ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

EDITORIAL

4/2021

Data Privacy Litigation und kein Ende?

Lesedauer: 11 Minuten

In den USA bezeichnet der Begriff „Data Privacy Litigation" Gerichtsverfahren, in denen datenschutzrechtliche Fragestellungen eine entscheidende Rolle spielen. Auch in Deutschland und den anderen Mitgliedstaaten der EU nimmt die Anzahl solcher Verfahren stetig zu. Im Mittelpunkt stehen hier vor allem die besonderen haftungsrechtlichen Regelungen der DS-GVO. Mittlerweile gibt es mit den Beschlüssen des *BVerfG* zum Recht auf Vergessen (ZD 2020, 100 m. Anm. *Petri* und Anm. *Gräbig* und ZD 2020, 109 m. Anm. *Gräbig*) und dem Urteil des *EuGH* zur Unwirksamkeit des Privacy Shield (ZD 2020, 511 m. Anm. *Moos/Rothkegel*) bereits höchstrichterliche Rechtsprechung, die erhebliche Auswirkungen auf die Praxis im Datenschutz hat. In der Praxis dominieren derzeit Klagen auf immateriellen Schadensersatz nach Art. 82 DS-GVO und Bußgelder nach Art. 83 DS-GVO das Geschehen.

Einfluss der Digitalisierung auf den Datenschutz

Die Bedeutung des Datenschutzes steigt auf Grund der sich schnell weiterentwickelnden technischen Möglichkeiten, personenbezogene Daten zu verarbeiten. Dementsprechend werden auch immer mehr Lebensbereiche – und damit auch Gerichtsverfahren – durch den Datenschutz geprägt. Denn sowohl soziale Medien, KI, moderne Formen der Werbung und viele andere Phänomene bzw. Geschäftsbereiche beruhen immer mehr auf der vielfältigen und effektiven Verarbeitung personenbezogener Daten.

Tim Wybitul
ist Partner und Fachanwalt für Arbeitsrecht bei Latham & Watkins in Frankfurt/M. sowie Mitherausgeber der ZD.

Gerichtsverfahren wegen Datenschutzverletzungen

Entsprechend den zunehmenden technischen und wirtschaftlichen Möglichkeiten werden die Vorgaben des europäischen und sonstigen Datenschutzrechts immer vielschichtiger. So ist z.B. die schnelle und effektive Reaktion auf Datenschutzverletzungen oder sonstige „Cyber Security Incidents" mittlerweile durchaus komplex. Neben der IT-forensischen Aufarbeitung eines solchen Vorfalls sowie der Erfüllung von Melde- und Informationspflichten nach Art. 33, 34 DS-GVO müssen Unternehmen viele weitere Punkte berücksichtigen. Sie müssen das Risiko späterer Bußgelder und Klagen auf immateriellen Schadensersatz abschätzen und nach Möglichkeit verringern. Für beide Aspekte ist es oftmals sehr wichtig, einen guten und engen Kontakt zu der zuständigen Datenschutzaufsichtsbehörde zu halten. Daneben können nach Datenschutzverletzungen sowohl das *BSI* als auch die spezialisierten Cybereinheiten der jeweiligen Kriminalpolizei oder Fachbehörden wie etwa die *BaFin* auf nationaler Ebene eine wichtige Rolle spielen. Bei grenzüberschreitenden Vorgängen sind zudem ggf. viele andere nationale und supranationale Behörden einzubinden. Dabei ist zu berücksichtigen, dass sich die jeweiligen Fachbehörden oftmals untereinander austauschen – mittlerweile geschieht dies oft auch auf internationalem Niveau, z.B. im *EDSA*. Insgesamt können also je nach Fall verschiedenste Akteure entscheidenden Einfluss auf die rechtliche Aufarbeitung eines Datenschutzverstoßes haben.

Neben den o.g. Themen müssen Unternehmen in einer solchen Situation oft auch die Vertragsbeziehungen zu Geschäftspartnern im Blick behalten. Je nach Branche und Art des jeweiligen Vorgangs kann ein Datenschutzvorfall umfassende vertragliche Informationspflichten, aber auch Kündigungsrechte von Geschäftspartnern nach sich ziehen. Insofern ist neben den rein rechtlichen Gesichtspunkten nicht selten auch eine strukturierte Informationspolitik oder sogar PR-Arbeit geboten. Dabei sollte auch die Information der eigenen Mitarbeiter nicht vernachlässigt werden – die verständlicherweise von wichtigen geschäftlichen Vorgängen nicht aus der Presse erfahren möchten.

Insbesondere in Bezug auf spätere Nachfragen oder Bußgelder von Datenschutzbehörden und (ggf. massenhafte) Klagen auf immateriellen Schadensersatz nach Art. 82 DS-GVO entscheiden oft die ersten 24 Stunden nach der Aufdeckung des Vorgangs über den Erfolg oder Misserfolg späterer Data Privacy Litigation.

BVerfG zu Bagatellschäden bei Schmerzensgeldern nach Art. 82 DS-GVO

Derzeit müssen deutsche Gerichte über eine Vielzahl von Klagen auf immateriellen Schadensersatz wegen tatsächlichen oder behaupteten Datenschutzverstößen entscheiden. Dabei ist in solchen Verfahren oftmals streitig, ob der Kläger oder die Beklagte beweisen müssen, dass es zu einem Verstoß gegen die DS-GVO gekommen ist. Ähnliches gilt für die Frage nach der haftungsbegründenden Kausalität zwischen vorgetragenem Verstoß und dem möglichen immateriellen Schaden. Hier sind eine ganze Reihe von relevanten materiell-rechtlichen und prozessualen Fragen bislang höchstrichterlich ungeklärt.

Diese Ausgangslage hat das *BVerfG* (B. v. 14.1.2021 – 1 BvR 2853/19) kürzlich zum Anlass genommen, um an mögliche bestehende Vorlagepflichten zum *EuGH* zu erinnern. In dem konkreten Fall hatte ein Unternehmen einem Rechtsanwalt eine ungewollte Werbe-E-Mail zugeschickt. Der Anwalt klagte vor dem *AG Goslar* u.a. auf Unterlassung und immateriellen Schadensersatz nach Art. 82 DS-GVO. Das *Gericht* gab dem Unterlassungsanspruch statt und wies den geltend gemachten Schadenser-

satzanspruch mit der Begründung ab, es handele sich um einen Bagatellschaden. Damit lag das *AG Goslar* auf der Linie einer ganzen Reihe von Entscheidungen, die bei zu ersetzendem immateriellen Schadensersatz eine gewisse Erheblichkeitsschwelle forderten. Eine Berufung hatte das *AG Goslar* nicht gesondert zugelassen. Damit war es in Deutschland das als letzte Instanz tätige Gericht. Nach einer Anhörungsrüge wurde dann Verfassungsbeschwerde erhoben.

Das *BVerfG* gab der Beschwerde statt. Es entschied, dass das *AG Goslar* als letztinstanzlich tätiges deutsches Gericht die Frage einer möglichen Erheblichkeitsschwelle bei materiellem Schadensersatz dem *EuGH* hätte vorlegen müssen, da es die Entscheidung allein auf diesen Gesichtspunkt stützte. Diese Entscheidung dürfte weitreichende Konsequenzen haben.

Zum einen dürften Kläger, Verbraucheranwälte, Prozessfinanzierer und sonstige auf die massenhafte Geltendmachung derartiger Ansprüche spezialisierte Anbieter die Entscheidung zum Anlass nehmen, weitere Klagen nach Art. 82 DS-GVO vor deutsche Gerichte zu bringen. Zum anderen wird damit wohl bald der *EuGH* eine zentrale Frage der Auslegung von Art. 82 DS-GVO klären. Gegen einen Verzicht auf die Erheblichkeitsschwelle sprechen neben einer gewissen Missbrauchsgefahr auch Erwägungsgrund 85 S. 1 und 146 S. 6 DS-GVO, die „erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person" sowie einen „erlittenen Schaden" vorsehen. Andererseits hat der *EuGH* in vielen Entscheidungen der vergangenen Jahre einen oft datenschutzfreundlichen oder verbraucherfreundlichen Kurs an den Tag gelegt. Sollte der *EuGH* der Auffassung sein, dass selbst eine einzige unverlangt zugesandte Werbe-E-Mail einen ersatzfähigen immateriellen Schaden darstellt, würde dies nicht nur das deutsche Schadensrecht ziemlich auf den Kopf stellen.

Die Königsdisziplin: Datenschutz-Bußgelder gegen Unternehmen

Nach wie vor sorgen sich Unternehmen bei der Verarbeitung personenbezogener Daten oftmals um mögliche Bußgelder. Der mögliche Bußgeldrahmen von bis zu 20 Mio. EUR oder von bis zu 4% des Vorjahresumsatzes ermöglicht empfindliche Sanktionen. Die deutschen Datenschutzbehörden machen von ihren mit der Geltung der DS-GVO dazu gewonnenen Bußgeld-Kompetenzen durchaus Gebrauch. Dies zeigt sich z.B. an einem rechtskräftigen Bußgeld i.H.v. 34,5 Mio. EUR, das die *Hamburger Datenschutzbehörde* verhängt hatte. Diese Entscheidung war aber kein Einzelfall. So haben mittlerweile auch die Landesdatenschutzbehörden in Berlin, Baden-Württemberg (ebenfalls rechtskräftig), Niedersachsen sowie der *BfDI* „Millionenbußgelder" verhängt.

Das *LG Bonn* reduzierte zwar ein vom *BfDI* verhängtes Bußgeld von 9,5 Mio. EUR auf „nur" 900.000,– EUR (ZD 2021, 154 m. Anm. *v. d. Bussche*). Allerdings wurde bei dem Vorfall lediglich eine einzige Telefonnummer offengelegt. Vor diesem Hintergrund ist es nachvollziehbar, dass der *BfDI* die (mittlerweile rechtskräftige) Entscheidung als Erfolg bewertet. Dies liegt aber auch an einem anderen wichtigen Aspekt des Urteils. Denn das *LG Bonn* folgte der Rechtsauffassung des *BfDI*, der das Bußgeld direkt gegen das betroffene Unternehmen als Täter bzw. bußgeldrechtlich „Betroffene" verhängte. Diese Vorgehensweise ergebe sich aus einem Verweis aus Art. 83 DS-GVO und Erwägungsgrund 150 S. 3 DS-GVO, die eine direkte Anwendbarkeit der Mechanismen des EU-Kartellrechts vorsähen, sog. Funktionsträgerprinzip.

Die direkte Bebußung von Unternehmen ist im deutschen Bußgeldrecht nicht vorgesehen. Zwar sind Unternehmen immer wieder als Nebenbeteiligte Adressaten von Bußgeldern, die teilweise ebenfalls Millionenhöhe erreichen. Hierfür ist aber eine nachgewiesene Anknüpfungstat einer natürlichen Person erforderlich. Eine solche Zurechnung von vorwerfbarem Verhalten setzt nach § 30 OWiG eine Pflichtverletzung einer Leitungsperson voraus. In der Praxis liegt diese Pflichtverletzung einer natürlichen Person oftmals in einer Aufsichtspflichtverletzung des Vorstands oder anderer Leitungsgremien nach § 130 OWiG. Haben diese nicht die erforderlichen Maßnahmen ergriffen, um die unternehmensbezogene Pflichtverletzung zu verhindern oder zumindest erheblich zu erschweren, kann der Gesetzesverstoß über § 30 OWiG dem Unternehmen zugerechnet werden. Dabei erlaubt das deutsche Bußgeldrecht unter gewissen Umständen auch den Erlass eines selbstständigen Bescheids gegen Unternehmen nach § 30 Abs. 4 OWiG. Auch hier muss aber eine vorwerfbare Ordnungswidrigkeit oder Straftat eines Inhabers bzw. einer Leitungsperson festgestellt werden.

Die Frage, ob man ein Unternehmen wegen eines schuldhaften DS-GVO-Verstoßes direkt oder i.R.d. deutschen Bußgeldrechts in Anspruch nimmt, hat in der Praxis erhebliche Folgen. Folgt man der Rechtsauffassung des *LG Bonn*, drohen Unternehmen auch dann Bußgelder, wenn sie die nach § 130 OWiG gebotenen Aufsichtsmaßnahmen zur Einhaltung der DS-GVO umgesetzt haben. Zwar sollen Verstöße von Mitarbeitern dann nicht dem Unternehmen zuzurechnen sein, wenn sie die Mittel und Zwecke der unerlaubten Datenverarbeitung selbst festgelegt haben. Doch der Nachweis eines solchen sog. „Mitarbeiterexzesses" dürfte dem verfolgten Unternehmen in der Praxis nur selten oder gar nicht gelingen. Das könnte die Unschuldsvermutung teilweise aushebeln. Ein weiterer gravierender Unterschied liegt auf der Beweisebene. Folgt man der Ansicht des *LG Bonn*, müssten die Datenschutzbehörden nur nachweisen, dass es „aus dem Unternehmen heraus" zu DS-GVO-Verstößen gekommen ist. Weder müssten sie eine datenschutzrechtliche Pflichtverletzung als Vortat i.S.d. § 130 OWiG noch eine Aufsichtspflichtverletzung des Vorstands nachweisen.

Dabei sprechen gute Gründe gegen die Annahme einer unmittelbaren bußgeldrechtlichen Haftung des Unternehmens. Denn der Wortlaut von Art. 83 DS-GVO ordnet eine dem Kartellrecht nachgebildete Haftung des Funktionsträgers gerade nicht an. Lediglich Erwägungsgrund 150 S. 3 DS-GVO verweist in Bezug auf den Bußgeldrahmen – aber nicht den Bußgeldadressaten – auf das Kartellrecht. Eine „Erfolgshaftung sui generis" bei DS-GVO-Bußgeldern wird hier nicht angeordnet – sie wäre auch weder mit dem Gesetzlichkeitsprinzip noch dem Schuldprinzip in Einklang zu bringen. Eine mögliche Haftung des Funktionsträgers wirft aber auch prozessuale Probleme auf. Denn nach § 66 Abs. 1 OWiG muss ein Bußgeldbescheid u.a. Tat, Täter, Tatort und Tatzeit hinreichend konkret bezeichnen. Gelingt dies der Behörde nicht, ist der Bescheid unwirksam. Erst kürzlich hatte das *LG Berlin* (B. v. 18.2.2021 – 526 OWi LG 212 Js – OWi 1/20) einen direkt gegen ein Unternehmen verhängten Bußgeldbescheid als unwirksam bewertet. Diese Entscheidung ist nicht rechtskräftig.

Wie geht es weiter?

Data Privacy Litigation ist im europäischen Raum angekommen und nimmt für Wirtschaftsunternehmen eine immer wichtigere Rolle ein. Es dürfte dabei auch feststehen, dass die DS-GVO und ihre Auslegung in den kommenden Jahren für viel Arbeit bei deutschen und anderen europäischen Gerichten bis hin zum *EuGH* sorgen werden. Bis die wesentlichsten Fragen des aktuellen europäischen Datenschutzrechts geklärt sind, dürfte es noch Jahre dauern und etliche Gerichtsverfahren erfordern.

■ Der Verfasser ist Teil des Verteidigerteams, das das betroffene Unternehmen in dem o.g Verfahren vor dem LG Berlin verteidigte.