Kommunikation & Recht

K&R
10 | Oktober 2023
26. Jahrgang
Seiten 633 - 704

dfv Mediengruppe
Frankfurt am Main

Kommunikation & Recht

21. @kit-Kongress –
11. Forum „Kommunikation & Recht“

Berlin
21. – 23. Juni 2023

Herausgegeben von:
Prof. Dr. Ruth Janal
Thorsten Feldmann
Kerstin Gießübel
Dr. David Jahn

www.kommunikationundrecht.de

dfv Mediengruppe . Frankfurt am Main

@kit

RA Dr. Hauke Hansen und David Schwarze*

Datenschutzrechtliche Schadensersatzklagen als Geschäftsmodell

Kurz und Knapp

Schadenersatzforderungen nach Datenschutzverstößen haben Konjunktur. Hinzu tritt das Phänomen datenschutzrechtlicher Massenverfahren, für die unterschiedliche Teilnehmer am „Klagemarkt" offensiv bei Betroffenen werben. Ziel dieser Verfahren ist es, meist eher geringe Schadensersatzansprüche Einzelner zu sammeln und trotz geringer Einzelbeträge Druck auf Unternehmen auszuüben.

I. Ausgangslage

Zunächst haben allgemein bekannte Verstöße gegen die DSGVO – beispielsweise das unverlangte Zusenden von Werbeemails oder eine verspätete Auskunft gemäß Art. 15 Abs. 1 DSGVO – zu Schadensersatzklagen von Betroffenen geführt. Neuerdings werden erfolgreiche Cyberattacken zum Anlass für datenschutzrechtliche Schadensersatzklagen genommen.[1]

Das Vorgehen der Hacker ist dabei meist gleich: Sind die Angreifer erst erfolgreich in die IT-Systeme eingedrungen, werden die Daten zunächst exfiltriert und im Anschluss verschlüsselt, was oftmals den gesamten Geschäftsbetrieb stillgelegt. Beide Maßnahmen werden zur Grundlage von Lösegeldforderungen gemacht. Wird dies abgelehnt, werden die Kunden- und Mitarbeiterdaten im Darknet veröffentlicht oder zum Verkauf angeboten. Selbst wenn dem Unternehmen also aktuelle Back-ups zur Verfügung stehen und der Betrieb kurzfristig wieder aufgenommen werden kann, können die finanziellen Folgen enorm sein.

Neben drohenden behördlichen Bußgeldern[2] durch Datenschutzbehörden entwickeln sich auch orchestrierte Schadensersatzansprüche betroffener Kunden zu einer ernst zu nehmenden Bedrohung für Unternehmen.

Im Zentrum dieser Ansprüche stehen meist die technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO, die ein Unternehmen zum Schutz personenbezogener Daten ergreifen muss.

II. Unternehmen haften auch zivilrechtlich

Neben der Verfolgung durch eine Behörde können Unternehmen auch zivilrechtlich haftbar gemacht werden, beispielsweise in Form von Klagen auf Schadensersatz. Mögliche Anspruchsgrundlage ist Art. 82 DSGVO, wenn die Hacker Kundendaten im Darknet veröffentlichen. Um Anspruch auf Schadensersatz zu haben, müssen betroffene Personen nachweisbar einen Schaden durch einen Datenschutzverstoß erlitten haben. Ein solcher Verstoß kann beispielsweise bereits in unzureichenden IT-Sicherheitsmaßnahmen der angegriffenen Unternehmen gesehen werden, die nicht dem Stand der Technik entsprechen.[3] Trotz dieses weiten Begriffs des „Stands der Technik" müssen aus rechtlicher Sicht Unternehmen nur angemessene IT-Sicherheitsmaßnahmen ergreifen. Ein vollumfänglicher Schutz und eine absolute Sicherheit muss nicht gewährleistet werden.[4]

Art. 82 DSGVO sieht auch einen Ersatz für immaterielle Schäden vor. Dies sind Beeinträchtigungen, die keine unmittelbar finanziellen (= materiellen) Folgen haben. Dies ist neu und im deutschen Recht die absolute Ausnahme. Beispiele sind entgangene Urlaubsfreuden im Reiserecht oder Schmerzensgeld bei Körperverletzungen. Deutsche Gerichte waren gerade beim Schmerzensgeld immer sehr zurückhaltend und haben es auch bei schwersten Verletzungen regelmäßig bei vierstelligen Beträgen belassen. Anders handhaben es neuerdings insbesondere die deutschen Arbeitsgerichte, wenn es um Datenschutzverstöße geht. Als besonders drastisches Beispiel sei ein Urteil des ArbG Oldenburg erwähnt, das einem Arbeitnehmer ohne konkreten Nachweis eines Schadens 10 000 Euro zugebilligt hat, weil die geforderte datenschutzrechtliche Auskunft zu spät erfolgte.[5] (Gänzlich anders beurteilt hat diese Frage kürzlich das LAG Baden-Württemberg,[6] nach dem die Höhe des Schadensersatzes in ein angemessenes Verhältnis zu zugesprochenem Schmerzensgeld zu setzen ist. Aus Datenschutzverletzungen entstandene Schäden müssten zwar vollständig kompensiert werden – es dürften aber keine überkompensatorischen Schadensersatzpflichten entstehen, die falsche Anreize erzeugen.)

Berühmt geworden ist auch ein Urteil des LG München,[7] das dem Kläger wegen eines von ihm empfundenen „Unwohlseins" einen Schadensersatz in Höhe von 100 Euro zugesprochen hat. Das beklagte Unternehmen hatte auf seiner Webseite dynamische Google Fonts eingesetzt, wodurch nach einem Besuch der Webseite durch den Kläger, dessen dynamische pseudonyme IP-Adresse an Google übermittelt worden war. Dieses Urteil hat im Anschluss zu datenschutzrechtlichen massenhaften Zahlungsaufforderungen gegen Unternehmen geführt.

In der deutschen Rechtsprechung war zudem einige Jahre umstritten, ob einem Kläger bereits dann ein immaterieller Schaden zusteht, wenn „lediglich" Datenschutzvorschriften verletzt wurden, oder ob zusätzlich ein konkreter Schaden

* Mehr über die Autoren erfahren Sie am Ende des Beitrags.

1 Vgl. Schlussanträge des Generalanwaltes beim EuGH, 27. 4. 2023 – C-340/21, GRUR-RS 2023, 8707 – NAP; LG München I, 9. 12. 2021 – 31 O 16606/20, ZD 2022, 242; LG Köln, 18. 5. 2022 – 28 O 328/21, ZD 2022, 506.

2 Gegen British Airways wurde ein Bußgeld von EUR 204 Mio. (später reduziert auf EUR 22 Mio.) verhängt, nachdem Hacker Daten von 400 000 Kunden und Mitarbeitern erlangt hatten. Die Marriott-Gruppe erhielt einen Bußgeldbescheid i. H. v. EUR 110 Mio. (später reduziert auf EUR 20,4 Mio.), nachdem Hacker mutmaßlich Zugriff auf Daten von 300 Mio. Kunden (!) hatten.

3 Orientierung zum Stand der Technik bieten das IT-Grundschutz-Kompendium des Bundesamtes Sicherheit in der Informationstechnik, Stand 2.2023; oder die „Handreichung zum ‚Stand der Technik' des Bundesverband IT-Sicherheit e. V. (TeleTrusT), Stand 5.2023.

4 Vgl. OLG Stuttgart, 1. 3. 2021 – 9 U 34/21, K&R 2021, 748 ff. = BeckRS 2021, 6282, Rn. 39 f., 52; Schlussanträge des Generalanwaltes beim EuGH, 27. 4. 2023 – C-340/21, GRUR-RS 2023, 8707, Rn. 26 – NAP; *Wybitul*, NJW 2020, 2577, Rn. 3.f.

5 AG Oldenburg, 9. 2. 2023 – 3 Ca 150/21, BeckRS 2023, 3950.

6 LAG Baden-Württemberg, 27. 1. 2023 – 12 Sa 56/21, NZA-RR 2022, 672, Rn. 219 f.

7 LG München, 20. 1. 2022 – 3 O 17493/20, K&R 2022, 865 ff. = ZD 2022, 290.

bewiesen werden muss.[8] Der EuGH hat nun klargestellt, dass neben einer Rechtsverletzung auch ein kausaler Schaden vorliegen muss, um einen Ersatzanspruch gem. Art. 82 DSGVO zu begründen. [9]

III. Schwierige Schadensbemessung

Eine entscheidende Frage aber ließ der EuGH unbeantwortet: Ab wann liegt ein immaterieller Schaden vor? Die DSGVO enthalte, so der EuGH, keine Bestimmung, die sich dieser Frage widme. Daher sei es Sache der Mitgliedsstaaten, Klageverfahren auszugestalten, die Kriterien für die Ermittlung geschuldeten Schadensersatzes festlegen. Aus dem europäischen Recht folge lediglich, dass einerseits die effektive Einhaltung der DSGVO gesichert sein müsse, andererseits aber Gerichte über den tatsächlich erlittenen Schaden hinaus auch keinerlei Strafschadensersatz zubilligten.

Es bleiben zahlreiche Fragen offen: Eine unverlangt, eine verspätete Auskunft, eine nicht gelöschte alte Adresse oder der Kontrollverlust über im Darknet veröffentlichte Kontodaten – begründet dies schon einen immateriellen Schaden? Ab wann wird ein individuell empfundenes ungutes Gefühl zu einem immateriellen Schaden im Sinne der DSGVO? Und hängt ein Schadensersatzanspruch von der betroffenen Person ab? Das heißt, sollen sehr sensible oder rechthaberische Personen, die sich über derartige Verstöße besonders stark ärgern, eher einen immateriellen Schaden geltend machen können als andere? Und schließlich: Werden die Gerichte in Anlehnung an Bußgeldkataloge für bestimmte Datenschutzverstöße Schadensersatzbeträge festlegen?

Zu diesen wichtigen Aspekten hat der EuGH keine Klarheit geschaffen. Betroffene und Unternehmen werden weiter vor Gericht viele Einzelfälle ausfechten, und der EuGH, der sich für diese Fragen für nicht zuständig erklärt hat, kann nur eingreifen, wenn er durch nationale Urteile den über allem schwebenden europäischen Effektivitätsgrundsatz gefährdet sieht.

Es gibt aber dennoch europäische Leitlinien: So hat der EuGH einerseits einem Strafschadensersatz eine Absage erteilt und eine objektiv nachvollziehbare Beeinträchtigung für einen Schadensersatzanspruch gefordert, gleichzeitig aber einer in Deutschland diskutierten Bagatellgrenze eine Absage erteilt.[10]

IV. Massenklage als Geschäftsmodell

Im Falle des erfolgreichen Hackerangriffs auf einen Dienstleister des Vermögensverwalters Scalable Capital hat das LG München einem Kunden, dessen Daten von den Hackern veröffentlicht wurden, einen Schadensersatzanspruch in Höhe von 2500 Euro zugesprochen – und das trotz TÜV-zertifizierter IT-Sicherheit beim Dienstleister. Der Kläger wurde von dem Prozessfinanzierer EuGD (Europäische Gesellschaft für Datenschutz mbH) unterstützt, weitere Klagen wurden an mehreren deutschen Gerichten eingereicht. Berücksichtigt man, dass von der Datenpanne insgesamt rund 33 200 Personen betroffen waren, entsteht ein Risiko in Millionenhöhe.

Diese Entwicklungen haben das Interesse der Klageindustrie geweckt.[11] Da die einzelnen Ansprüche in diesen Fällen eher von geringer Höhe sind, lohnt sich das Tätigwerden für die kommerziellen Kläger erst in der Masse. Es gibt mittlerweile eine Reihe von Anwaltskanzleien, die sich auf die Durchsetzung von Schadensersatzansprüchen im Zusammenhang mit Datenschutzverletzungen spezialisiert haben. Dabei haben sich unterschiedliche Geschäftsmodelle entwickelt. Zum einen existiert ein Abtretungsmodell, bei dem die Ansprüche von betroffenen Personen an ein Unternehmen abgetreten werden, welches diese anschließend im eigenen Namen geltend macht. Zum anderen besteht ein Vermittlungsmodell, bei dem betroffene Personen und Rechtsanwälte bzw. Kanzleien über eine Plattform zusammengebracht werden und die Plattform im Erfolgsfall eine Provision erhält. Daneben hat sich die Methode etabliert, Anspruchsschreiben zu verschicken, in denen die Möglichkeit eines außergerichtlichen Vergleiches angeboten wird.

Bei den Akteuren handelt es sich oft um gut organisierte Verbraucherkanzleien, die von ihren Erfahrungen mit Massenverfahren in Zusammenhang mit dem Diesel-Skandal oder der Insolvenz der US-amerikanischen Bank Lehman Brothers profitieren wollen. Aber auch Prozessfinanzierer und LegalTech-Unternehmen etablieren sich auf dem Markt. Dienstleister wie RightNow („Verkaufe dein Problem“) werben gezielt um betroffene Kunden oder Mitarbeiter der gehackten Unternehmen. Sie nutzen dabei die Möglichkeit, aus Datenlecks und ähnlichen Vorfällen Profit zu schlagen. Prozessfinanzierer übernehmen dabei die Kosten für den Kläger und erhalten im Erfolgsfall eine Provision. Aktuell werden insbesondere Kunden von Facebook und Deezer angesprochen.

Ziel dieser Geschäftsmodelle ist dabei nicht, jeden Fall vor Gericht zu bringen, sondern das betroffene Unternehmen zu außergerichtlichen Vergleichen zu bewegen. Ein Paradebeispiel für diese Strategie ist die Vereinbarung mit Mastercard von Januar 2023, bei der Kunden aufgrund einer illegalen Veröffentlichung von Kundendaten im Zusammenhang mit dem „Mastercard Priceless Specials“-Datenleck jeweils 300 Euro erhielten. Ein Prozessfinanzierer vertrat 2000 von insgesamt 90 000 betroffenen Kunden und erhielt dem Vernehmen nach eine Provision von 25 Prozent.

Die Kommerzialisierung datenschutzrechtlicher Schadensersatzansprüche ist bereits in vollem Gange und wird in nächster Zeit noch an Fahrt aufnehmen. Gerade nach Cyberattacken stellen Schadensersatzforderungen ein Risiko für die betroffenen Unternehmen dar.

Der zukünftige Erfolg des Geschäftsmodells hängt entscheidend von der weiteren Auslegung des Art. 82 DSGVO durch den EuGH ab. Neben der oben erwähnten Entscheidung vom 4. 5. 2023 liegen dem EuGH zahlreiche weitere Verfahren mit Vorlagefragen aus Deutschland zur Entscheidung vor.

Ebenfalls wird sich zeigen, inwieweit insbesondere die deutschen Arbeitsgerichte ihre Rechtsprechung durch die Entscheidung des EuGH anpassen werden: So können sie entweder seine Forderung nach dem Nachweis eines konkreten Schadens zum Anlass nehmen, ihre eigene Rechtsprechung einzuschränken und uferlosen und oftmals unsubstantiierten Behauptungen von Klägern Grenzen zu setzen. Oder sie behalten im Ergebnis ihre verbraucherfreundliche Linie bei, in-

8 Vgl. BAG, Vorlagebeschl. v. 26. 8. 2021 – 8 AZR 253/20 (A), NZA 2021, 1713, Rn. 32 ff.; BAG, 5. 5. 2023 – 2 AZR 363/21, NZA 2022, 1191, Rn. 23 ff.; OLG Stuttgart, 31. 3. 2021 – 9 U 34/21, K&R 2021, 748 ff. = BeckRS 2021, 6282, Rn. 23, 40; OLG Bremen, 16. 7. 2021 – 1 W 18/21, ZD 2021, 652.

9 Vgl. EuGH, 4. 5. 2023 – C-300/21, K&R 2023, 416 ff. = NJW 2023, 1930, Rn. 33 ff.

10 Vgl. EuGH, 4. 5. 2023 – C-300/21, K&R 2023, 416 ff. = NJW 2023, 1930, Rn. 33 ff.

11 *Thomas Bindl*, Geschäftsführer der EuGD zum EuGH-Urt. v. 4. 5. 2023: „Wir leben eine Zeitenwende. Verletzte, die bisher meinten, sie könnten sich zurücklehnen und Betroffenen den Nachweis eines besonders hohen Schadens abverlangen, um einen zuvor bei vielen Betroffenen eingetretenen Schaden (‚Streuschaden‘) punktuell abzugelten, muss nicht zukünftig eine veränderte Raumtemperatur einstellen, denn jeder Schaden ist ersatzfähig. […]“.

dem sie sehr knappe Begründungen zu einer immateriellen Betroffenheit als Schadensnachweis genügen lassen.

In Bezug auf Cyberangriffe ist auch das vor dem EuGH anhängige Verfahren C-340/21 relevant. Dort geht es um die Frage, ob und inwieweit ein Unternehmen für erfolgreiche Cyberangriffe gem. Art. 82 Abs. 1 DSGVO haftet. Nach Ansicht des Generalanwalts ist eine Exkulpation alleine aufgrund des Vorliegens eines Cyberangriffes – und damit eines von außen auftretenden Ereignisses – nicht möglich, da der datenschutzrechtliche Vorwurf sich nicht auf den Cyberangriff als solchen bezieht, sondern vielmehr auf die fehlende Verhinderung.[12] Gleichzeitig führt aber auch nicht jeder Verstoß gegen den Stand der Technik im Sinne des Art. 32 DSGVO zu einer Schadenshaftung. Dieser erwähnt zahlreiche andere im Rahmen der IT-Sicherheit zu berücksichtigende Aspekte, aus Unternehmenssicht insbesondere auch die der Implementierungskosten.[13]

V. Verteidigungsstrategien

Als problematisch bei der Verteidigung gegen Massenverfahren können sich folgende Aspekte erweisen: Vergleiche mit einzelnen Antragstellern können einen Fall schnell erledigen, bergen aber das Risiko, öffentlich zu werden und andere Kläger anzulocken. Eine Vertraulichkeitsvereinbarung wirkt dem nur bedingt entgegen, da die Informationen auch anderweitig „durchgestochen" werden können. Gerichtsverfahren wiederum bringen eine öffentliche Verhandlung und mögliche Presseberichterstattung mit sich. Zudem kommt einem Urteil, das einen Schadensersatzanspruch zuspricht, eine größere Autorität als ein Vergleich zu, und von einem Urteil kann eine gewisse Signalwirkung ausgehen.

Rechtlich bietet die DSGVO in der aktuellen Auslegung durch die Rechtsprechung gute Verteidigungsmöglichkeiten: So begründet, wie oben dargestellt, nicht jeder Verstoß gegen die DSGVO automatisch einen Schadensersatzanspruch. Weiterhin wird im Rahmen von Massenverfahren häufig nicht zu individuellen Schäden vorgetragen, sondern lediglich Textbausteine aneinandergereiht, die nicht hinreichend konkret für den jeweiligen Sachverhalt sind. Darüber hinaus stellt auch ein erfolgreicher Hackerangriff nicht zwingend einen Beweis für einen Verstoß gegen Art. 32 DSGVO dar. Im Übrigen besteht für Unternehmen daneben auch immer die Möglichkeit, sich gemäß Art. 82 Abs. 3 DSGVO zu exkulpieren.

Aufgrund der in Massenverfahren sehr ähnlichen Sachverhalte und der überschaubaren Anzahl von rechtlichen Aspekten lässt sich auch die Verteidigung gegen Schadensersatzklagen automatisieren und (kosten-)effizient durchführen.

Hauke Hansen

Fachanwalt für IT-Recht, zert. Datenschutzbeauftragter (TÜV®) und Partner der Kanzlei FPS in Frankfurt/M. Herr Hansen ist Experte für Cybersicherheit, er entwirft Cyber-Security-Strategien, um Unternehmen und Unternehmer zu schützen und unterstützt sie bei der Abwehr von Schadensersatzansprüchen und behördlichen Bußgeldern.

David Schwarze

Jahrgang 1994; Studium der Wirtschaftswissenschaften an der Karlshochschule International University in Karlsruhe; Studium der Rechtswissenschaften an der Philipps-Universität Marburg; seit 2023 Volljurist; Schwerpunktbereiche: IT- und Datenschutzrecht.

12 Schlussanträge des Generalanwaltes beim EuGH, 27. 4. 2023 – C-340/21, GRUR-RS 2023, 8707, Rn. 58 - 69 – NAP.

13 Schlussanträge des Generalanwaltes beim EuGH, 27. 4. 2023 – C-340/21, GRUR-RS 2023, 8707, Rn. 32, 36 – NAP.

Dr. iur. Hendrik Wieduwilt*

Private Diskurswächter unter staatlichem Druck

Kurz und Knapp

Das Internet hat eine neue Ordnung bekommen. Besonders der „Desinformation", was immer das genau ist, will die EU-Kommission mit dieser Ordnung den Kampf ansagen. Das „Digitale Dienste Gesetz" greift seit dem 25. 8. unter anderem für eine Reihe von Plattformgiganten, darunter Google, Facebook und Twitter, aber auch Zalando, das sich jetzt gerade juristisch gegen die Gleichsetzung mit den Amerikanern wehrt. Das Netz soll sicherer, wahrhaftiger, kontrollierter werden.

Es ist ein gewaltiges Gesetz. Allein 156 Erwägungsgründe müssen durchkämmt werden, bevor der eigentliche Regelungstext beginnt, 102 Seiten hat das gesamte Werk – es ist in Struktur und Komplexität der Datenschutzgrundverordnung (DSGVO) ähnlich, mit dem Unterschied, dass dieses Gesetz nicht Datenflüsse und die Zulässigkeit beim Beschriften von Klingelschildern reguliert, sondern die Kommunikation von Milliarden Menschen im Internet. Es macht den Plattformen Vorgaben auch dazu, wie sie mit Inhalten umgehen sollen. Wie genau das gehen soll, ergänzen zahllose abgeleitete Rechtsakte: Empfehlungen, Standards, Methoden, die Stiftung Neue Verantwortung hat diese Texte gesammelt und in einer Excel-Tabelle mit derzeit 83 Einträgen gelistet.

Das Vorhaben ist bislang auch wegen seiner grotesken Komplexität in Deutschland kaum diskutiert worden. Eine Weile zankten Verlage und Journalistenorganisationen wegen möglicher Unterdrückung von Presseerzeugnissen. Doch diese Kritik greift zu kurz: Denn es ist praktisch jede digitale Kommunikation betroffen, ganze virtuelle Denkräume. Das Gesetz

* Mehr über den Autor erfahren Sie am Ende des Beitrags.