Dr. Daniel Ashkar, RA, Tobias Lantwin und Dr. Christian Schröder, RA

Datenschutzrecht – Was bringt das Jahr 2022?

Schwerpunkte der behördlichen Sanktionierung und der privaten Rechtsdurchsetzung

Verletzungen des Datenschutzrechts werden für Unternehmen deutlich teurer und Schadensersatzansprüche können auch Geschäftsführer treffen. Das Jahr 2021 stellte in mehrfacher Hinsicht ein Rekordjahr in Bezug auf von europäischen Datenschutzaufsichtsbehörden verhängte Bußgelder dar. Parallel beschäftigen datenschutzrechtliche Rechtsstreitigkeiten mehr und mehr die Gerichte in Deutschland und Europa. Ein besonderer Schwerpunkt lag insbesondere bei der gerichtlichen Geltendmachung immaterieller Schadensersatzansprüche. Der Beitrag beinhaltet einen Ausblick auf zukünftige Entwicklungen in diesen Bereichen und insbesondere auch darauf, in welchen Themengebieten im Jahr 2022 und womöglich darüber hinaus für Unternehmen die größten Risiken im Hinblick auf die Verhängung von Bußgeldern und die Verwicklung in Rechtsstreitigkeiten bestehen. Kurz eingegangen wird zudem auf ein Urteil des Oberlandesgerichts Dresden, bei dem ein Geschäftsführer persönlich auf Schadensersatz in Anspruch genommen wurde.

I. Rückblick zu Datenschutzbußgeldern in Deutschland und dem Europäischen Wirtschaftsraum

Während in den ersten Jahren nach Inkrafttreten der Datenschutz-Grundverordnung („DS-GVO“) nur zögerlich Bußgelder verhängt wurden, steigerten sich die Anzahl und die Höhe der Bußgelder in den letzten Jahren deutlich. Interessant ist dabei auch die Entwicklung weg von einer starken Fokussierung auf einzelne Spezialthemen wie Marketing. Zunehmend sind allgemeine Verstöße gegen das Transparenzgebot oder auch das Verbot von Datenverarbeitungen ohne Rechtsgrundlage Gegenstand von Bußgeldverfahren.

1. Bereiche, in denen wesentliche Datenschutzbußgelder verhängt wurden

Insbesondere in den nachfolgend genannten Bereichen wurden in der nahen Vergangenheit wesentliche Datenschutzbußgelder in Mitgliedstaaten des Europäischen Wirtschaftsraums („EWR“) verhängt.

a) Fehlende oder unzureichende Rechtsgrundlage

Ein wesentlicher Schwerpunkt der Bebußung von Datenschutzverstößen liegt bei Datenverarbeitungen ohne Rechtsgrundlage.

Beispielsweise hat die norwegische Datenschutzbehörde, Datatilsynet, Ende 2021 gegen die Dating-App Grindr ein Bußgeld in Höhe von umgerechnet etwas mehr als 6 Mio. Euro verhängt.[1] Datatilsynet hielt fest, dass Grindr in mehrfacher Hinsicht nicht die Anforderungen an eine wirksame Einholung einer Einwilligung der Betroffenen erfüllt und demnach personenbezogene Daten ohne gültige Rechtsgrundlage an seine Werbepartner übermittelt habe.[2]

b) Transparenzpflichten

Seit Inkrafttreten der DS-GVO gibt es eine breite Diskussion zur Detailtiefe von Datenschutzhinweisen und Datenschutzerklärungen.

Dass die Erwartungen der europäischen Datenschutzbehörden insoweit mittlerweile sehr hoch sind, hat das Bußgeldverfahren gegen WhatsApp gezeigt. Hier verhängte die irische Datenschutzbehörde, die Data Protection Commission (DPC), im Jahr 2021 – auf Druck von mehreren anderen europäischen Datenschutzbehörden – gegen WhatsApp ein Bußgeld in Höhe von 225 Mio. Euro wegen einer Reihe von festgestellten Verstößen gegen Transparenzpflichten.[3] Nachdem mehrere europäische Datenschutzbehörden mit der ursprünglichen Entscheidung der DPC nicht einverstanden waren, hat der Europäische Datenschutzausschuss („EDSA“) in diesem Fall einen verbindlichen Beschluss gefasst, in dem strenge Vorgaben mit Blick auf das Transparenzgebot gemacht und die DPC zur Neubemessung und Erhöhung des verhängten Bußgeldes angewiesen wurde.[4] Sowohl dieser Beschluss als auch die sehr umfassende Entscheidung der DPC machen deutlich, dass europäische Datenschutzbehörden inzwischen eine hohe Granularität bei Datenschutzhinweisen und Datenschutzerklärungen erwarten,[5] die bisher in der Praxis nur selten erreicht wird.

c) Marketing und AdTech

Im Jahr 2021 hat die luxemburgische Datenschutzbehörde CNPD mit 746 Mio. Euro das bislang höchste Bußgeld in der Geschichte des europäischen Datenschutzrechts gegen Amazon aufgrund eines festgestellten Verstoßes im Bereich der personalisierten Werbung verhängt.[6] Insoweit soll Amazon beim Tracking von Nutzern auf Webseiten, welche von anderen Anbietern operiert werden, datenschutzrechtliche Vorgaben nicht eingehalten haben.[7]

Anfang des Jahres 2022 gab die französische Datenschutzbehörde CNIL bekannt, dass sie ein Bußgeld von 150 Mio. Euro gegen Google und ein Bußgeld von 60 Mio. Euro gegen Facebook verhängt hat, weil

1 Datatilsynet, Administrative fine – Grindr LLC, 13.12.2021, unter www.noyb.eu/sites/default/files/2021-12/Administrative%20fine%20-%20Grindr%20LLC_Public%20version.pdf (Abruf: 8.3.2022).
2 Datatilsynet, Administrative fine – Grindr LLC, 13.12.2021 (Fn. 1), S. 14 ff.
3 DPC, Data Protection Commission announces decision in WhatsApp inquiry, 2.9.2021, unter www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry (Abruf: 8.3.2022).
4 EDSA, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, 28.7.2021, unter www.edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_ 202101_ie_sa_whatsapp_redacted_en.pdf (Abruf: 8.3.2022), S. 5.
5 DPC, In the matter of WhatsApp Ireland Limited Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, 20.8.2021, unter www.edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf (Abruf: 8.3.2022).
6 *Klages*, Rekordbußgeld gegen Amazon, 9.8.2021, unter www.datenschutz-notizen.de/rekordbussgeld-gegen-amazon-2530680/ (Abruf: 8.3.2022).
7 *Klages*, Rekordbußgeld gegen Amazon, 9.8.2021 (Fn. 6).

die Ablehnung von Cookies auf den jeweiligen Webseiten nicht so einfach gewesen war, wie deren Annahme.[8]

Im Übrigen verhängte die spanische Datenschutzbehörde, AEPD, ein Bußgeld von mehr als 8 Mio. Euro gegen Vodafone España aufgrund von festgestellten Verstößen gegen die DS-GVO und gegen spanisches Recht im Zusammenhang mit Werbemaßnahmen.[9] Die monierten Verstöße betrafen insbesondere die Nichtbeachtung von geltenden Anforderungen an die Nutzung von Auftragsverarbeitern in Ländern außerhalb des EWR sowie die Kontaktierungen von Personen zu Werbezwecken, ohne deren Einwilligung bzw. trotz deren vorher erklärten Widerspruchs.[10]

d) Deutschland: traditionell im Bereich Arbeitnehmerüberwachung

In Deutschland verhängen die Datenschutzbehörden traditionell im Bereich der Arbeitnehmerüberwachung die höchsten Bußgelder.

Bereits vor dem Inkrafttreten der DS-GVO wurde LIDL wegen der Verletzung des Beschäftigtendatenschutzrechts mit einem Bußgeld in Höhe von etwa 1,5 Mio. Euro belegt.[11] In 2020 verhängte der hamburgische Datenschutzbeauftragte gegen H&M wegen unzulässiger Ausspionierung von Beschäftigten das bisher höchste Bußgeld in Deutschland nach der Einführung der DS-GVO in Höhe von knapp 35,3 Mio. Euro.[12] Im Jahr 2021 kam es ebenfalls in Deutschland in diesem Bereich zu der Verhängung eins erheblichen Bußgeldes in Höhe von 10,4 Mio. Euro.[13]

II. Was bringt das Jahr 2022 im Bereich der behördlichen Sanktionierung?

1. Anstehende Richtungsentscheidungen

Die nachfolgenden Richtungsentscheidungen dürften einen maßgeblichen Einfluss auf die zukünftige Sanktionierungspraxis im Bereich des Datenschutzrechts haben.

a) EuGH-Vorlage: Verhältnis zwischen Art. 83 DS-GVO und § 30 OWiG

Eine in Deutschland bisher ungeklärte Frage ist, ob § 30 OWiG im Rahmen von DS-GVO-Bußgeldverfahren zur Anwendung kommen sollte. Diese Frage hat erhebliche Bedeutung, da § 30 OWiG für die Verhängung von Geldbußen gegen Unternehmen den Nachweis der Begehung einer Straftat oder Ordnungswidrigkeit durch eine vertretungsberechtigte oder leitende Person erfordert.

Das Landgericht Bonn entschied in seinem Urteil vom 11.11.2020 zu einem Bußgeld gegen einen Telekommunikationsanbieter, dass § 30 OWiG bei Bußgeldentscheidungen nach Art. 83 DS-GVO keine Anwendung findet, weil ansonsten eine divergierende Sanktionierungspraxis in Europa drohen würde.[14] Demgegenüber solle das aus dem EU-Kartellrecht bekannte Haftungsregime im Einklang mit der Intention des europäischen Gesetzgebers gelten, welches nicht den Nachweis eines Fehlverhaltens von Organen oder Leitungspersonen erfordert.[15]

Demgegenüber ging das Landgericht Berlin in seinem Beschluss vom 18.2.2021 von der Anwendung des § 30 OWiG in DS-GVO-Bußgeldverfahren aus und erklärte den Bußgeldbescheid gegen ein Immobilienunternehmen für unwirksam, weil darin insbesondere keine Begehung einer Ordnungswidrigkeit durch eine natürliche Person dargestellt wurde.[16]

Aufgrund einer sofortigen Beschwerde der Staatsanwaltschaft Berlin befasste sich das Kammergericht mit dem vorgenannten Beschluss und entschied sich hierbei zu einer Vorlage der vorgenannten Thematik zur Entscheidung durch den EuGH.[17] Der EuGH wird nunmehr zu klären haben, ob von einer Datenschutzbehörde eine durch eine natürliche Person begangene Ordnungswidrigkeit festgestellt werden muss, um in Deutschland ein DS-GVO-Bußgeld gegen ein Unternehmen verhängen zu können.[18] Sollte der EuGH diese Frage verneinen, hätte er nach der Vorlage des Kammergerichts noch zu entscheiden, ob ein schuldhaft begangener Verstoß zur Verhängung eines Bußgeldes nach der DS-GVO notwendig ist oder ob bereits lediglich ein „zuzuordnender objektiver Pflichtenverstoß" für eine Bebußung genügt.[19]

Aufgrund der bereits vom Landgericht Bonn verfolgten Argumentation zur Notwendigkeit einer einheitlichen Sanktionspraxis in der Europäischen Union erscheint es wahrscheinlicher, dass der EuGH keine Notwendigkeit der Feststellung einer Ordnungswidrigkeit durch eine natürliche Person annimmt. In jedem Fall wird die Entscheidung des EuGH Rechtssicherheit bei der Bußgeldverhängung in Deutschland schaffen und den deutschen Datenschutzbehörden aufzeigen, welche Anforderungen sie bei der Bußgeldverhängung und den diesbezüglichen Ermittlungen zu erfüllen haben werden. Darüber hinaus könnte die Antwort auf die zweite Vorlagefrage zur Notwendigkeit eines Verschuldens einen nicht unerheblichen Einfluss auf die europaweite Bußgeldpraxis haben. So würde ein Verzicht auf das Verschuldenserfordernis den Weg für ein datenschutzrechtliches Unternehmenssanktionsrecht ebnen und deutschen Datenschutzbehörden die Verhängung von Bußgeldern gegen Unternehmen deutlich erleichtern.

b) Europäisches Bußgeldmodell

Der bereits geschilderte WhatsApp-Fall und immer deutlicher werdende Kritik an der irischen Datenschutzbehörde[20] zeigen, dass die europäischen Datenschutzbehörden starkes Interesse an einer einheitlicheren Linie im Hinblick auf die Sanktionierung von DS-GVO-Verstößen haben. So verwundert die Ankündigung nicht, dass ein europäisches Bußgeldmodell entstehen soll.[21]

Fraglich scheint jedoch, ob hierbei das Konzept zur Bußgeldbemessung der deutschen Datenschutzbehörden, welches sich sehr stark auf

8 CNIL, Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation, 6.1.2022, unter www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance (Abruf: 8.3.2022).

9 *Borovsky/Brigagliano/Witt*, Cross-Border Data Transfers: Spain's Data Protection Authority Imposes Its Largest Fine, 24.3.2021, unter www.jdsupra.com/legalnews/cross-border-data-transfers-spain-s-2691270/ (Abruf: 8.3.2022).

10 *Borovsky/Brigagliano/Witt*, Cross-Border Data Transfers: Spain's Data Protection Authority Imposes Its Largest Fine, 24.3.2021 (Fn. 9).

11 Reuters Staff, Lidl akzeptiert Bußgeld wegen Bespitzelung, 11.9.2008, unter www.reuters.com/article/deutschland-einzelhandel-datenschutz-zf-idDEBER15559420080911 (Abruf: 8.3.2022).

12 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg, 35,3 Mio. Euro Bußgeld wegen Datenschutzverstößen im Servicecenter von H&M, 1.10.2020, unter www.datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren (Abruf: 8.3.2022).

13 Die Landesbeauftragte für den Datenschutz Niedersachsen, LfD Niedersachsen verhängt Bußgeld über 10,4 Mio. Euro gegen notebooksbilliger.de, 8.1.2021, unter www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html (Abruf: 8.3.2022).

14 LG Bonn, 11.11.2020 – 29 OWi 1/20, ZD 2021, 154, 156.

15 LG Bonn, 11.11.2020 – 29 OWi 1/20, ZD 2021, 154, 156.

16 LG Berlin, 18.2.2021 – 526 OWi LG 212 Js-OWi 1/20 (1/20), ZD 2021, 270, 271.

17 KG Berlin, 6.12.2021 –3 Ws 250/21, K&R 2022, 135 mit K&R-Komm. *Schnabe*l, BeckRS 2021, 39748, Rn. 6.

18 KG Berlin, 6.12.2021 – 3 Ws 250/21, K&R 2022, 135 mit K&R-Komm. *Schnabe*l, BeckRS 2021, 39748, Tenor.

19 KG Berlin, 6.12.2021 – 3 Ws 250/21, K&R 2022, 135 mit K&R-Komm. *Schnabe*l, BeckRS 2021, 39748, Tenor.

20 *Fanta*, in: Netzpolitik.org vom 18.3.2021, unter www.netzpolitik.org/2021/vorwurf-von-ulrich-kelber-irische-datenschutzbehoerde-macht-falsche-aussagen/ (Abruf: 8.3.2022).

21 EDSA, EDPB Work Programme 2021/2022, 16.3.2021, unter www. edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf (Abruf: 8.3.2022).

den weltweit erzielten Vorjahresumsatz eines Unternehmens fokussiert, als Vorbild dienen wird.[22] So hat das Landgericht Bonn in seinem – bereits vorstehend erwähnten – rechtskräftigen Urteil vom 11.11.2020 moniert, dass sich das Bußgeldkonzept der deutschen Behörden zu stark an dem Umsatz orientiert, was aus Sicht des Gerichts in dieser Form nicht aus der DS-GVO hervorgeht.[23]

Es bleibt abzuwarten, wie das zukünftige europäische Bußgeldmodell letztlich aussehen wird. Allerdings ist zu vermuten, dass es einen Ansatz enthalten wird, welcher weniger stark auf den Unternehmensumsatz abstellt, sondern eine ausgewogenere Berücksichtigung sämtlicher in Art. 83 Abs. 2 DS-GVO vorgesehenen Bemessungskriterien vorsieht.

2. Erwartete Schwerpunktthemen der behördlichen Sanktionierung

Auf Basis der vorstehend dargelegten Entwicklungen spricht einiges dafür, dass die folgenden Themen mit Blick auf das Jahr 2022 und darüber hinaus Schwerpunktbereiche darstellen, in denen das Risiko einer Verhängung von wesentlichen Bußgeldern durch europäische Aufsichtsbehörden besonders hoch erscheint. Unternehmen sollten den Fokus ihrer Bemühungen im Bereich der Datenschutz-Compliance demnach insbesondere auf die nachfolgenden Felder legen.

a) Internationale Datenübermittlungen

Nachdem das sog. Schrems II-Urteil bald zwei Jahre zurückliegt und die Aufsichtsbehörden in der Vergangenheit bei der Durchsetzung der in dem Urteil aufgestellten Anforderungen[24] an internationale Datenübermittlungen Zurückhaltung gezeigt haben, ist zu erwarten, dass sich dies künftig ändern wird. Internationale Datenübermittlungen rücken auch aufgrund von Beschwerden zunehmend in den Fokus der Aufsichtsbehörden.

aa) Anforderungen des Schrems II-Urteils vom 16.7.2020

In seinem Schrems II-Urteil vom 16.7.2020[25] hat der EuGH den für Datenübermittlungen aus der EU in die USA verabschiedeten EU-US Privacy Shield-Beschluss für ungültig erklärt.[26] Übermittlungen auf der Grundlage von geeigneten Garantien, wie Standarddatenschutzklauseln oder verbindlichen internen Datenschutzvorschriften (*Binding Corporate Rules*), bleiben nach dem Urteil aber vom Grundsatz her weiterhin zulässig. Unternehmen müssen jedoch zusätzliche Anforderungen erfüllen, wenn sie auf dieser Basis personenbezogene Daten in ein Drittland übermitteln wollen.[27] Insbesondere müssen eine Einzelfallbeurteilung im Hinblick auf einen angemessenen Schutz im jeweiligen Drittland[28] (*Transfer Impact Assessment*, „TIA") vorgenommen und, sofern notwendig und zielführend, zusätzliche Schutzmaßnahmen (technischer, organisatorischer und/oder vertraglicher Natur) getroffen werden.[29]

bb) Erste Behördenentscheidungen

Bisher kam es in diesem Bereich lediglich zu vereinzelten behördlichen Entscheidungen, wobei zu Beginn des Jahres 2022 ein Trend erkennbar wird, wonach Datenschutzbehörden im Hinblick auf die Durchsetzung der Vorgaben des Schrems II-Urteils deutlich aktiver werden wollen.

So hat das Bayerische Landesamt für Datenschutzaufsicht („BayLDA") im März 2021 die Nutzung des Newsletter-Dienstes „Mailchimp" untersagt, weil der US-Dienstleister unter Sec. 702 FISA, also das vom EuGH monierte Überwachungsgesetz der USA, falle und keine Prüfung im Hinblick auf die Implementierung möglicher Schutzmaßnahmen erfolgt sei.[30]

Außerdem hat der Europäische Datenschutzbeauftragte („EDSB") Anfang 2022 moniert, dass das Europäische Parlament beim Tracking auf einer seiner Webseiten zur Durchführung von COVID-19 Tests unter anderem *Google Analytics* eingesetzt hatte, welches Nutzerdaten in die USA übermittelte.[31] *Google Analytics* und die Trackingsoftware eines weiteren US-Anbieters wurden Ende 2020 auf der besagten Webseite deaktiviert.[32] Nachdem das Parlament auf Anfrage des EDSB keinen Nachweis zu implementierten vertraglichen, technischen und organisatorischen Maßnahmen zur Sicherstellung eines der Sache nach gleichwertigen Schutzniveaus bei den Datenübermittlungen in die USA erbringen konnte, ging der EDSB hinsichtlich des damaligen Einsatzes von *Google Analytics* unter anderem davon aus, dass die Vorgaben des Schrems II-Urteils nicht erfüllt worden waren, und verwarnte das Parlament.[33]

Mit ähnlichen Erwägungen hatten zuletzt auch die österreichische Datenschutzbehörde am 13.1.2022[34] und die französische Datenschutzbehörde am 10.2.2022[35] für den Einsatz des von dem jeweiligen Webseitenbetreiber genutzten Tracking-Tools *Google Analytics* festgestellt, dass – in dem von ihnen jeweils entschiedenen Fall – die Standardvertragsklauseln keine ausreichenden Garantien darstellten.[36] Diese würden auch in Verbindung mit den zum relevanten Zeitpunkt durch Google implementierten zusätzlichen Maßnahmen keinen ausreichenden Schutz vor möglichen Zugriffen von US-Geheimdiensten bieten.[37]

cc) Einschätzung

Nachdem Unternehmen mehr als eineinhalb Jahre Zeit für die Umsetzung der Vorgaben des Schrems II-Urteils hatten, ist davon auszugehen, dass Datenschutzbehörden mittlerweile zumindest die Erfüllung von grundsätzlichen Anforderungen des Urteils (also insbesondere die Prüfung der Datenflüsse in Drittländer, die Durchführung von TIAs, die Implementierung von zusätzlichen Maßnahmen und den

22 Datenschutzkonferenz, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, unter www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf (Abruf: 8.3.2022).
23 LG Bonn, 11.11.2020 –29 OWi 1/20, ZD 2021, 154, 158.
24 Dazu ausführlich *Schröder*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 46, Rn. 17 f.
25 EuGH, 16.7.2020 – C-311/18, K&R 2020, 588, WRP 2020, 1158.
26 EuGH, 16.7.2020 – C-311/18, K&R 2020, 588, WRP 2020, 1158, 1174 ff., Rn. 198 ff.
27 EuGH, 16.7.2020 – C-311/18, K&R 2020, 588, WRP 2020, 1158, Rn. 132 ff.
28 Drittländer sind Länder, welche nicht Teil des EWR sind.
29 EuGH, 16.7.2020 – C-311/18, K&R 2020, 588, 591 ff., WRP 2020, 1158, 1167 ff., Rn. 132 ff.
30 GDPRHub, Zusammenfassung der Entscheidung des BayLDA v. 15.3.2021, LDA-1085.1-12159/20-IDV, unter www.gdprhub.eu/index.php?title=BayLfD_(Bavaria)_-_LDA-1085.1-12159/20-IDV (Abruf: 8.3.2022).
31 European Data Protection Supervisor, Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament, 5.1.2022, unter www.noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf (Abruf: 8.3.2022), S. 2, 12 ff.
32 European Data Protection Supervisor, Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament, 5.1.2022 (Fn. 31), S. 3.
33 European Data Protection Supervisor, Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament, 5.1.2022 (Fn. 31), S. 12 ff., 18.
34 Österreichische DSB, Teilbescheid, 13.1.2022, D155.027, 2021-0.586.257, unter www.dsb.gv.at/dam/jcr:c1eb937b-7527-450c-8771-74523b01223c/D155.027%20GA.pdf (Abruf: 8.3.2022).
35 CNIL, Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply, 10.2.2022, unter www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply (Abruf: 8.3.2022).
36 CNIL, Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply, 10.2.2022 (Fn. 35); Österreichische DSB, Teilbescheid, 13.1.2022, D155.027, 2021-0.586.257, a. a. O., S. 32 ff.
37 CNIL, Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply, 10.2.2022 (Fn. 35); Österreichische DSB, Teilbescheid, 13.1.2022, D155.027, 2021-0.586.257 (Fn. 34), S. 35 f.

Stopp gewisser Datenübermittlungen) erwarten.[38] Allerdings werden Behörden bei Überprüfungen, womöglich aufgrund von bei ihnen eingegangen Beschwerden, weiterhin auf Fälle treffen, in denen diese Anforderungen noch nicht (vollständig) erfüllt worden sind, weshalb es nur als eine Frage der Zeit erscheint, bis in diesem Bereich das erste nennenswerte Bußgeld verhängt wird.

Insbesondere wird der Druck auf Behörden insoweit tätig zu werden – auch durch Datenschutzaktivisten wie Max Schrems und seine Organisation NOYB – stetig erhöht. So stellten die beiden vorgenannten Entscheidungen zu *Google Analytics* Reaktionen auf Beschwerden von NOYB dar, wobei NOYB allein in Bezug auf Drittlandsübermittlungen beim Einsatz von *Google Analytics* und *Facebook Connect* nach eigenen Angaben insgesamt 101 Beschwerden im gesamten EWR eingereicht hat.[39]

Darüber hinaus hat beispielweise die französische Datenschutzbehörde erst im Februar 2022 angekündigt, künftig auch verstärkt den Einsatz von Cloud-Dienstleistern im Hinblick auf Drittlandsübermittlungen zu überprüfen.[40]

b) Fehlende oder unzureichende Rechtsgrundlage

Auch bei der Verarbeitung von Daten ohne oder bei unzureichender Rechtsgrundlage ist in Zukunft mit weiteren wesentlichen Bußgeldern zu rechnen. Dies liegt auch daran, dass in Bezug auf diverse Rechtsgrundlagen – wie etwa der Wahrnehmung berechtigter Interessen, auf die in der Praxis vielfach zur Rechtfertigung zurückgegriffen wird – interpretationsbedürftige Einzelfallprüfungen notwendig sind. Allein schon aufgrund der ständigen Einführung von neuen Geschäftsmodellen und Technologien, deren datenschutzrechtliche Rechtmäßigkeit aus Sicht der Behörden erst noch geklärt werden muss, kann insoweit regelmäßig eine gewisse Rechtsunsicherheit nicht vermieden werden.

Des Weiteren werden personenbezogene Daten und deren Verarbeitung für Unternehmen aus nahezu allen Wirtschaftszweigen immer wichtiger, so dass hierdurch die Anzahl und der Umfang von Datenverarbeitungsaktivitäten sowie gleichzeitig auch der Innovationsdruck stetig wächst, wodurch auch das Risiko ansteigt, dass personenbezogene Daten ohne (hinreichende) Rechtsgrundlage verarbeitet werden.

Besonders risikoreich ist der „Blindflug" von Unternehmen, die keine Übersicht über ihre Datenverarbeitungen (sog. *Data Mapping*) haben und daher nicht einmal im Ansatz geprüft haben, ob ihre Datenverarbeitungen rechtskonform sind. Einmal mehr unterstreicht das wachsende Bußgeldrisiko die Wichtigkeit eines sorgfältig erstellten Verarbeitungsverzeichnisses und einer gründlichen Prüfung der Voraussetzungen der Rechtsgrundlage vor Beginn der Datenverarbeitungen.

c) Transparenzpflichten

In Anbetracht des verbindlichen Beschlusses des EDSA in dem vorgenannten WhatsApp-Fall (s. unter I.1.b) dürften auch Transparenzpflichten insbesondere im Hinblick auf öffentlich (beispielsweise auf Webseiten) einsehbare Datenschutzhinweise und -erklärungen in den Fokus der europäischen Sanktionspraxis rücken.

Wie vorstehend dargelegt, hat der EDSA hohe Anforderungen an die Erfüllung von Informationspflichten und insbesondere an deren Detailgrad gestellt.[41] Bei der Umsetzung dieser Anforderungen wird der ohnehin schon schwierige Balanceakt zwischen der einerseits von Behörden nunmehr erwarteten Genauigkeit und der andererseits gewünschten Praktikabilität und Verständlichkeit der Datenschutzhinweise für Unternehmen zu einer noch größeren Herausforderung werden. Sehr detaillierte Datenschutzhinweise führen in Anbetracht der sich stetig ändernden Datenverarbeitungsaktivitäten regelmäßig zu erheblichem und ständigem Aktualisierungsaufwand. Es ist zu erwarten, dass sich insoweit modulare Ansätze, welche ohne allzu großen Aufwand in verschiedener Hinsicht aktualisiert werden können, mehr und mehr durchsetzen. Unternehmen sollten insofern zeitnah ihre Datenschutzhinweise und -erklärungen überprüfen und ergänzen lassen.

d) Marketing und AdTech

In Anbetracht der vorstehend dargelegten gravierenden Bußgelder im Bereich Marketing und AdTech ist zu erwarten, dass dieses Feld auch in der Zukunft eines der Schwerpunktthemen für behördliche Sanktionierungen darstellen wird.

Hierfür sprechen auch die erwähnten Entscheidungen der österreichischen und französischen Datenschutzbehörden zu *Google Analytics* und die zahlreichen weiteren Beschwerden, die NOYB bei Behörden bei verschiedenen Aufsichtsbehörden im EWR eingereicht hat, über die noch keine Entscheidungen gefällt wurden.

Außerdem hat beispielweise die CNIL erst im Februar 2022 angekündigt, im Jahr 2022 insbesondere die rechtskonforme Datenverarbeitung im Bereich der kommerziellen Werbung überprüfen zu wollen.[42]

e) Datenschutzverletzungen

In dem Bericht zur Lage der IT-Sicherheit in Deutschland 2021 bilanzierte das Bundesamt für Sicherheit in der Informationstechnik („BSI"), dass die Digitalisierung – auch durch COVID-19 – in Deutschland sowie weltweit schnell voranschreitet und stellte gleichzeitig fest, dass die Bedrohungslage durch Cyber-Angriffe weiter zugenommen hat.[43] Zugleich steigt auch das Risiko, dass Unternehmen im Zusammenhang mit der zunehmend angespannten geopolitischen Weltlage Opfer von (teils auch staatlich organisierten) Cyber-Angriffen werden.

Nachdem die DS-GVO sowohl im Hinblick auf die Annahme einer Datenschutzverletzung als auch die Meldepflicht gegenüber der/n zuständigen Datenschutzbehörde/n sehr niedrige Schwellen vorsieht, dürfte die Beachtung dieser Vorgaben zukünftig immer schwerer fallen.

In Anbetracht der vorstehenden Umstände und auch der stetig steigenden Mengen an verarbeiteten personenbezogenen Daten erscheint die Wahrscheinlichkeit demnach relativ hoch, dass es in diesem Bereich zu wesentlichen Sanktionierungen kommen wird.

Unternehmen können ihr Bußgeldrisiko aber insbesondere durch die Implementierung von technischen und organisatorischen Maßnahmen, die dem Stand der Technik entsprechen, sowie die Sensibilisierungen der Beschäftigten im Hinblick auf (i) IT-Sicherheit, (ii) den Umgang mit personenbezogenen Daten und (iii) die sofortige Mel-

38 Vgl. BayLDA, 10. Tätigkeitsbericht 2020, Juli 2021, unter www.lda.bayern.de/media/baylda_report_10.pdf (Abruf: 8.3.2022), S. 47 f.

39 NOYB, 101 Beschwerden zu EU-US-Transfers eingereicht, 17.8.2020, unter www.noyb.eu/de/101-beschwerden-zu-eu-us-transfers-eingereicht (Abruf: 8.3.2022).

40 CNIL, Priority topics for investigations in 2022: commercial prospecting, cloud and telework monitoring, 15.2.2022, unter www.cnil.fr/en/priority-topics-investigations-2022-commercial-prospecting-cloud-and-telework-monitoring (Abruf: 8.3.2022).

41 EDSA, Binding Decision 01/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, 28.7.2021 (Fn. 4), S. 17.

42 CNIL, Priority topics for investigations in 2022: commercial prospecting, cloud and telework monitoring, 15.2.2022 (Fn. 40).

43 BSI, Die Lage der IT-Sicherheit in Deutschland 2021, September 2021, unter www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3 (Abruf: 8.3.2022).

dung von Sicherheitsvorfällen an die zuständigen Stellen im Unternehmen maßgeblich verringern.[44]

III. Bisherige Schwerpunkte der privaten Rechtsdurchsetzung im Datenschutzrecht

Nachdem im Datenschutzrecht für lange Zeit eine besondere Aufmerksamkeit auf der behördlichen Rechtsdurchsetzung lag, rückte insbesondere im Jahr 2021 die private Rechtsdurchsetzung mehr und mehr in den Fokus.

1. Immaterieller Schadensersatz

Ein in seiner Bedeutung stetig wachsendes Instrument der privaten Rechtsdurchsetzung ist der immaterielle Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO. So ist es insbesondere bei Auseinandersetzungen mit ehemaligen Mitarbeitern inzwischen geübte Praxis der Arbeitnehmervertreter, Schadensersatz wegen behaupteter datenschutzrechtlicher Verstöße zu verlangen.

In der Praxis sind jedoch zahlreiche Fragen bislang ungeklärt und insoweit Vorabentscheidungsverfahren beim EuGH anhängig.[45] Ungeklärt ist insbesondere die Frage, ob Betroffene das Vorliegen eines immateriellen Schadens näher darlegen und beweisen müssen sowie ferner die Frage, ob Art. 82 Abs. 1 DS-GVO auch die Geltendmachung von Bagatellschäden ermöglicht. Insoweit ist es nicht verwunderlich, dass die im Jahr 2021 erheblich angewachsene Liste[46] der Gerichtsentscheidungen im Kontext datenschutzrechtlicher Schadensersatzansprüche keine einheitliche Linie erkennen lässt. So hat ein nicht unerheblicher Teil der Gerichte Schadensersatzklagen unter Verweis auf eine Bagatellschwelle oder wegen eines nicht nachgewiesenen Schadens abgewiesen.[47] Besonders in jüngerer Zeit mehren sich jedoch Entscheidungen, die einen immateriellen Schadensersatz bis zu einem mittleren vierstelligen Bereich zusprechen und dabei zum Teil auf den Nachweis eines Schadenseintritts verzichten. So haben Gerichte etwa immaterielle Schadensersatzansprüche i. H. v. 5000 Euro für eine um einige Monate verspätete und unvollständige Beantwortung eines Auskunftsersuchens,[48] für eine rechtswidrige Meldung eines Betroffenen bei der SCHUFA[49] sowie für eine rechtswidrige Erhebung sensibler Daten i. S. v. Art. 10 DS-GVO[50] zugesprochen. Ferner wurden immaterielle Ersatzansprüche i. H. v. 2500 Euro infolge einer Datenschutzverletzung aufgrund eines IT-Sicherheitsvorfalls[51] sowie i. H. v. 2000 Euro für eine rechtsgrundlose konzerninterne Datenübermittlung[52] zuerkannt.

Eine besonders niedrige Schwelle für die Geltendmachung von Schadensersatzansprüchen legt das Bundesarbeitsgericht („BAG") an. Nach seinem Vorlagebeschluss an den EuGH vom August 2021 ist das BAG der Auffassung, dass *jede* Verletzung der DS-GVO zu einem auszugleichenden immateriellen Schaden bei den Betroffenen führen soll, ohne dass diese einen weiteren Beweis über den Schadenseintritt anzutreten hätten.[53] Zudem geht das BAG – wie zuvor andere Gerichte – davon aus, dass mit dem Schadensersatz auch eine „wirklich abschreckende Wirkung" zu gewährleisten sei.[54]

Von diesen theoretischen Fragen abgesehen zeigt jedenfalls ein Blick auf die Entscheidungen, in denen ein Schadensersatz zugesprochen wurde, einen eindeutigen Trend: Die Zahl der Entscheidungen steigt, ebenso wie der Umfang der zuerkannten Schadensersatzsummen. Auch die von Schadensersatzklagen betroffenen Themenbereiche werden zunehmend vielfältiger. Besonders im Beschäftigungskontext besteht dabei nach wie vor ein stetiges Schadensersatzrisiko.

Aufsehen erregte auch ein Urteil des OLG Dresden, in dem von einer Verantwortlichkeit eines Geschäftsführers für einen festgestellten Verstoß gegen die DS-GVO (neben der Verantwortlichkeit der Gesellschaft) ausgegangen und der vom LG Dresden zugesprochene Anspruch auf immateriellen Schadensersatz i. H. v. 5000 Euro bestätigt wurde.[55] Demnach kann der vorgenannte Trend nicht nur ein wesentliches Risiko für Unternehmen, sondern auch für Geschäftsführer selbst darstellen.

2. Betroffenenrechte

Ein mit den Schadensersatzrisiken eng zusammenhängendes Themenfeld betrifft die Betroffenenrechte der Art. 15 ff. DS-GVO. Insbesondere der Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO, dessen konkreter Umfang teilweise noch umstritten ist, erweist sich oftmals als „Einfallstor" für weitere private Durchsetzungsmaßnahmen. Dies unterstreicht einmal mehr die Wichtigkeit eines funktionsfähigen Betroffenenrechte-Managements einerseits, andererseits aber auch die Bedeutung eines möglichst geordneten Ausscheidens von Beschäftigten. Denn immer öfter stellen ehemalige Beschäftigte im Rahmen von Kündigungen auch Auskunftsansprüche, um im Fall einer unzulänglichen Beantwortung ihre Verhandlungsposition in Abfindungsverhandlungen durch potentielle Schadensersatzansprüche gegen den (früheren) Arbeitgeber zu stärken. Auch hinsichtlich der Geltendmachung von Betroffenenrechten bestehen daher mitunter die größten Risiken im Beschäftigungskontext. Doch auch die stetig ansteigende Zahl an Cyber-Attacken bilden ein wachsendes Risiko für Unternehmen,[56] im Fall eines Sicherheitsvorfalles mit einer Vielzahl von Auskunftsansprüchen konfrontiert zu werden.

3. Datenschutzrechtliche Unterlassungsansprüche

Vergleichsweise wenig Aufmerksamkeit wurde bislang der Frage zuteil, ob Verstöße gegen datenschutzrechtliche Vorschriften auch zivilrechtliche bzw. öffentlich-rechtliche Unterlassungsansprüche gegen den Verantwortlichen oder Auftragsverarbeiter auslösen können. Trotz einer beachtlichen Fülle gerichtlicher Entscheidungen[57] scheint die Frage noch nicht eindeutig geklärt zu sein. In einer erheblichen Anzahl an Entscheidungen wurden Betroffenen im Falle rechtswidriger Datenverarbeitungen bereits ein Unterlassungsanspruch zugesprochen, wobei jedoch wiederum Uneinigkeit herrscht, aus welcher Anspruchsgrundlage dieser abzuleiten ist. So wird der Unterlassungsanspruch teils auf § 1004 Abs. 1 S. 2 BGB i. V. m. § 823 Abs. 1 BGB analog,[58] teils auch i. V. m. § 823

44 S. auch *Schröder/Lantwin*, ZD 2021, 614 zu den erforderlichen Schritten eines effektiven Krisenmanagements bei IT-Sicherheitsvorfällen.

45 Der Österreichische OGH und das BAG haben Vorlagefragen u. a. zur Auslegung des Art. 82 DS-GVO vorgelegt; ÖOGH,. 23.6.2021 – 6 Ob 56/21k, ZD 2021, 627; BAG, 26.8.2021 – 8 AZR 253/20 (A), BB 2021, 2739 Ls, BeckRS 2021, 29622.

46 Einen sehr ausführlichen Überblick über die bis Ende 2021 ergangenen Entscheidungen gibt *Leibold*, ZD 2022, 18.

47 So etwa OLG Dresden, 20.8.2020 – 4 U 784/20, ZD 2021, 93; LG Karlsruhe, 9.2.2021 – 4 O 67/20, ZD 2022, 55; AG Frankfurt a. M., 10.7.2020 – 385 C 155/19 (70), ZD 2021, 47.

48 ArbG Düsseldorf, 3.2.2020 – 9 Ca 6557/18, NZA-RR 2020, 409.

49 LG Mainz, 12.11.2021 – 3 O 12/20, GRUR-RS 2021, 34695.

50 OLG Dresden, 30.11.2021 – 4 U 1158/21, BeckRS 2021, 39660.

51 LG München I, 9.12.2021 – 31 O 16606/20, BeckRS 2021, 41707.

52 LAG Hamm, 14.12.2021 – 17 Sa 1185/20, BeckRS 2021, 45536.

53 BAG, 26.8.2021 – 8 AZR 253/20 (A), BB 2021, 2739 Ls, BeckRS 2021, 29622, Rn. 33.

54 BAG, 26.8.2021 – 8 AZR 253/20 (A), BB 2021, 2739 Ls, BeckRS 2021, 29622, Rn. 36; ähnlich auch OLG Dresden, 30.11.2021 – 4 U 1158/21; LG Mainz, 12.11.2021 – 3 O 12/20, GRUR-RS 2021, 34695; ArbG Düsseldorf, 5.3.2020 – 9 Ca 6557/18, ZD 2020, 649, 650.

55 OLG Dresden, 30.11.2021 – 4 U 1158/21, ZD 2022, 159.

56 Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2021, September 2021 (Fn. 43).

57 Ein umfassender Überblick über die Entscheidungen findet sich bei *Leibold/Laoutoumai*, ZD-Aktuell 2021, 05583.

58 LG Darmstadt, 26.5.2020 – 13 O 244/19, ZD 2020, 642, 643; LG München I, 20.1.2022 – 3 O 17493/20, BeckRS 2022, 612; zahlr. w. N. bei *Leibold/Laoutoumai*, ZD-Aktuell 2021, 05583.

Abs. 2 BGB und DS-GVO-Vorschriften als Schutzgesetze[59] gestützt oder sehr vereinzelt direkt aus der DS-GVO[60] abgeleitet.[61] Teile der Literatur und der Rechtsprechung lehnen einen Unterlassungsanspruch hingegen in Gänze ab, denn nach Art. 79 DS-GVO seien allenfalls die Betroffenenrechte der Art. 15 ff. DS-GVO gerichtlich durchsetzbar, nicht aber ein Unterlassungsanspruch nach nationalem Recht.[62]

Die überwiegende Zahl der deutschen Gerichte, welche sich bisher mit der Thematik befasst haben, scheint jedenfalls von dem Bestehen eines Unterlassungsanspruchs nach § 1004 Abs. 1 S. 2 BGB i.V.m. § 823 Abs. 1 oder 2 BGB (ggf. i.V.m. Schutzgesetzen der DS-GVO) auszugehen.[63] Damit stellen sich weitere Folgefragen, insbesondere etwa, ob ein möglicher Ersatz von Abmahnkosten alte Befürchtungen einer Abmahnwelle im Datenschutzrecht wiederaufleben lässt. Zusätzlich besteht für Unternehmen das Risiko, dass die Rechtsdurchsetzung im Datenschutzrecht durch Verfahren im einstweiligen Rechtsschutz teils deutlich beschleunigt werden könnte.

4. Erste deutsche Gerichtsentscheidungen nach dem Schrems II-Urteil

Schließlich erreichen die Folgen des Schrems II-Urteils nun vermehrt auch deutsche Gerichte. So hatten sich Land- und Verwaltungsgerichte in jüngerer Zeit mit internationalen Datenübermittlungen in die USA auseinanderzusetzen und in diesem Zusammenhang Untersagungsverfügungen für Datenübermittlungen in Drittländer ausgesprochen oder sogar Schadensersatzansprüche zuerkannt. Das VG Wiesbaden hatte die Verwendung eines Cookie-Consent-Management-Tools im Wege einer einstweiligen Anordnung untersagt, da mit ihr eine unrechtmäßige Datenübermittlung in die USA verbunden sei und der rechtswirksame Abschluss von Standardvertragsklauseln nicht nachgewiesen werden konnte (diese im einsteiligen Rechtsschutzverfahren ergangene Entscheidung ist inzwischen aufgehoben).[64] In einem anderen Fall hat das Landgericht München I einen Unterlassungsanspruch wegen einer unrechtmäßigen Übermittlung von IP-Adressen in die USA durch den Einsatz von *Google Fonts* bejaht und zugleich einen immateriellen Schadensersatzanspruch i.H.v. 100 Euro zugesprochen.[65] Wenngleich folglich noch keine ausgeprägte gerichtliche Fallpraxis im Zusammenhang mit Datenübermittlungen in Drittländer besteht, deuten diese Entscheidungen darauf hin, dass die zunehmende behördliche Durchsetzung der Vorgaben des Schrems II-Urteils allmählich auch durch flankierende gerichtliche Entscheidungen begleitet wird.

IV. Was bringt das Jahr 2022 im Bereich der privaten Rechtsdurchsetzung?

Es ist zu erwarten, dass sich einige der im Jahr 2021 gesetzten Trends aller Voraussicht nach auch im Jahr 2022 fortsetzen werden und die private Rechtsdurchsetzung des Datenschutzrechts weiter an Bedeutung gewinnen wird.

1. Anstehende Richtungsentscheidungen

Mit Spannung erwartet werden insbesondere die Entscheidungen in den derzeit beim EuGH anhängigen Vorabentscheidungsverfahren zum immateriellen Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO.[66] Die Entscheidungen werden maßgeblichen Einfluss darauf haben, welche Bedeutung die Durchsetzung von immateriellem Schadensersatzansprüchen in Zukunft haben wird.

Im Übrigen ist in Anbetracht eines diesbezüglichen Vorabentscheidungsersuchens aus Finnland zu erwarten, dass der EuGH die Reichweite des Auskunftsanspruchs nach Art. 15 DS-GVO näher konkretisieren wird.[67]

2. Erwartete Schwerpunktthemen

Für das Jahr 2022 ist generell mit einer Intensivierung der privaten Durchsetzung des Datenschutzrechts zu rechnen. Hierbei dürften die Schwerpunkte in den nachfolgenden Bereichen liegen.

a) Immaterielle Schadensersatzansprüche und Betroffenenrechte

Angesichts der immer vielfältigeren Fallkonstellationen, in denen Schadensersatzansprüche gerichtlich zugesprochen werden, ist auch im Jahr 2022 mit einem umfassend steigenden Risiko der Geltendmachung von Schadensersatzansprüchen in unterschiedlichen materiellen Bereichen des Datenschutzrechts zu rechnen. Wesentliche Schwerpunkte dürften dabei künftig auch internationale Datenübermittlungen sowie Datenschutzverletzungen (u.a. nach Cyber-Angriffen) darstellen. Gerichtsentscheidungen aus der Vergangenheit zeigen jedoch, dass auch klassische Compliance-Themen, wie etwa konzerninterne Datenübermittlungen, insoweit verstärkt in den Fokus geraten.[68] In vielen Fällen bilden dabei Auskunftsersuchen die Grundlage für weitere private Durchsetzungsmaßnahmen.[69] Insbesondere im Beschäftigungskontext ist zu erwarten, dass Beschäftigte im Rahmen von Kündigungsstreitigkeiten versuchen oder zumindest in Aussicht stellen werden, unterschiedliche Möglichkeiten wahrzunehmen, gegen den (früheren) Arbeitgeber wegen einer etwaigen Verletzung des Datenschutzrechts vorzugehen. Unternehmen sollten das Ausscheiden von Mitarbeitern deshalb auch im Interesse der Vermeidung datenschutzrechtlicher Haftungsrisiken durch ein möglichst geordnetes „Offboarding" begleiten und ein besonderes Augenmerk auf den Beschäftigtendatenschutz legen.

59 So etwa OLG Köln, 14.11.2019 – 14.11.2019, MMR 2020, 186, 187; OLG Stuttgart, 18.5.2021 – 12 U 296/20, ZD 2022, 105; LG Hamburg, 13.2.2020 – 312 O 372/18, ZD 2020, 477, 478; LAG Hamm, 14.12.2021 – 17 Sa 1185/20; zahlr. w. N. bei *Leibold/Laoutoumai*, ZD-Aktuell 2021, 05583.

60 LG Frankfurt a.M., 28.6.2019 – 2-03 O 315/17, ZD 2019, 410, 411; offenbar auch *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 79, Rn. 1.

61 Vgl. *Leibold/Laoutoumai*, ZD-Aktuell 2021, 05583.

62 Vgl. *Leibold/Laoutoumai*, ZD-Aktuell 2021, 05583; vgl. mit im Wesentlichen ähnlichen Wertungen: VG Regensburg, 6.8.2020 – RN 9 K 19.1061, ZD 2020, 601, 602; ferner LG Wiesbaden, 22.1.2022 – 10 O 21; LG München I, 7.11.2019 – 34 O 13123/19, ZD 2020, 204; LG Mainz, 24.10.2019 – 5 O 283/19; *Kreße*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 79, Rn. 30.

63 Vgl. *Leibold/Laoutoumai*, ZD-Aktuell 2021, 05583 m.w.N.

64 VG Wiesbaden, 1.12.2021 – 6 L 738/21.WI; aufgehoben durch den Hessischen VGH, 17.1.2022 – 10 B 2486/21, jedoch nicht aus datenschutzrechtlichen Erwägungen, sondern weil der Antragsteller bereits einen Anordnungsgrund i.S.d. § 123 Abs. 3 VwGO i.V.m. § 920 Abs. 2 ZPO nicht glaubhaft gemacht habe.

65 LG München I, 20.1.2022 – 3 O 17493/20, BeckRS 2022, 612.

66 Fragen zu Einzelheiten und Umfang des Schadensersatzes wurden u.a. vorgelegt durch ÖOGH, 23.6.2021 – 6 Ob 56/21k, ZD 2021, 627; BAG, 26.8.2021 – 8 AZR 253/20 (A), BB 2021, 2739 Ls, BeckRS 2021, 29622; LG Saarbrücken, 22.11.2021 – 5 O 151/19, GRUR-Prax 2022, 95.

67 Fragen zu Einzelheiten und Umfang des Auskunftsanspruchs wurden u.a. vorgelegt durch *Itä-Suomen hallinto-oikeus (Finnland)*, Vorabentscheidungsersuchen v. 22.9.2021 – C-579/21, BeckEuRS 2021, 746655.

68 Vgl. insb. LAG Hamm, 14.12.2021 – 17 Sa 1185/20, BeckRS 2021, 45536.

69 S. z.B. LAG Hamm, 11.5.2021 – 6 Sa 1260/20, ZD 2021, 710; ArbG Düsseldorf, 5.3.2020 – 9 Ca 6557/18, NZA-RR 2020, 409.

b) Zunahme einstweiliger Verfügungsverfahren?

Nachdem bereits eine erhebliche Anzahl an deutschen Gerichten davon ausgegangen ist, dass auch im Datenschutzrecht Unterlassungsansprüche bestehen,[70] ist auch im Jahr 2022 mit einer fortgesetzten gerichtlichen Durchsetzung datenschutzrechtlicher Unterlassungsansprüche zu rechnen. Insoweit dürfte zudem zu erwarten sein, dass Betroffene zunehmend auch eine Durchsetzung im Wege des einstweiligen Rechtsschutzes versuchen werden. Beim einstweiligen Rechtsschutz könnte es sich jedoch nicht selten als schwierig erweisen, den Anordnungs- bzw. Verfügungsgrund ausreichend glaubhaft zu machen.[71]

c) Massenklage- und Verbandsklageverfahren

Eine künftige Möglichkeit zur privaten Rechtsdurchsetzung bildet die europäische Verbandsklage-Richtlinie,[72] die bis Ende 2022 durch die Mitgliedstaaten in nationales Recht zu überführen ist.[73] Danach wird es sog. qualifizierten Einrichtungen[74] unter anderem auch im Datenschutzrecht möglich sein, Verbandsklagen für betroffene Verbraucher zu erheben. Dies dürfte vor allem der Durchsetzung von Schadensersatzklagen, in denen eine Vielzahl von Personen in gleich gelagerten Fällen betroffen sind, was vor allem im Beschäftigungskontext und bei Kundendaten regelmäßig der Fall ist, deutlich vereinfachen.

Abhängig von der konkreten Umsetzung in das nationale Recht könnte diese Richtlinie die Rechtsdurchsetzung (u. a. in Deutschland) auch deshalb erleichtern, weil sie eine Möglichkeit vorsieht, die Offenlegung von Beweismitteln von dem Beklagten oder einem Dritten zu beantragen.[75]

Nachdem qualifizierte Einrichtungen in Fällen, in denen eine Beeinträchtigung für Verbraucher aus verschiedenen Mitgliedstaaten besteht oder droht, nach der Richtlinie auch in einem anderen Mitgliedstaat klagen können,[76] droht für Unternehmen das Risiko, dass in solchen Fällen der Gerichtsort gewählt wird, in dem die größten Erfolgschancen und womöglich höchsten Schadensersatzsummen zu erwarten sind.

Aber auch jenseits dieser zukünftigen Entwicklung bestehen bereits jetzt unterschiedliche Möglichkeiten, welche die gerichtliche Durchsetzung von Schadensersatzansprüchen erleichtern. Ihnen wird durch die stark abgesenkten Hürden des BAG für die Geltendmachung von Schadensersatzansprüchen (s. dazu oben unter III. 1.) zusätzlicher Vorschub geleistet. So wurde etwa vom Landgericht Essen angenommen, dass Schadensersatzansprüche gemäß Art. 82 Abs. 1 DS-GVO abgetreten werden können und nicht zwingend von der betroffenen Person selbst eingeklagt werden müssen.[77] Darüber hinaus gibt es mittlerweile auch Anbieter, wie die Europäische Gesellschaft für Datenschutz, die speziell darauf ausgerichtet sind, Betroffene bei der Geltendmachung derartiger Schadensersatzansprüche zu unterstützen.[78] Diese Möglichkeiten können die Hürden für das Einklagen solcher Ansprüche deutlich absenken und zu einem Ansteigen der Häufigkeit von deren Geltendmachung nicht unwesentlich beitragen.

d) Durchsetzung der Anforderungen des Schrems II-Urteils

Die Durchsetzung der Anforderungen des Schrems II-Urteils wird aller Voraussicht nach auch weiterhin die Gerichte beschäftigen. Denkbar erscheinen in diesem Zusammenhang unterschiedlichste private Durchsetzungsinstrumente: von Auskunftsansprüchen, über immaterielle Schadensersatzansprüche wegen einer ungerechtfertigten Drittlandübermittlung, bis hin zu einer Geltendmachung eines Unterlassungsanspruchs gegen Datenübermittlungen in die USA, wie etwa bei der Verwendung von US-Dienstleistern im Cloud-Bereich.

V. Fazit und Ausblick

Die Durchsetzung des Datenschutzrechts nimmt weiter Fahrt auf. Datenschutzbehörden im EWR sind mehr und mehr bereit, Bußgelder in beträchtlicher Höhe zu verhängen und zusehends darauf bedacht, ihre Bußgeldpraxis europaweit zu vereinheitlichen. Auf Basis von bereits verhängten Bußgeldern und aktuellen Entwicklungen zeichnet sich ab, in welchen Bereichen des Datenschutzrechts Unternehmen insoweit insbesondere erhebliche Risiken drohen. Gerade im Hinblick auf die Umsetzung der Vorgaben des Schrems II-Urteils vom 16.7.2020 ist davon auszugehen, dass die von den Behörden faktisch gewährte Schonfrist nunmehr endgültig endet. Gleichzeitig stehen betroffenen Personen immer mehr Möglichkeiten zur Verfügung, um auf dem privaten Klageweg gegen Unternehmen vorzugehen. Im Übrigen könnten anstehende Entscheidungen des EuGH richtungsweisenden Einfluss auf die Zukunft der privaten Rechtsdurchsetzung im Bereich des Datenschutzrechts haben. Unter Betrachtung der derzeitigen Entwicklungen ist in jedem Fall von einer weiteren Verschärfung der Rechtsdurchsetzung im Datenschutzrecht sowohl von behördlicher als auch von privater Seite auszugehen. Wie die Vergangenheit gezeigt hat, können Unternehmen aber durch proaktive Maßnahmen – gerade auch in den in diesem Aufsatz erläuterten Schwerpunktbereichen des materiellen Datenschutzrechts – diesbezügliche Risiken signifikant und nachhaltig minimieren.

Dr. Daniel Ashkar ist Senior Associate der IP/IT- und Datenschutzpraxisgruppe der internationalen Wirtschaftssozietät Orrick, Herrington & Sutcliffe LLP in München.

Tobias Lantwin ist Wissenschaftlicher Mitarbeiter der IP/IT- und Datenschutzpraxisgruppe der internationalen Wirtschaftssozietät Orrick, Herrington & Sutcliffe LLP in Düsseldorf.

Dr. Christian Schröder ist Partner und Leiter der IP/IT- und Datenschutzpraxisgruppe der internationalen Wirtschaftssozietät Orrick, Herrington & Sutcliffe LLP in Düsseldorf.

70 Vgl. *Leibold/Laoutoumai*, ZD-Aktuell 2021, 05583.
71 Wegen der fehlenden Glaubhaftmachung eines Anordnungsgrundes hat etwa der Hessische VGH eine einstweilige Untersagungsanordnung einer Datenübermittlung des VG Wiesbaden wieder aufgehoben: Hessischer VGH, 17.1.2022 – 10 B 2486/21, BeckRS 2022, 790.
72 RL (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25.11.2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der RL 2009/22/EG, ABl. L 409/1, 4.12.2020 („Verbandsklage-Richtlinie").
73 Art. 24 Abs. 1 der Verbandsklage-Richtlinie.
74 Nach Art. 3 Nr. 4 der Verbandsklage-Richtlinie ist das „jede Organisation oder öffentliche Stelle, welche die Verbraucherinteressen vertritt und die von einem Mitgliedstaat als für die Erhebung von Verbandsklagen gemäß dieser Richtlinie qualifiziert benannt wurde". Gemäß Art. 4 Abs. 3 der der Verbandsklage-Richtlinie müssen qualifizierte Einrichtungen u. a. „nachweislich zwölf Monate zum Schutz von Verbraucherinteressen öffentlich tätig gewesen" sein und dürfen „keinen Erwerbszweck" verfolgen.
75 Art. 18 der Verbandsklage-Richtlinie.
76 Art. 6 der Verbandsklage-Richtlinie.
77 LG Essen, 23.9.2021 – 6 O 190/21, ZD 2022, 50, 50 f.
78 Vgl. Europäische Gesellschaft für Datenschutz, unter www.eugd.org/ (Abruf: 8.3.2022).