ZEITSCHRIFT FÜR DATENSCHUTZ
EDITORIAL
ZD
1/2022

Gerichte und Behörden geben Vollgas bei Bußgeldern und Schadensersatz

Lesedauer: 8 Minuten

Europäische Gerichte und Behörden sanktionieren Verstöße gegen die Vorgaben des Datenschutzes immer härter. Das betrifft zum einen Bußgelder nach Art. 83 DS-GVO. Europäische Aufsichtsbehörden verhängen dreistellige Millionenbußgelder. Der *Europäische Datenschutzausschuss (EDSA)* will bald sein EU-weit geltendes Bußgeldmodell vorstellen, das zu noch höheren Bußgeldern als nach dem Bußgeldkonzept der *DSK* führen könnte. Zum anderen drohen Unternehmen auch wegen Schadensersatzforderungen nach Art. 82 DS-GVO hohe Risiken. Immer mehr ordentliche Zivilgerichte sprechen Klägern Schmerzensgeld wegen Datenschutzverletzungen zu. Das *BAG* (ZD 2022, 56 mAnm *Leibold* – in diesem Heft) geht in einem aktuellen Vorlagebeschluss zu Art. 82 DS-GVO offenbar sogar von einer Art verschuldensunabhängiger Gefährdungshaftung aus und verzichtet auf die Geltendmachung eines eingetretenen Schadens. Es vertritt dabei auch weitere Positionen, die es Klägern künftig massiv erleichtern könnten, vor Gericht erfolgreich Forderungen nach immateriellem Schadensersatz durchzusetzen.

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

EU-Behörden verhängen dreistellige Millionenbußgelder

Hohe Bußgelder wegen Datenschutzverstößen sind mittlerweile Realität. Nachdem die französische Aufsichtsbehörde *CNIL* bereits recht bald nach Geltung der DS-GVO ein Bußgeld über 50 Mio. EUR verhängte, markiert die *hamburgische Behörde* mit gut 35 Mio. EUR den bisherigen Höchstwert für deutsche Aufsichtsbehörden. Doch das war offenbar erst der Anfang. Kürzlich hat die *irische Behörde* ein Bußgeld iHv 225 Mio. EUR verhängt. Sogar noch deutlich höher fiel ein von der *luxemburgischen Behörde* verhängtes Bußgeld iHv 746 Mio. EUR aus. Beide Bußgelder sind nicht rechtskräftig. In beiden Fällen ging der Verhängung des Bußgelds eine Abstimmung auf EU-Ebene voraus, die zu einer massiven Erhöhung der zunächst von der zuständigen federführenden Behörde vorgeschlagenen Beträge führte. In Bezug auf derzeit laufende Verfahren bewahren Behörden und betroffene Unternehmen aus gutem Grund Stillschweigen. Bereits jetzt zeigt sich klar, dass Bußgelder nach Art. 83 DS-GVO für Unternehmen mittlerweile ein sehr konkretes Risiko darstellen.

Neues EDSA-Modell zur Festlegung einheitlicher und hoher Bußgelder

Von Behördenvertretern hört man, dass damit gerechnet wird, dass der *EDSA* bald seinen seit geraumer Zeit diskutierten Beschluss über ein EU-weit verbindliches Modell zur Bestimmung von DS-GVO-Bußgeldern verabschiedet. Dieser soll womöglich zu noch höheren Bußgeldern als nach dem Bußgeldkonzept der *DSK* führen. Vor allem hätte ein Bußgeldmodell des *EDSA* voraussichtlich eine nicht unerhebliche Bindungswirkung und würde so den Entscheidungsspielraum nationaler Behörden bei der Verhängung der Geldbuße nach Art. 83 DS-GVO erheblich einschränken.

Verteidigung gegen DS-GVO-Bußgelder

Bei der Verhängung derart hoher Sanktionen ist es nicht überraschend, dass sich Unternehmen vor Gericht – teilweise auch durchaus erfolgreich – gegen solche Bußgelder wehren. So hat etwa die *große Strafkammer des LG Berlin* (ZD 2021, 270) einem Einspruch gegen einen Bescheid über ein zweistelliges Millionenbußgeld stattgegeben. Die *Kammer* hat das Bußgeldverfahren wegen gravierender Verfahrensmängel nach § 206a StPO iVm §§ 46, 71 OWiG eingestellt. Über das von der Staatsanwaltschaft auf Bitte der Behörde eingelegte Rechtsmittel wird das *KG* entscheiden. Das Verfahren zeigt deutlich, dass es bei der Verteidigung gegen Bußgelder nach Art. 83 DS-GVO wichtig ist, Bußgeldentscheidungen nicht nur in materieller Hinsicht, sondern auch in Bezug auf mögliche prozessuale Fehler genau zu prüfen (vgl. *Wybitul/Venn*, ZD 2021, 343). Die deutschen Behörden verfolgen derzeit den Ansatz, Bußgelder gegen Unternehmen ohne konkrete Feststellungen zum vorwerfbaren Verhalten einzelner Personen im Unternehmen zu verhängen. Allein dieses Vorgehen gibt schon Anlass zur gerichtlichen Überprüfung entsprechender Bußgelder. Darüber hinaus lohnt es sich erfahrungsgemäß durchaus, Bußgeldentscheidungen gründlich auf mögliche prozessuale Fehler zu prüfen. Gerade bei Fragen der Akteneinsicht und dem Recht auf Gehör passieren schnell Fehler. Zudem verhängen Datenschutzbehörden nicht selten auch Bußgeldentscheidungen auf der Basis einer materiell-rechtlichen Auslegung der DS-GVO, über die es sich durchaus zu streiten lohnt. Manchmal kann es leichter sein, eine Strafkammer von einer praxisgerechten Interpretation des Datenschutzrechts zu überzeugen als die zuständige Datenschutzbehörde.

Datenschutzverstöße als Geschäftsmodell

Aber nicht nur in Bezug auf hohe Bußgelder drohen Unternehmen beim Datenschutz Risiken. Vielmehr können auch mög-

liche Schadensersatzansprüche ganze Geschäftsmodelle erheblich gefährden. Denn gerade bei Datenverarbeitungen oder Vorfällen, die eine Vielzahl von potenziellen Klägern betreffen, müssen Unternehmen auch an mögliche Massenklagen auf immateriellen Schadensersatz nach Art. 82 DS-GVO denken. Einige Unternehmen haben hieraus bereits ein Geschäftsmodell gemacht. Kommt es zu Presseberichten über mögliche Verstöße gegen die Vorgaben des Datenschutzes, so schalten sie schnell entsprechende Angebotsseiten im Internet, auf denen sich betroffene Personen registrieren können, um ihre Ansprüche geltend zu machen. Auch in sozialen Medien werben sie um potenzielle Kläger. Im Erfolgsfalle behalten Sie einen Teil des eingeklagten Schadensersatzes als Provision ein. Andere Anbieter gehen sogar noch direkter vor. Sie lassen sich Schadensersatzansprüche nach Art. 82 DS-GVO für die Zahlung einer kleinen Summe abtreten – und machen dann Ansprüche gegen das betroffene Unternehmen gebündelt geltend.

Typische Anlasstatbestände für solche Forderungen sind etwa Datenpannen oder andere Cybersecurity-Vorfälle. Die Forderungssteller tragen in entsprechenden zivilrechtlichen Verfahren oftmals vor, die mit dem Vorfall verbundene Offenlegung von Daten sei nur dadurch ermöglicht worden, dass das Unternehmen etwa die Anforderungen der Datensicherheit nach Art. 32 DS-GVO nicht ordnungsgemäß umgesetzt habe. Aber auch Presseberichte über sonstige mögliche Datenschutzverstöße, die eine Vielzahl von Personen betreffen, sind für diese Anbieter attraktiv.

Rechtsprechungstendenz zu Schadensersatzforderungen

Zunächst waren vor allem Arbeitsgerichte gewillt, Klägern immateriellen Schadensersatz nach Art. 82 DS-GVO zuzusprechen. Das *ArbG Düsseldorf* (ZD 2020, 649) sprach einem ehemaligen Arbeitnehmer in einer vielbeachteten Entscheidung 5.000 EUR Schadensersatz wegen eines verspätet und intransparent beantworteten Auskunftsersuchens nach Art. 15 DS-GVO zu. Diese Entscheidung blieb kein Einzelfall. Mittlerweile verurteilen sogar Landesarbeitsgerichte beklagte Unternehmen zur Zahlung von Schadensersatz.

Das *LAG Hamm* (ZD 2021, 710) sprach z.B. kürzlich einem Kläger 1.000 EUR wegen der verspäteten Beantwortung eines Auskunftsersuchens zu. In einer ähnlichen Fallkonstellation verurteilte das *LAG Niedersachsen* (ZD 2022, 61 – in diesem Heft) einen Arbeitgeber sogar zur Zahlung von 1.250 EUR. Aber auch ordentliche Gerichte verurteilen beklagte Unternehmen immer öfter zur Zahlung von immateriellem Schadensersatz nach Art. 82 DS-GVO. So sprach etwa auch das *LG Mainz* (U. v. 12.11.2021 – 3 O 12/20) einem Kläger wegen der Verarbeitung seiner personenbezogenen Daten 5.000 EUR zu.

Daneben gibt es auch eine Vielzahl von Entscheidungen, die sich klar gegen überbordende Möglichkeiten zur Geltendmachung von Datenschutz-Schadensersatz positionieren. Die Meinungsvielfalt in der aktuellen deutschen Rechtsprechung ist beeindruckend. So hat z.B. der *9. Zivilsenat des OLG Stuttgart* (ZD 2021, 375) klar – und nach Auffassung des *Verfassers* sehr überzeugend – geurteilt, dass weder aus Art. 82 DS-GVO noch aus der Rechenschaftspflicht nach Art. 5 Abs. 2, 24 Abs. 1 DS-GVO eine Umkehr oder Erleichterung der Beweislast folge. Nur wenig später entschied der *12. Zivilsenat* desselben Gerichts, dass Beklagte in Verfahren wegen Ansprüchen nach Art. 82 DS-GVO auf Grund der datenschutzrechtlichen Rechenschaftspflicht nicht nur für die Rechtmäßigkeit der Datenerhebung verantwortlich seien, sondern die Einhaltung der DS-GVO auch nachweisen müssten. Im Ergebnis habe daher der Beklagte nachzuweisen, dass er seine Datenverarbeitungen rechtmäßig betreibe. Gelinge ihm dies nicht, sei von einem Verstoß iSv Art. 82 Abs. 1 DS-GVO auszugehen. Mittlerweile ist auch der *EuGH* mit der Frage befasst, ob in solchen Verfahren Kläger oder Beklagte DS-GVO-Verstoß, Schaden und Kausalität beweisen müssen (Rs. C-340/21).

In der Praxis wird die Frage der Beweislast künftig wohl über den Ausgang der allermeisten Verfahren um immateriellen Schadensersatz wegen DS-GVO-Verstößen entscheiden (vgl. die Übersichten bei *Leibold*, ZD 2022, 18 – in diesem Heft).

Ein Paukenschlag des BAG hilft Klägern

Mittlerweile hat sich auch das *BAG* umfassend mit der Auslegung von Art. 82 DS-GVO befasst. In einem Vorlagebeschluss v. 26.8.2021 (ZD 2022, 56 mAnm *Leibold* – in diesem Heft) hat es dem *EuGH* einige für die Praxis überaus wichtige Fragen vorgelegt. In der Entscheidung trifft der *8. Senat* einige überraschende Aussagen, die der *EuGH* hoffentlich korrigieren wird. Das *BAG* geht von einer sehr weiten Auslegung von Art. 82 DS-GVO aus.

Bereits der bloße Verstoß gegen die Vorgaben der DS-GVO solle einen ersatzfähigen immateriellen Schaden begründen. Das *BAG* verzichtet damit vollständig auf den Nachweis eines konkreten Schadens des Klägers. Bereits der Verstoß selbst solle einen Schaden darstellen. Zudem setze die Haftung nach Art. 82 DS-GVO auch kein schuldhaftes Handeln des Verantwortlichen voraus. Der *8. Senat* stellt somit schon auf Tatbestandsseite ungewöhnlich niedrige Anforderungen an die Geltendmachung von Schadensersatz wegen Datenschutzverstößen. Im Ergebnis propagiert er letztlich eine Art verschuldensunabhängiger Gefährdungshaftung beim Datenschutz.

Aber auch in Bezug auf die Rechtsfolgen trifft der *8. Senat* für Unternehmen sehr problematische Aussagen. Aus Sicht des *BAG* solle DS-GVO-Schadensersatz abschreckend wirken. Der *8. Senat* verweist zur Begründung auf Erwägungsgrund 146 DS-GVO, wonach betroffene Personen vollständig und wirksam entschädigt werden sollen. Er stellt die Vermutung auf, dass Gerichte bei der Bemessung von immateriellen Schadensersatzansprüchen general- und spezialpräventive Aspekte berücksichtigen sollten.

Wie geht es weiter?

Es bleibt zu hoffen, dass sich der *EuGH* sowohl bei Bußgeldern nach Art. 83 DS-GVO als auch bei Schadensersatz nach Art. 82 DS-GVO für eine maßvolle Anwendung des Datenschutzrechts entscheidet, anstatt einer übermäßig extensiven und strengen Auslegung der DS-GVO den Weg zu ebnen. Sollte der *EuGH* hingegen etwa die extensive Auslegung des *8. Senats des BAG* bestätigen, drohen Unternehmen weitreichende Haftungsrisiken bis hin zu DS-GVO-Massenklagen.

HEIKO RICHTER

2022: Ankunft im Post-Open-Data-Zeitalter

Datenwirtschaftsrecht II: Die Zukunft der Regulierung von Daten des öffentlichen Sektors

Open Data
Data Governance Act
Forschungsdaten
Informationszugang
Innovation

■ Der als EU-Verordnung konzipierte Data Governance Act (DGA) erweitert Open-Data-Ansätze um die zweckgebundene Prüfung und Erlaubnis der Weiterverwendung von Daten der öffentlichen Hand. Das verändert den Charakter der Datenregulierung im Ganzen. Die Ankunft im Post-Open-Data-Zeitalter bildet einen willkommenen Anlass, um die damit einhergehenden Herausforderungen der nächsten Jahre für Gesetzgebung, Praxis und Wissenschaft zu erörtern.

■ The Data Governance Act (DGA), drafted as an EU regulation, expands upon open-data approaches by including the purpose-based review and permission of the re-use of public sector data. This changes the character of data regulation as a whole. The arrival in the post-open-data era is a welcome opportunity to discuss the accompanying challenges for legislation, practice and academia in the coming years.
Lesedauer: 22 Minuten

I. Problemstellung und Hintergrund

2022 wird aller Voraussicht nach ein Kernstück der EU-Datenregulierung in Kraft treten: der Data Governance Act (DGA).[1] Dieser als Verordnung konzipierte Rechtsakt gründet auf Art. 114 AEUV, was unmittelbar mit seiner Zielsetzung zusammenhängt: Durch Rechtsangleichung soll der DGA gerade den Akteuren der Datenwirtschaft helfen, „sich die Größe des Binnenmarktes zunutze zu machen".[2] Es geht also darum, das datenbasierte Wohlstandspotenzial in der EU freizusetzen.[3] Der DGA ist ein Baustein zur Umsetzung der Datenstrategie der *Kommission* von 2020.[4] Er regelt die Bereitstellung bestimmter Daten des öffentlichen Sektors, Dienste für die gemeinsame Datennutzung sowie die Nutzung von Daten aus altruistischen Gründen.[5] Dieser Beitrag konzentriert sich auf die Regelungen über bestimmte Daten des öffentlichen Sektors. Die Nutzung dieser Daten birgt hohe Wohlfahrtsgewinne – sei es im Bereich der medizinischen Forschung, der sozialen Innovation oder des maschinellen Lernens im Allgemeinen.[6]

Für den rechtlichen Ordnungsrahmen von Informationen des öffentlichen Sektors war bisher das Open-Data-Postulat leitend. Hiernach soll die öffentliche Hand die zumeist steuerfinanzierten Informationen jedermann möglichst kostenfrei bereitstellen und Nutzer*innen keine Verwendungsbeschränkungen auferlegen.[7] Der Open-Data-Gedanke durchdringt das zentrale Regelwerk für Informationen der öffentlichen Hand: die Public-Sector-Information-Richtlinie (PSI-RL).[8] Diese regelt die Bedingungen der Nutzung von uneingeschränkt zugänglichen Informationen öffentlicher Stellen und – neuerdings auch – öffentlicher Unternehmen. Der EU-Gesetzgeber hat die PSI-RL im Jahr 2003 erlassen und seitdem ihren Anwendungsbereich kontinuierlich erweitert,[9] um datengetriebene Innovationstätigkeit privater Akteure zu fördern. In Deutschland wurde sie im Informationsweiterverwendungsgesetz (IWG) und nach der letzten Änderung der PSI-RL von 2019 nunmehr im Datennutzungsgesetz (DNG) v. 16.7.2021 weitgehend 1:1 umgesetzt.[10] Neu ist insbesondere die Bereitstellung hochwertiger Datensätze nach Open-Data-Prinzipien, § 9 DNG iVm § 3 Nr. 9 DNG. Diese sollen in einem Durchführungsakt der *Kommission* definiert werden, dessen Erlass allerdings noch für das Jahr 2022 aussteht.[11] Während die PSI-RL bzw. das DNG allein die Weiterverwendung bzw. Nutzung der Daten betreffen, regeln hingegen andere Rechtsakte den Zugang zu bzw. die Bereitstellung von Daten der öffentlichen Hand, so etwa die ebenfalls 2021 reformierte Open-Data-Regelung des Bundes (§ 12a EGovG)[12] ebenso wie verschiedene Landesregelungen.[13]

Der DGA verkörpert nun aber einen Paradigmenwechsel. Er betrifft sensible und somit allenfalls eingeschränkt zugängliche Daten der öffentlichen Hand. Dank fortschrittlicher Technologien ist ihre Nutzung mittlerweile unter Wahrung der Rechte Dritter möglich. Um das gesellschaftliche Potenzial solcher Daten zu erschließen, kombiniert der EU-Gesetzgeber nun im Data-Governance-Ansatz Technologie, Institutionen, Verfahren und materielles Recht. So ergeben sich deutlich ausdifferenziertere, granulare Regeln zur Datennutzung.[14] Dadurch vollzieht sich letztlich ein grundsätzlicher Wandel bzw. eine Weiterentwicklung

1 S. zum Gesetzgebungsstand: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-governance-act.
2 DGA-E COM(2020) 767 final, S. 2.
3 Vgl. Impact Assessment Report SWD(2020) 295, S. 19.
4 COM(2020) 66 final; zum konkreten Hintergrund SWD(2020) 295, S. 5 ff.
5 Hilfreicher Überblick zum DGA-E bei *Spindler*, CR 2021, 99.
6 Vgl. Übersicht zu Studien zum ökonomischen Potenzial bei *Richter*, Information als Infrastruktur, 2021, S. 44 f.
7 Zu den Open-Data-Grundsätzen im Einzelnen *Richter* (o. Fußn. 6), S. 42 f., 53 ff.
8 RL EU/2019/1024.
9 Die Änderung von 2013 schloss die Informationen von öffentlichen Museen, Archiven und Bibliotheken ein, die Neufassung von 2019 erstreckt den Anwendungsbereich auch auf Informationen öffentlicher Unternehmen und öffentlich finanzierte Forschungsdaten.
10 Zur PSI-RL ausf. *Richter* (o. Fußn. 6), S. 121 ff.; zur Reform des DNG *Hartl/Ludin*, MMR 2021, 534; zur Diskussion *Richter*, Stellungnahme abrufbar unter: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/2021-01-12_Richter_Stellungnahme_Open_Data_Gesetz.pdf; *Wiebe*, Open Data in Deutschland und Europa, 2020.
11 Zur Diskussion in Deutschland *Bruns/Demary/Horn*, Hochwertige Datensätze in Deutschland, 2020.
12 Vgl. *Hartl/Ludin*, MMR 2021, 534 (535 f.); zur Diskussion *Richter*, Stellungnahme (o. Fußn. 10), S. 6 ff.; zur Regelung vor der Reform *Richter*, NVwZ 2017, 1408.
13 Hierzu *Richter*, NVwZ 2021, 760 (761); zum Stand ferner *Smart Service Welt II*, Open Public Data in Deutschland, 2020, S. 38 ff.
14 So auch in Australien, s. Commonwealth of Australia, Data Availability and Transparency Bill, Consultation Paper, 2020.