Kommunikation & Recht

K&R
1 | Januar 2025
28. Jahrgang
Seiten 1 - 72

dfv Mediengruppe
Frankfurt am Main

Medienpranger – Medienverbot – Mediensatire: 14. Presserechtsforum
Prof. Dr. Roger Mann

1 Die Entwicklung des Presserechts 2024
Dr. Diana Ettig

8 Herausforderungen für den Grundrechtsschutz der Presse in der digitalen Welt
Prof. Dr. Christoph Fiedler

11 Tauziehen um die Reputation
Christian Schwarz

15 Die vertragstypologische Einordnung von KI-Verträgen
Jannik Scherer

22 Anwendbarkeit der Text- und Data-Mining-Schranke bei KI-Trainingsdaten
Dr. Hendrik Schöttle und Beata Völker

26 Kontrollverlust über Facebook-Daten – Ein Weckruf für datenverarbeitende Unternehmen
Dr. Jakob Horn und Alexander Schmalenberger

35 **BGH:** Immaterieller Schadensersatz nach Datenschutzverletzung

41 **BGH:** Verstoß gegen Grundsatz der Staatsferne der Presse durch kostenlose Online-Jobbörse

47 **OLG Zweibrücken:** Politikerbeleidigung nicht von Reichweite abhängig
mit Kommentar von **Dominik Höch**

49 **OLG Köln:** Kritische Bewertung der Russlandhaltung einer Politikerin zulässig
mit Kommentar von **Christine Libor**

52 **OLG Köln:** Rechtswidriges Anteasern vor der Bezahlschranke
mit Kommentar von **Dr. Jasper Prigge**

65 **OVG NRW:** Nutzersperrung auf Facebook-Seite eines öffentlich-rechtlichen Mediums rechtswidrig
mit Kommentar von **Dr. Fiete Kalscheuer**

Beilage
Jahresregister 2024

RA Dr. Jakob Horn, LL.M. (Harvard) und RA Alexander Schmalenberger, LL.B.*

Kontrollverlust über Facebook-Daten – Ein Weckruf für datenverarbeitende Unternehmen

Zugleich Kommentar zu BGH, Urteil vom 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff. (in diesem Heft)

Kurz und Knapp

Mit Urteil vom 18. 11. 2024 hat der BGH im Facebook-Scraping-Fall den Kontrollverlust über personenbezogene Daten als DSGVO-Schaden anerkannt – ohne Missbrauchsnachweis. Dies erleichtert Klagen und erhöht den wirtschaftlichen Druck auf Unternehmen, insbesondere durch drohende Klagewellen. Trotz moderater Schadenshöhen könnten massenhafte Klagen Summen erreichen, die existenzbedrohend sind. Ihre Vermeidung erfordert striktere technische und organisatorische Schutzmaßnahmen.

I. Einleitung

Mit Urteil vom 18. 11. 2024[1] hat der BGH eine grundlegende Auslegung von Art. 82 Abs. 1 DSGVO vorgenommen. Der Entscheidung lag der sogenannte Facebook-Scraping-Fall zugrunde. Unbekannte luden hier von der Plattform Facebook weltweit 533 Millionen Datensätze mit personenbezogenen Daten von Facebook-Nutzern herunter, darunter rund sechs Millionen Menschen in Deutschland.

Die BGH-Entscheidung dürfte weitreichende Auswirkungen auf Schadensersatzklagen nach Art. 82 DSGVO haben. Zwar hat der EuGH die Voraussetzungen für Schadensersatz nach Art. 82 Abs. 1 DSGVO bereits in mehreren Entscheidungen konkretisiert. Insbesondere beim Kontrollverlust als Schaden waren aber noch Fragen offen. Zudem verweist der EuGH für die konkrete Bemessung des Schadens stets an die Gerichte der Mitgliedsstaaten.[2]

Genau zu diesen zwei – neben weiteren – Punkten verhält sich die Entscheidung nun:

Zum einen stellt der BGH klar, dass bereits der Verlust der Möglichkeit, die Verarbeitung personenbezogener Daten zu kontrollieren und zu steuern (Kontrollverlust)[3] für sich genommen ein Schaden sein kann. Für den Kontrollverlust sind nach dem BGH weder der Nachweis eines Missbrauchs der Daten noch anderer konkreter Folgen erforderlich.[4] Diese Entscheidung erleichtert es Betroffenen, Ansprüche geltend zu machen, weil der Nachweis des Kontrollverlusts erleichtert wird.

Zum anderen hält der BGH eine Größenordnung von 100 EUR als Schadensersatz im vorliegenden Fall für vertretbar, währenddessen eine einstellige Summe nicht angemessen sei.[5] Die konkrete Summe muss jedoch vom Tatrichter nach § 287 ZPO geschätzt werden.

Für Unternehmen hat die BGH-Entscheidung weitreichende Konsequenzen, wenn es zu einem Datenschutzverstoß mit massenhaftem Abfluss von Daten kommt. In diesen Fällen werden häufig massenhafte Schadensersatzforderungen geltend gemacht. Die Entscheidung gibt den Klägern nun Auftrieb, weil der Nachweis, dass überhaupt ein Schaden vorliegt, erheblich erleichtert wird. Bei solchen massenhaften Schäden dürfen sich Unternehmen auch nicht von der geringen Höhe von 100 Euro täuschen lassen. Denn würden beispielsweise sämtliche der 6 Millionen deutschen Betroffenen Facebook-Nutzer einen Schadensersatz geltend machen, wären allein als Schadenssumme 600 Millionen Euro zu zahlen. Hinzu kommen noch z. B. zu ersetzende Rechtsverfolgungs- und etwaige Rechtsverteidigungskosten. Dieses Beispiel verdeutlicht, dass selbst geringe Schadensbeträge in der Masse erhebliche wirtschaftliche Risiken bergen.

II. Die Entscheidung und ihre Tragweite

1. Kontrollverlust als Schaden

Der EuGH hatte bereits mehrfach entschieden, dass der Kontrollverlust Schaden sein kann.[6] Deutsche Instanzgerichte hatten dies allerdings bisher häufig so ausgelegt, dass nicht der Kontrollverlust selbst Schaden ist, sondern nur etwaige negative Folgen aus dem Kontrollverlust.[7] Hier hat der BGH nun klargestellt, dass der Kontrollverlust über personenbezogene Daten – definiert als der Verlust der Möglichkeit, über die Verarbeitung dieser Daten zu entscheiden – selbst dann einen immateriellen Schaden darstellen kann, wenn keine weiteren negativen Folgen wie Missbrauch oder psychische Belastungen nachweisbar sind.[8] Entscheidend ist, dass der Betroffene konkret darlegt, dass er vor dem Verstoß tatsächlich Kontrolle über die fraglichen Daten hatte und diese durch den Vorfall beeinträchtigt wurde.[9] Dabei ist zu beachten, dass bloße Behauptungen oder pauschale Textbausteine, wie sie etwa in Massenverfahren häufig vorkommen, für die Darlegung des Kontrollverlusts nicht ausreichen.[10] Die Anforderungen an eine Individualisierung sind jedoch nicht besonders groß.[11] Gerade in Fällen, in denen viele Personen mit vergleichbaren Daten betroffen wurden, tragen auch die Folgen vergleichbare Züge.[12] Auch eine umfassende Darlegung, wie der Betroffene bislang verfahren ist, um die Kontrolle über die Daten zu erhalten, ist nicht gefordert.[13] Der Kläger hatte im vorliegenden Fall lediglich geschildert, dass er seine Telefonnummer

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 10. 12. 2024.

1 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff.

2 EuGH, 11. 4. 2024 – C-741/21, K&R 2024, 342 ff. = juris, Rn. 58; EuGH, 25. 1. 2024 – C-687/21, K&R 2024, 192 ff., Rn. 53 – MediaMarktSaturn; EuGH, 21. 12. 2023 – C-667/21, K&R 2024, 114 ff. = EuZW 2024, 270, Rn. 83 und 101 – Krankenversicherung Nordrhein; jeweils m. w. N.

3 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 30, 31.

4 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 30, 31.

5 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 99 f.

6 EuGH, 11. 4. 2024 – C-741/21, K&R 2024, 342 ff. = juris, Rn. 28 m. w. N.

7 Z. B. OLG Oldenburg, 20. 2. 2024 – 13 U 43/23; OLG Köln, 7. 12. 2023 – 15 U 33/23, OLG Stuttgart, 22. 11. 2023 – 4 U 20/23.

8 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 30.

9 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 39 ff.

10 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 36.

11 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., vgl. Rn. 39 f.

12 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 36.

13 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 41.

gezielt und nicht wahllos weitergebe. Der BGH stellte klar, dass solche Darlegungen genügen und keine weiteren Details erforderlich sind, um einen Kontrollverlust zu begründen.[14] Für datenverarbeitende Unternehmen bedeutet dies eine erhöhte Verantwortung, da auch subjektive Unsicherheiten von Betroffenen eine Rolle spielen können. Welche Anforderungen an die Darlegung solcher Unsicherheiten konkret gestellt werden, bleibt offen und könnte zukünftige Verfahren prägen.

Eine weitere Frage wird sein, ob ein Kontrollverlust vorgelegen hat. Welche Nachweise für den Kontrollverlust – etwa Server-Logs oder Zugriffsdaten – letztlich als ausreichend angesehen werden, bleibt offen.

Mit Blick auf die EuGH-Rechtsprechung[15] ist zwar zu fordern, dass mehr als die bloße theoretische/hypothetische Möglichkeit eines Kontrollverlustes verlangt werden muss – ein Dritter muss die Daten zur Kenntnis genommen haben. [16] Der Anspruchsteller muss also Tatsachen vortragen, die die Weitergabe von Daten belegen.[17] Dieser Grundsatz könnte auch auf die Darlegung des Kontrollverlusts Anwendung finden, da die Anforderungen an die Substantiierung und Nachweisführung bei immateriellen Schäden von zentraler Bedeutung sind.

Ein Kontrollverlust liegt also nur dann vor, wenn bewiesen werden kann, dass ein Dritter die Daten tatsächlich zur Kenntnis genommen hat, etwa durch Zugriffsdaten, Protokolle über unautorisierte Aktivitäten oder Sicherheitsberichte, die eine Schwachstelle dokumentieren. Dazu zählen etwa Server-Logs, die unautorisierte Zugriffe dokumentieren, Protokolldaten, die ungewöhnliche Aktivitäten wie unautorisierte IP-Adressen aufführen, oder Sicherheitswarnungen, die auf Schwachstellen oder Sicherheitsverletzungen hinweisen. Diese Daten liegen dem Betroffenen jedoch in der Regel nicht vor.

Daher ist anzunehmen, dass sich künftige Klagen verstärkt der – in ihrer Anwendung nicht vollständig vorhersagbaren – Institute der Aufklärungslast der nicht beweisbelasteten Partei sowie der sekundären Behauptungslast bedienen werden. Die Aufklärungslast nach den Vorschriften der §§ 142, 144 ZPO ermöglicht es dem Gericht, auch Dritte zur Vorlage von Dokumenten oder zur Mitwirkung bei der Beweiserhebung zu verpflichten, wenn diese Unterlagen zur Klärung des Sachverhalts notwendig sind. Dies gilt unabhängig davon, ob ein materiellrechtlicher Herausgabeanspruch besteht. Die nicht beweisbelastete Partei kann daher angehalten werden, relevante technische Daten – etwa Logs oder Sicherheitsberichte – bereitzustellen, sofern diese in ihrem Einflussbereich liegen.[18]

Die sekundäre Behauptungslast greift ein, wenn zwischen den Parteien ein Informationsgefälle besteht, beispielsweise weil die beweisbelastete Partei keine Kenntnis über Vorgänge hat, die ausschließlich im Verantwortungsbereich der Gegenseite liegen. In solchen Fällen muss die nicht beweisbelastete Partei darlegen, welche technischen Schutzmaßnahmen ergriffen wurden oder ob ein Zugriff auf die Daten erfolgt sein könnte.[19] Kommt sie dieser Verpflichtung nicht nach, wird das Vorbringen der beweisbelasteten Partei gemäß § 138 Abs. 3 ZPO als wahr fingiert.

2. Befürchtung eines Datenmissbrauchs als Schaden

Daneben bestätigte der BGH auch die bisherige EuGH-Rechtsprechung, wonach auch die Befürchtung, dass Dritte die Daten missbrauchen könnten, einen Schadensersatzanspruch begründen kann.[20] Dadurch sinken die Hürden für die Geltendmachung solcher Ansprüche, da Betroffene keine konkreten negativen Folgen wie Missbrauch nachweisen müssen.[21] Allerdings genügt hier nicht die bloße Behauptung einer Befürchtung. Der Nachweis solcher „inneren Tatsachen“ wie der Befürchtung kann jedoch durch Indizien erbracht werden, wie der BGH hier im vorliegenden Fall festgestellt hat. Die Rechtsprechung betont dabei, dass solche inneren Tatsachen einem unmittelbaren Beweis oftmals nicht zugänglich sind und stattdessen auf Indizien gestützt werden müssen.[22] Diese Indizien können beispielsweise Handlungen, Äußerungen oder bestimmte Verhaltensweisen sein, die nach der allgemeinen Lebenserfahrung auf das Vorliegen einer bestimmten Befürchtung schließen lassen. Im vorliegenden Fall führte der Kläger als Indizien für seine Befürchtungen unter anderem Kontaktversuche und Phishing-Attacken an.[23]

Dies hat der BGH ausreichen lassen: Das BVerfG[24] hat klargestellt, dass der Beweis innerer Tatsachen durch Umstände möglich ist, die nach allgemeiner Lebenserfahrung auf das Vorhandensein der behaupteten Tatsache hindeuten. Daraus folgt, dass insbesondere angesichts der derzeit virulenten, auch durch generative KI unterstützten Zunahme von Angriffen geleakte Daten mit hoher Wahrscheinlichkeit irgendwann zu einem Angriff verwendet werden. Was es Unternehmen schwerer macht, die behaupteten Befürchtungen effektiv zu widerlegen. Diese Dynamik erhöht die Bedeutung des Indizienbeweises im Bereich der Datenschutzrechtsprechung erheblich.

3. Beweislastverteilung und Darlegungspflichten

Die Beweislast für die Voraussetzungen des Schadensersatzanspruchs liegt grundsätzlich bei den Klägern. Sie müssen den Verstoß, den Schaden und den Kausalzusammenhang darlegen.[25] Allerdings greift bei Art. 82 Abs. 3 DSGVO eine Verschuldensvermutung, sodass Unternehmen sich entlasten müssen, indem sie nachweisen, dass sie angemessene technische und organisatorische Maßnahmen (TOMs) implementiert hatten.[26]

Wichtig ist allerdings, dass der Nachweis eines DSGVO-Verstoßes für einen Schadensersatzanspruch allein nicht ausreicht.[27] Kläger müssen zudem nachvollziehbar schildern, wie sich der Kontrollverlust auf sie ausgewirkt hat, um den Schaden zu beziffern. Dies kann subjektive Empfindungen wie Angst oder Unsicherheit umfassen, wenn diese objektiv nachvollziehbar gemacht werden.[28]

Für Unternehmen bedeutet dies, dass TOMs nicht nur implementiert, sondern auch gerichtsfest dokumentiert werden müssen. Beispiele hierfür sind Sicherheitszertifikate, Audit-Protokolle oder Nachweise zur Verschlüsselung sensibler Daten. Diese Dokumentation wird künftig ein zentrales Verteidigungsinstrument sein, um Haftungsrisiken zu minimieren.

4. Individuelle Klagen oder Verfahren nach dem VduG?

Das Urteil wirft die Frage auf, ob Betroffene künftig vermehrt individuelle Klagen anstrengen oder ob sich Klagen nach dem

14 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 39, 41.
15 EuGH, 5. 3. 2024 C-755/21 P, K&R 2024, 339 ff., Rn. 138.
16 EuGH, 25. 1. 2024 – C-687/21, K&R 2024, 192 ff., Rn. 68 – MediaMarkt-Saturn.
17 Vgl. EuGH, 5. 3. 2024 C-755/21 P, K&R 2024, 339 ff., Rn. 138.
18 Für Details *Baumgärtel/Laumen/Prütting*, Handbuch der Beweislast, 5. Aufl. 2023, Kap. 21, Rn. 19 m. w. N.
19 *Baumgärtel/Laumen/Prütting*, (Fn. 19), Kap. 22, Rn. 2 m. w. N.
20 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 32.
21 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., vgl. Rn. 40.
22 Vgl. BGH, 5. 11. 2003 – VIII ZR 218/01, NJW-RR 2004, 247, 248; BVerfG, 30. 6. 1993 – 2 BvR 459/93, NJW 1993, 2165; OLG Karlsruhe, 5. 2. 2013 – 12 U 140/12, NJW-RR 2013, 869.
23 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 40.
24 BVerfG, 30. 6. 1993 – 2 BvR 459/93, NJW 1993, 2165.
25 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 23.
26 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., vgl. Rn. 21.
27 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 28.
28 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 41.

Verbraucherrechtedurchsetzungsgesetz (VduG) durchsetzen könnten – die erste derartige Klage zum gerade entschiedenen Facebook-Fall wurde gerade angekündigt.[29] Das VduG ermöglicht die Bündelung gleichartiger Verbraucheransprüche in Abhilfeklagen (§ 15 VduG). Voraussetzung dafür ist jedoch, dass die Ansprüche „im Wesentlichen gleichartig" sind, das heißt, dass sie auf „demselben Sachverhalt" oder „einer Reihe im Wesentlichen vergleichbarer Sachverhalte" beruhen (§ 15 Abs. 1 Nr. 1 VduG). In Massenverfahren wie dem Facebook-Scraping-Fall weist der BGH ausdrücklich darauf hin, dass standardisierte Textbausteine nicht ausreichen.[30] Trotz der Vielzahl der Betroffenen muss jede einzelne Klage darlegen, wie sich der konkrete Datenschutzverstoß individuell ausgewirkt hat. Allerdings sind an die Ausführungen keine allzu hohen Anforderungen zu stellen – da die Folgen eines millionenfachen Datenverlustes notwendig in vielen Fällen vergleichbare Züge trügen.

Das Urteil des BGH erschwert damit die Anwendbarkeit des VduG in Datenschutzfällen jedenfalls nicht. Im Gegenteil könnte man die Ausführungen so verstehen, dass die notwendigen Anforderungen an die „Gleichartigkeit" nach § 15 Abs. 1 VduG möglicherweise erfüllt werden können. Damit könnte der Schadensverlauf – abweichend von einem Teil der bisher zum Scraping ergangenen Entscheidungen[31] – hinreichend gleichartig sein, um Abhilfeklagen zu erlauben.

Gleichzeitig könnten individuelle Klagen aufgrund des vereinfachten Nachweises eines Schadens attraktiver werden. Die Festlegung eines pauschalen Schadensersatzbetrags von ca. 100 Euro schon für den Verlust von relativ wenig sensiblen Daten wie Telefonnummern senkt die Hürde für Betroffene, Klagen einzureichen, und erhöht das Risiko massenhafter Individualverfahren.

5. Schadensbemessung

Schwierig ist die Bemessung des Schadens bei einem Kontrollverlust. Hier ist eine differenzierte Betrachtung der jeweiligen Umstände des Einzelfalls erforderlich. Der BGH hat in seinem Urteil klargestellt, dass die Höhe des Schadensersatzes wesentlich von sieben Faktoren abhängt: der Sensibilität der betroffenen Daten, deren typischerweise zweckgemäßer Verwendung, der Art des Kontrollverlusts (begrenzter/unbegrenzter Empfängerkreis), der Dauer des Kontrollverlusts, der Möglichkeit der Wiedererlangung der Kontrolle (z. B. durch Entfernung einer Veröffentlichung aus dem Internet), und dem dafür notwendigen Aufwand.[32]

Für den hier entschiedenen Fall der unbefugten Offenlegung einer Telefonnummer an einen unbegrenzten Empfängerkreis äußerte der BGH nun, dass er keine Bedenken gegen einen Schadensersatz in Höhe von 100 Euro hätte.[33] Gleichzeitig meldete der BGH Zweifel an, ob eine einstellige Schadensersatzsumme gerechtfertigt wäre, die das Berufungsgericht in den Raum gestellt hatte.

Insgesamt ordnet sich dieser vergleichsweise geringe Betrag in die Linie des EuGH ein, der ebenfalls eher niedrige Beträge bei Datenschutzverstößen ansetzt. Für die Veröffentlichung intimer Chatnachrichten, was erhebliche Auswirkungen für den Betroffenen hatte, sprach der EuGH 2000 Euro Schadensersatz zu.[34] Insgesamt verdeutlichen die Urteile von EuGH und BGH daher, dass die Schadenshöhe proportional zur Schutzwürdigkeit der Daten und den Auswirkungen des Kontrollverlusts steigen kann, insgesamt aber eher niedrig anzusetzen ist.

Ein systematischer Ansatz zur Schadensbemessung könnte sich an einer Kombination dieser beiden Faktoren orientieren. So lässt sich die Schutzwürdigkeit der Daten durch eine Punkteskala (1 - 5) bewerten, wobei weniger sensible Daten wie Telefonnummern niedrig eingestuft werden und hochsensible Daten wie Gesundheitsinformationen oder sexuelle Orientierung den höchsten Schutzbedarf aufweisen. Ebenso kann die Schwere des Kontrollverlusts – von einem begrenzten Empfängerkreis bis hin zu einer irreversiblen Veröffentlichung – nach einer ähnlichen Skala bewertet werden. Die Multiplikation dieser beiden Werte mit einem geeigneten Multiplikator, der an die Umstände des Einzelfalls angepasst werden kann, ermöglicht eine nachvollziehbare Schadensberechnung.

Insgesamt bleibt Gerichten aber weiterhin großer Spielraum bei der Bemessung des Schadens. Während der BGH im Facebook-Scraping-Fall die Veröffentlichung wenig sensiblen Daten mit 100 Euro bewertete, könnten andere Gerichte in begründeten Fällen von diesen Werten abweichen. Hierbei ist sowohl Spielraum nach unten – der BGH meldete nur Zweifel an einstelligen, nicht aber zweistelligen Beträgen an[35] – als auch nach oben.

III. Herausforderungen für Unternehmen

Das Urteil birgt für Unternehmen erhebliche wirtschaftliche Risiken, denn auch bei vergleichsweise geringen Schadensersatzbeträgen kann die Gesamtsumme schnell sehr hohe Beträge erreichen, wenn zahlreiche Kläger erfolgreich Schadensersatz geltend machen.

Hierbei ist zweierlei zu berücksichtigen: Zum einen setzte der BGH die Anforderungen an die Begründung des Schadensersatzes erheblich herab. Sobald Daten tatsächlich abgeflossen sind, liegt ein grundsätzlich ersatzfähiger Kontrollverlust vor.

Zum anderen dürften die vom BGH in den Raum gestellten 100 Euro zwar einen Anhaltspunkt für die Schadensbemessung bieten. Sie sind allerdings wohl eher als Untergrenze anzusehen. Insbesondere wenn Daten betroffen sind, die ihrem Zweck oder ihrer Art nach sensibel sind – etwa Finanzdaten oder mit Daten im Sinn von Art. 9 DSGVO – wird mit höheren Schadenssummen zu rechnen sein.

Unternehmen in allen Branchen sind daher gut beraten, regelmäßig ihre Datenschutz-Compliance zu überprüfen. Das gilt insbesondere für die technischen und organisatorischen Maßnahmen (TOMs) sowie deren gerichtsfeste Dokumentation. Außerdem sollte geprüft werden, ob insbesondere der Kontrollverlust durch geeignete Maßnahmen gering gehalten werden kann, etwa indem die weitere Verwendung der Daten unmöglich gemacht wird. Zum Beispiel könnte man die Änderung von Passwörtern erzwingen, Nutzer-IDs sperren oder durch Kooperationen mit Mobilfunkanbietern den Wechsel von Telefonnummern erleichtern.

Idealerweise verhindern gute TOMs Datenschutzvorfälle. Kommt es dennoch zu einem Vorfall – was nie auszuschließen ist – so bieten gute TOMs eine Verteidigungslinie, um Ansprüche abzuwehren. Nach der EuGH-Rechtsprechung begründet der Datenschutzvorfall nämlich noch keinen Datenschutzverstoß, sondern es muss stets geprüft werden, ob angemessene TOMs ergriffen wurden.[36]

29 https://www.vzbv.de/pressemitteilungen/nach-bgh-urteil-zu-facebook-datenleck-vzbv-reicht-sammelklage-ein.
30 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 36 ff.
31 Vgl. die Darstellung bei *Thönissen*, ZD 2024, 253, 256 f.
32 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 99.
33 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 100.
34 EuGH, 5. 3. 2024 – C-755/21 P, K&R 2024, 339 ff., Rn. 138.
35 BGH, 18. 11. 2024 – VI ZR 10/24, K&R 2025, 35 ff., Rn. 100.
36 EuGH, 25. 1. 2024 – C-687/21, K&R 2024, 192 ff., Rn. 39.

IV. Fazit

Der BGH hat mit seinem Urteil die Voraussetzungen für einen Schadensersatzanspruch bei Datenschutzverstößen deutlich abgesenkt. Der Kontrollverlust über personenbezogene Daten wird nun als eigenständiger Schaden anerkannt. Das erleichtert es Klägern, Schadensersatz geltend zu machen, sodass bei Datenschutzvorfällen das Klagerisiko steigt. Das Klagerisiko wird gerade bei Massenfällen noch dadurch gestärkt, dass der BGH die Anforderungen an die Darlegung im Einzelfall herabgesetzt wird. Dadurch ist es einerseits leichter, in Klageschriften mit Standardtexten zu arbeiten. Gleichzeitig ist denkbar, dass bei Datenschutzverstößen künftig auch Klagen nach dem Verbraucherrechtedurchsetzungsgesetzes (VDuG) erhoben werden.

Die eher geringe Schadenshöhe, die der BGH im konkreten Fall für angemessen hielt, sollte Unternehmen dagegen nicht in Sicherheit wiegen, weil sich die Summen bei Massenklagen schnell aufsummieren können.

Unternehmen sind daher gut beraten, durch gute TOMs möglichst Schadensvermeidung anzustreben und dadurch gleichzeitig eine rechtliche Verteidigungslinie abseits der Darlegung des Schadens aufzubauen.

Dr. Jakob Horn

LL.M. (Harvard), Jahrgang 1988; Studium der Rechtswissenschaft an der Friedrich-Schiller-Universität Jena, Promotion 2018; 2018/19 LL.M. Harvard Law School; seit 2024 Associate bei Taylor Wessing; Schwerpunkte: Datenschutz, IT-Vertragsrecht, KI und darauf bezogene Prozessführung; umfangreiche Erfahrung in technologierechtlichen Fragestellungen.

Alexander Schmalenberger

Jahrgang 1982; Studium der Rechtswissenschaften an der Bucerius Law School (LL.B., Erstes Staatsexamen 2007) und der Victoria University, Wellington; seit 2021 Knowledge Lawyer bei Taylor Wessing; Schwerpunkte: digitales, Datenschutz-, Technologie- und Telekommunikationsrecht.

Rechtsprechung

Schadensersatz wegen veröffentlichter Daten im Online-Handelsregister

EuGH, Urteil vom 4. 10. 2024 – C-200/23

Volltext-ID: KuRL2025-29, www.kommunikationundrecht.de

Agentsia po vpisvaniyata ./. OL

ECLI:EU:C:2024:827

Verfahrensgang: Varhoven administrativen sad (Oberstes VG, Bulgarien), 21. 3. 2023

Art. 21 Abs. 2 RL (EU) 2017/1132; Art. 4 Abs. 1, Art. 16, Art. 17, Art. 58 Abs. 3, Art. 82 Abs. 1, 2, 3 VO (EU) 2016/679

1. Art. 21 Abs. 2 der RL (EU) 2017/1132 […] ist dahin auszulegen, dass er einem Mitgliedstaat keine Verpflichtung auferlegt, die Offenlegung eines Gesellschaftsvertrags im Handelsregister zuzulassen, der der Offenlegungspflicht nach dieser Richtlinie unterliegt und der über die erforderlichen personenbezogenen Mindestdaten hinaus weitere personenbezogene Daten enthält, deren Offenlegung nach dem Recht dieses Mitgliedstaats nicht vorgeschrieben ist.

2. Die VO (EU) 2016/679 […], insbesondere deren Art. 4 Nrn. 7 und 9, ist dahin auszulegen, dass die für die Führung des Handelsregisters eines Mitgliedstaats zuständige Stelle, die in diesem Register die personenbezogenen Daten veröffentlicht, die in einem Gesellschaftsvertrag enthalten sind, der der Offenlegungspflicht nach der RL 2017/1132 unterliegt und der ihr im Rahmen eines Antrags auf Eintragung der betreffenden Gesellschaft in das Register übermittelt wurde, sowohl „Empfänger" dieser Daten als auch – insbesondere indem sie diese der Öffentlichkeit zugänglich macht – für die Verarbeitung dieser Daten „Verantwortlicher" im Sinne dieser Bestimmung ist, selbst wenn dieser Vertrag personenbezogene Daten enthält, die nach dieser Richtlinie oder dem Recht dieses Mitgliedstaats nicht vorgeschrieben sind.

3. Die RL 2017/1132, insbesondere deren Art. 16, sowie Art. 17 der VO 2016/679 sind dahin auszulegen, dass sie einer Regelung oder Praxis eines Mitgliedstaats entgegenstehen, die dazu führt, dass die mit der Führung des Handelsregisters dieses Mitgliedstaats betraute Stelle jeden Antrag auf Löschung von nach dieser Richtlinie oder dem Recht dieses Mitgliedstaats nicht erforderlichen personenbezogenen Daten ablehnt, die in einem in diesem Register offengelegten Gesellschaftsvertrag enthalten sind, wenn dieser Stelle entgegen den in dieser Regelung vorgesehenen Verfahrensmodalitäten keine Kopie des Vertrags vorgelegt wurde, in der diese Daten unkenntlich gemacht wurden.

4. Art. 4 Abs. 1 der VO 2016/679 ist dahin auszulegen, dass die eigenhändige Unterschrift einer natürlichen Person unter den Begriff „personenbezogene Daten" im Sinne dieser Bestimmung fällt.

5. Art. 82 Abs. 1 der VO 2016/679 ist dahin auszulegen, dass ein zeitlich begrenzter Verlust der Kontrolle der betroffenen Person über ihre personenbezogenen Daten aufgrund der durch Online-Bereitstellung im Handelsregister eines Mitgliedstaats bewirkten öffentlichen Zugänglichmachung dieser Daten ausreichen kann, um einen „immateriellen Schaden" zu verursachen, sofern diese Person nachweist, dass sie tatsächlich einen solchen Schaden – so geringfügig er auch sein mag – erlitten hat, ohne dass dieser Begriff des immateriellen Schadens den Nachweis zusätzlicher spürbarer negativer Folgen erfordert.

6. Art. 82 Abs. 3 der VO 2016/679 ist dahin auszulegen, dass eine auf der Grundlage von Art. 58 Abs. 3 lit. b dieser Verordnung abgegebene Stellungnahme der Aufsichtsbehörde eines Mitgliedstaats nicht ausreicht, um die mit der Führung des Handelsregisters dieses Mitgliedstaats betraute Stelle, die „Verantwortlicher" im Sinne von Art. 4 Nr. 7 dieser Verordnung ist, von der Haftung nach Art. 82 Abs. 2 dieser Verordnung zu befreien. (Tenor des Gerichts)

Sachverhalt

Das Vorabentscheidungsersuchen betrifft die Auslegung der Art. 3 und 4 der RL 2009/101/EG des Europäischen Parla-