bisherigen Linie treu.

Insgesamt scheinen die Anforderungen aber zunehmend zu sinken. So kann bereits die begründete **Befürchtung** eines Datenmissbrauchs zu einem Schaden führen. Nach Hackerangriffen sind zudem die Opfer in der **Beweislast**, dass die von ihnen ergriffenen Sicherheitsmaßnahmen angemessen waren, um einen Schadensersatzanspruch abzuwehren.

Dies verdeutlicht, wie wichtig eine ausreichende Informationssicherheit im Unternehmen ist – ganz ungeachtet der aktuellen gesetzgeberischen Entwicklungen zum neuen IT-Sicherheitsrecht und dem Cyber Resilience Act aus der EU.

Welche Bedeutung den EuGH-Entscheidungen für die Unternehmenspraxis im Einzelnen zukommen, diskutieren wir mit Ihnen im Rahmen unseres Lunch@Loschelder-Webinars am 31.01.2024. Wir freuen uns über Ihre Anmeldung unter webinare@loschelder.de (Teilnahme kostenfrei, weitere Informationen auch zeitnah hier).

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

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

Dennis Pethke, LL.M.
+49(0)221 65065-337
dennis.pethke@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