datenschutz-berater.de

45. Jahrgang

DSB 07+08/2021

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Interview

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Tim Wybitul und Johannes Zhou

Verteidigung gegen Bußgelder und Schadensersatzforderungen nach der DSGVO

Data Privacy Litigation hat durch die DSGVO erheblich an Bedeutung gewonnen. Die Praxis hat in den letzten drei Jahren gezeigt, dass Datenschutzbehörden von ihrer Befugnis nach Art. 83 DSGVO, Bußgelder zu verhängen, umfangreich Gebrauch machen. Auch Schadensersatzklagen wegen Datenschutzverstößen nach Art. 82 DSGVO nehmen stetig zu. Dieser Beitrag gibt zunächst einen Überblick über die rechtlichen Rahmenbedingungen für die Verhängung von Bußgeldern und die Geltendmachung von Schadensersatzforderungen nach der DSGVO. Daran schließen sich Maßnahmen und Handlungsempfehlungen für eine effektive Verteidigung gegen Bußgelder und Schadensersatzforderungen an.

Risiken wegen möglichen Datenschutzverstößen

Seit dem 25.5.2018 bergen Datenschutzverstöße für Unternehmen erhebliche Risiken: Zum einen können zuständige Datenschutzbehörden nach Art. 83 DSGVO Bußgelder von bis zu 20 Millionen Euro oder von bis zu 4 % des weltweit erzielten Vorjahresumsatzes verhängen. Das bislang höchste in Deutschland verhängte Bußgeld beträgt 35,3 Millionen Euro. In anderen EU-Mitgliedsstaaten sind Bußgelder von bis zu 60 Millionen Euro verhängt worden.

Zum anderen können die von Datenschutzverstößen betroffenen Personen nach Art. 82 DSGVO immateriellen Schadensersatz geltend machen. Unternehmen mussten Klägern Schmerzensgeld von bis zu 5.000 Euro zahlen (ArbG Düsseldorf, Urt. v. 5.3.2020 – 9 Ca 6557/18; ArbG Münster, Urt. v. 25.3.2021 – 3 Ca 391/20). Da Datenpannen oder sonstige Cybersecurity-Vorfälle typischerweise eine Vielzahl von Personen betreffen können, besteht das Risiko der massenhaften Geltendmachung von Schadensersatzansprüchen (umfassend hierzu Laoutoumai, Privacy Litigation, 1. Aufl. 2021). Einige Verbraucheranwälte und kommerzielle Organisationen haben sich bereits auf solche Verfahren spezialisiert und werben nach öffentlich bekannt gewordenen Cybersecurity-Vorfällen oder sonstigen möglichen DSGVO-Verstößen gezielt um betroffene Personen, deren Schadensersatzansprüche sie geltend machen wollen.

Rechtliche Rahmenbedingungen

Die Voraussetzungen für die Verhängung von Bußgeldern und Geltendmachung von Schadensersatzforderungen sind teilweise sehr umstritten. Im Folgenden werden die jeweiligen rechtlichen Rahmenbedingungen im Überblick dargestellt.

Bußgelder (Art. 83 DSGVO)

Für die Verhängung von Bußgeldern ist Art. 83 DSGVO maßgeblich, wonach Datenschutzbehörden Bußgelder gegen Verantwortliche und Auftragsverarbeiter verhängen können. Allerdings sind die genauen Anforderungen an die Sanktionierung von Unternehmen weder in dieser Norm noch an anderer Stelle in der DSGVO geregelt.

Deutsche Datenschutzbehörden vertreten die Auffassung, dass Art. 83 DSGVO eine unmittelbare Haftung von Unternehmen vorsehe. Danach genüge die bloße Feststellung eines Datenschutzverstoßes für die Haftung eines Unternehmens. Weitergehende Feststellungen seien in einem Bußgeldbescheid daher nicht erforderlich. Damit stellen sich die Behörden gegen die Anforderungen des deutschen Ordnungswidrigkeitenrechts. Denn dieses sieht in § 30 Abs. 1 OWiG für die Festsetzung einer Verbandsgeldbuße eine sog. Anknüpfungstat vor. Danach muss eine Leitungsperson rechtswidrig und schuldhaft bzw. vorwerfbar eine unternehmensbezogene Straftat oder Ordnungswidrigkeit begangen haben. Auch die Verletzung einer Aufsichtspflicht gem. § 130 Abs. 1 OWiG kann eine solche Anknüpfungstat darstellen. Letztlich muss das Verhalten einer natürlichen Person dem Unternehmen als juristische Person oder Personenvereinigung nach dem sog. Rechtsträgerprinzip zugerechnet werden können.

Eine einheitliche Rechtsprechung zu diesem sehr praxisrelevanten Thema gibt es bislang nicht. Vielmehr fallen die ersten beiden Entscheidungen zu der Frage, ob die DSGVO eine unmittelbare Unternehmenshaftung vorsieht oder ob §§ 30, 130 OWiG Anwendung finden, sehr unterschiedlich aus:

Das LG Bonn (Urt. v. 11.11.2020 – 29 OWi 1/20) folgte der Auffassung der Datenschutzbehörden, wonach sie Bußgelder direkt gegen Unternehmen als bußgeldrechtlich Betroffene verhängen können. Dies folge aus der Anwendung des EU-kartellrechtlichen Funktionsträgerprinzips. Art. 83 DSGVO und Erwägungsgrund 150 Satz 3 DSGVO würden auf den sog. funktionalen Unternehmensbegriff des Kartellrechts verweisen. Der dem Urteil zugrundeliegende

Bußgeldbescheid sei auch ohne Feststellungen hinsichtlich einer (Aufsichts-)Pflichtverletzung einer Leitungsperson wirksam.

Das LG Berlin (Beschl. v. 18.2.2021 – 526 OWi LG, 212 Js-OWi 1/20) hingegen widerspricht dieser Ansicht. Es sieht in einer unmittelbaren Unternehmenshaftung eine Verletzung des Gesetzlichkeits- und des Schuldprinzips. Vielmehr würden die Grundsätze des deutschen Bußgeldrechts gelten. Das Gericht erklärte den der Entscheidung zugrundeliegenden Bußgeldbescheid für unwirksam, weil dieser die nach §§ 30, 130 OWiG, aber auch nach § 66 OWiG erforderlichen Voraussetzungen nicht erfülle und daher ein Verfahrenshindernis bestehe. Weder Tat noch Täter seien im Bescheid hinreichend festgestellt. Die Entscheidung des LG Berlin ist zwar im Gegensatz zu der des LG Bonn nicht rechtskräftig; sie eröffnet aber einige Spielräume für eine effektive Verteidigung. Vor allem zeigt sie, dass auch die Datenschutzbehörden gut beraten sind, die allgemeinen prozessualen Anforderungen des OWiG zu beachten.

Schadensersatzforderungen (Art. 82 DSGVO)

Auch die Rechtsprechung zu Schadensersatzforderungen wegen Datenschutzverstößen ist teilweise uneinheitlich. Der Tatbestand des Art. 82 DSGVO setzt einen Schaden voraus, der kausal auf einem Verstoß gegen die DSGVO beruht.

Ordentliche Gerichte vertreten bei der Beurteilung und Bemessung von DSGVO-Schadensersatz oft einen eher restriktiven Ansatz. Viele Gerichte nehmen an, dass der bloße Datenschutzverstoß selbst für sich genommen noch keinen immateriellen Schaden begründet. Sie fordern in der Regel den Nachweis eines tatsächlich eingetretenen, objektiv nachvollziehbaren Schadens. Im Vergleich dazu setzen Arbeitsgerichte nicht selten einen niedrigeren Maßstab an und sprechen eher Schadensersatz zu. So müsse der zuzusprechende Schadensersatz eine abschreckende Höhe erreichen bzw. eine abschreckende Wirkung haben.

Auch das BVerfG setzte sich bereits mit Art. 82 DSGVO auseinander: Es stellte in einem Beschluss (BVerfG, Beschl. v. 14.1.2021 – 1 BvR 2853/19) fest, dass das AG Goslar im Ausgangsverfahren eine Schadensersatzklage nicht mit der Begründung hätte abweisen dürfen, dass es sich bei der vom Kläger erlittenen Beeinträchtigung lediglich um einen Bagatellschaden handele. Der Schadensbegriff und die Anspruchsvoraussetzungen des Art. 82 DSGVO seien im Detail weder erschöpfend geklärt noch könnten sie unmittelbar aus der DSGVO abgeleitet werden. In letzter Instanz tätige Gerichte seien daher verpflichtet, ungeklärte entscheidungserhebliche Rechtsfragen des Europarechts dem EuGH zur Vorabentscheidung nach Art. 267 AEUV vorzulegen.

Auch in anderen EU-Mitgliedsstaaten stehen die Gerichte vor dem Problem der genauen Auslegung des Art. 82 DSGVO. Der österreichische Oberste Gerichtshof (OGH, Beschl. v. 15.4.2021 – 6Ob35/21x) legte dem EuGH folgende Fragen zur Vorabentscheidung vor:

- Reicht bereits die Verletzung von Bestimmungen der DSGVO als solche für die Zuerkennung von Schadensersatz aus?
- Gibt es neben den Grundsätzen der Effektivität und Äquivalenz noch weitere Vorgaben des Unionsrechts, die nationale Gerichte bei der Bemessung des Schadensersatzes nach Art. 82 DSGVO beachten müssen?
- Setzt ein immaterieller Schaden voraus, dass die Rechtsverletzung Folgen von zumindest einigem Gewicht hat, die über den durch die Rechtsverletzung hervorgerufenen Ärger hinausgehen?

Bis zu einer Entscheidung des EuGH wird noch einige Zeit vergehen. Man sollte daher die weitere Rechtsprechung im Blick behalten. Angesichts der zahlreichen Entscheidungen zu Art. 82 DSGVO ist eine Kenntnis der einschlägigen Rechtsprechung für eine effektive Verteidigung unerlässlich. Eine Übersicht zu relevanten Entscheidungen bietet die DSGVO-Schadensersatztabelle (Wybitul, DSB 2021, 42). Sie fasst aktuelle Entscheidungen zusammen und zeigt die bisher zugesprochenen Schadenssummen in übersichtlicher Form. Eine jeweils aktuelle Fassung der Tabelle können Sie unter diesem Link abrufen: https://de.lw.com/thoughtLeadership/Latham-DSGVO-Schadensersatztabelle.

Präventive Maßnahmen

Unternehmen sollten auch präventive Maßnahmen umsetzen, um das Risiko von Datenschutzverstößen (und damit das Risiko von Bußgeldern und Schadensersatzforderungen) zu minimieren. Diese Maßnahmen beeinflussen sich wechselseitig und haben zugleich erhebliche Auswirkungen auf spätere Bußgeld- und Schadensersatzverfahren.

Umsetzung datenschutzrechtlicher Vorgaben

Um das Risiko von Vorwürfen wegen Datenschutzverstößen zu minimieren, sollten Unternehmen bestehende Lücken bei der Umsetzung datenschutzrechtlicher Vorgaben identifizieren und schließen. Dazu gehört die Implementierung von entsprechenden Strukturen und Prozessen.

Die Praxis zeigt, dass Unternehmen ein besonderes Augenmerk auf folgende Aspekte legen sollten: Erfahrungsgemäß stellen nicht den Vorgaben von Art. 30 DSGVO entsprechende Verarbeitungsverzeichnisse häufig eine relevante Schwachstelle dar. Auch bei Auftragsverarbeitungsverträgen und Vereinbarungen über gemeinsame Verantwortlichkeiten sollten Unternehmen genauer hinschauen. Dies gilt insbesondere für Datenübermittlungen in Drittländer

im Hinblick auf die „Schrems II"-Entscheidung des EuGH (Urt. v. 16.7.2020 – C-311/18).

Dokumentation

Unternehmen sollten die Umsetzung datenschutzrechtlicher Vorgaben so dokumentieren, dass sie diese zur Verteidigung vor Gericht nutzen können. Dies betrifft sowohl Form als auch Inhalt der Dokumentation. Hilfreich sind entsprechende Prozesse, die eine ordnungsgemäße Datenschutzdokumentation gewährleisten. Ohne vor Gericht und in Behördenverfahren überzeugend vorzeigbare Dokumentation ist der Nachweis, dass datenschutzrechtliche Vorgaben eingehalten worden sind, nur schwer zu führen.

Datenschutzorganisation

Um die Identifizierung und Schließung von Lücken bei der Umsetzung datenschutzrechtlicher Vorgaben sowie dessen Dokumentation zu gewährleisten, sollten Unternehmen über eine hinreichend personell und finanziell ausgestattete Datenschutzorganisation verfügen. Unternehmen sind gut beraten entsprechende Strukturen, Prozesse und Arbeitsanweisungen an operative Einheiten im Unternehmen zu implementieren und zu dokumentieren. Ein pragmatischer Maßstab für die Ausgestaltung der Datenschutzorganisation kann die bisherige Rechtsprechung zu Aufsichtspflichten nach §§ 30, 130 OWiG sein.

Zudem sollten Unternehmen für mögliche Datenschutzverstöße und Cybersecurity-Vorfälle die Verantwortlichkeiten und Aufgabenverteilung innerhalb eines Unternehmens vorab regeln.

Ablaufplan für Umgang mit Datenschutzverstößen

Im Falle eines (möglichen) schwerwiegenden Datenschutzverstoßes oder Cybersecurity-Vorfalls ist ein guter Ablaufplan empfehlenswert, an dem sich die Beteiligten orientieren können. Die im Folgenden dargestellten Beispiele für Handlungsempfehlungen haben sich in der Praxis bewährt.

Ad-hoc-Maßnahmen

Unmittelbar nach Erlangung der Kenntnis von einem relevanten Vorfall sind schadensmindernde und -begrenzende Maßnahmen wichtig. An dieser Stelle ist die Zusammenarbeit mit der IT-Abteilung oft entscheidend. Die Beteiligten müssen die Sachverhaltsaufklärung und die getroffenen Maßnahmen dokumentieren. Sofern möglich, sind auch Beweismittel (z. B. Log-Files) zu sichern. Oft sollte man an dieser Stelle auch IT-Forensiker einbinden.

Unternehmen sollten die Bedeutung solcher Ad-hoc-Maßnahmen nicht unterschätzen. Häufig werden hier die Weichen für die spätere rechtliche Aufarbeitung von Vorfällen gestellt.

Kommunikation

Bei Datenschutzverstößen und Cybersecurity-Vorfällen ergeben sich unter Umständen Melde- und Benachrichtigungspflichten. Auch sollten Unternehmen die Kommunikation nach innen und außen mitberücksichtigen. Folgende Adressaten können in Betracht kommen:

- Zuständige Datenschutzbehörden (Art. 33 DSGVO)
- Sonstige Behörden wie z. B. Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Die vom Vorfall betroffenen Personen (Art. 34 DSGVO)
- Versicherungen
- Geschäftspartner
- Relevante interne Unternehmensfunktionen, etwa Rechtsabteilung, Risikomanagement oder in Bezug auf mögliche Mitteilungspflichten nach dem WpHG
- Eigene Mitarbeiter
- Öffentlichkeit

Vorbereitung von Dokumenten

In der Praxis versenden Klägervertreter vor Erhebung einer Schadensersatzklage nach Art. 82 DSGVO häufig Forderungsschreiben. Es bietet sich daher an, (anwaltliche) Zurückweisungsschreiben und sonstige Muster-Schreiben vorzubereiten. Auch die Vorbereitung einer Schutzschrift für mögliche einstweilige Verfügungsverfahren ist sehr hilfreich, sofern betroffene Personen Unterlassungsverfügungen anstrengen könnten.

Zudem stellen betroffene Personen bei tatsächlichen oder behaupteten Datenschutzverstößen regelmäßig Auskunftsanträge nach Art. 15 DSGVO. Hier sollten Unternehmen ihre Auskunftsprozesse überprüfen, damit eine fristgerechte Bearbeitung gewährleistet ist.

Prozessstrategie in Bußgeldverfahren

In Bußgeldverfahren gibt es mehrere Anknüpfungspunkte für eine erfolgreiche Verteidigung.

Prozessuale Verteidigungsmöglichkeiten

In Bußgeldverfahren nach Art. 83 DSGVO finden gem. § 41 BDSG die Vorschriften des OWiG, der StPO und des GVG Anwendung. Dabei sollten insbesondere die prozessualen Verteidigungsmöglichkeiten, die die Verfahrensvorschriften bieten, berücksichtigt werden. Dazu gehören beispielsweise Auskunftsverweigerungsrechte oder die Geltendmachung von Erklärungsrechten.

Überprüfung des Bußgeldbescheids

Die Praxis zeigt, dass man von Datenschutzbehörden verhängte Bußgeldbescheide genau auf formelle und materielle Schwachstellen überprüfen sollte, die man zur erfolgreichen Verteidigung nutzen kann. Insbesondere sollte man prüfen, ob Bußgeldbescheide die nach § 66 OWiG zu treffenden Feststellungen enthalten. Danach muss der Bescheid unter anderem konkrete Angaben zur Person des

Täters machen und die Tat, die dem Betroffenen zur Last gelegt wird, bezeichnen. Zudem sind Ort und Zeit der Tatbegehung anzugeben. Bei einer Anwendung der §§ 30, 130 OWiG ist zudem erforderlich, dass eine Leitungsperson an einem Datenschutzverstoß beteiligt war oder eine Aufsichtspflicht verletzt hat.

Prozessstrategie in Schadensersatzverfahren

Beklagte Unternehmen sollten die im Folgenden dargestellten Aspekte bei ihrer Prozessstrategie in zivilrechtlichen Schadensersatzverfahren beachten.

Behauptete Datenschutzverstöße

In der Praxis stützen Kläger ihre Schadensersatzforderungen oftmals auf nur diffus behauptete Verstöße gegen datenschutzrechtliche Vorgaben. Eine genaue datenschutzrechtliche Überprüfung ist daher empfehlenswert.

Erfahrungsgemäß rügen Kläger wegen möglichen Datenpannen, Hackerangriffen oder sonstigen Cybersecurity-Vorfällen häufig eine Verletzung der Datensicherheit nach Art. 32 DSGVO. Hier sollten Unternehmen in der Lage sein, nachzuweisen, dass sie ein angemessenes Maß an Datensicherheit bzw. IT-Security eingehalten haben. Idealerweise können sie hier auf bestehende Dokumentation zurückgreifen und diese vor Gericht darlegen.

Ersatzfähiger und kausaler Schaden

Kläger argumentieren zudem häufig, dass der Datenschutzverstoß selbst automatisch einen immateriellen Schaden begründe. Diese Auffassung geht unseres Erachtens von einem zu weit gefassten Schadensbegriff aus. Vielmehr sind nach Erwägungsgrund 146 Satz 6 DSGVO nur „erlittene" Schäden zu ersetzen. Zudem verlangt der Wortlaut von Art. 82 Abs. 1 DSGVO, dass ein Schaden „wegen eines Verstoßes gegen diese Verordnung" entstanden sein muss (Kausalität). Ein Verstoß allein begründet daher nicht automatisch einen ersatzfähigen Schaden. Ferner fordert auch Erwägungsgrund 85 Satz 1 a. E. DSGVO die Erheblichkeit eines Schadens.

Darlegungs- und Beweislast

Auch das Zivilprozessrecht kann ein Anknüpfungspunkt für eine erfolgreiche Verteidigung sein. Unternehmen unterliegen zwar nach Art. 5 Abs. 2 DSGVO einer Rechenschaftspflicht, d. h. sie müssen – gegenüber Behörden – nachweisen können, dass sie die Datenschutzprinzipien aus Art. 5 Abs. 1 DSGVO einhalten. Daraus folgt jedoch nicht, dass Beklagte in zivilrechtlichen Verfahren nach Art. 82 DSGVO beweisen müssen, sämtliche Vorgaben der DSGVO eingehalten zu haben. Das OLG Stuttgart (Urt. v. 31.3.2021 – 9 U 34/21) stellt klar, dass die Rechenschaftspflicht keine Beweislastumkehr oder Beweiserleichterung begründet. Vielmehr würden die Beweisregeln des jeweiligen nationalen Rechts gelten. Demnach trage zunächst der Kläger die Darlegungs- und Beweislast für die anspruchsbegründenden Voraussetzungen.

Fazit

Datenschutzverstöße und Cybersecurity-Vorfälle können erhebliche finanzielle und geschäftliche Risiken mit sich bringen. Bei Fehlern können Bußgelder in Millionenhöhe und massenhafte Schadensersatzforderungen nach der DSGVO drohen. Effektive Verteidigungsstrategien gegen Bußgelder und Schadensersatzforderungen sind daher von erheblicher Bedeutung.

Die bisherige Rechtsprechung hat einige Spielräume für eine effektive Verteidigung eröffnet. Allerdings sollten Unternehmen den weiteren Verlauf in der Rechtsprechung im Blick behalten. Entscheidungen von höheren gerichtlichen Instanzen in Deutschland und des EuGH werden erheblichen Einfluss auf die weitere Entwicklung haben. Angesichts möglicher verbraucherfreundlicher Entscheidungen des EuGH sind Unternehmen gut beraten, Maßnahmen zu ergreifen, die das Risiko von Datenschutzverstößen und Cybersecurity-Vorfällen minimieren.

Präventive Maßnahmen wie eine gute Dokumentation und Datenschutzorganisation verhindern nicht nur Datenschutzverstöße, sondern können Bußgeld- und Schadensersatzverfahren entscheidend beeinflussen. Die Praxis zeigt zudem, dass vorab erstellte Ablaufpläne für den Umgang mit Datenschutzverstößen sehr hilfreich sind. Im Notfall ermöglicht dies ein konsequentes und strukturiertes Vorgehen, welches sich wiederum positiv auf spätere Verfahren auswirken kann.

Autoren: **Tim Wybitul ist Partner im Frankfurter Büro von Latham & Watkins LLP. Er berät Unternehmen in komplexen Datenschutzfragen und verteidigt sie vor Gericht und in Behördenverfahren. Dazu gehören auch mehrere der in diesem Beitrag genannten Verfahren.**

Johannes Zhou ist Rechtsreferendar und Wissenschaftlicher Mitarbeiter bei Latham & Watkins LLP.