www.compliance-berater.de

Compliance Berater

4 / 2020

Betriebs-Berater Compliance

25.3.2020 | 8.Jg
Seiten 89–132

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Dr. Thomas Kehr, RA, und Benjamin Zapp

DSGVO – Ein erster Überblick aus der Bußgeldpraxis der Aufsichtsbehörden

Die EU-Datenschutz-Grundverordnung („DSGVO") hat seit dem 25.5.2018 in jedem Mitgliedstaat der Europäischen Union unmittelbare Geltung. In der Zwischenzeit haben sowohl internationale als auch nationale deutsche Aufsichtsbehörden damit begonnen, datenschutzrechtliche Verstöße mit Bußgeldern zu ahnden. Dieser Beitrag soll einen ersten Überblick über einige besonders relevante Entscheidungen der Aufsichtsbehörden und deren Folgen für Unternehmen geben.

I. Einleitung

Die DSGVO gilt seit nunmehr ca. zwei Jahren in jedem Mitgliedstaat der Europäischen Union.[1] Mit der Einführung der DSGVO hat auch die Regelung des Art. 83 DSGVO über die Verhängung einer Geldbuße bei Verstößen gegen die DSGVO ihre Gültigkeit erlangt.[2] Die Vorschrift ermächtigt die Aufsichtsbehörden im Falle eines Verstoßes eine Geldbuße zu verhängen, deren Höhe sich an verschiedenen Kriterien bemisst. Zunächst ist für die maximale Höhe der Geldbuße entscheidend, welchen Verstoß der Verantwortliche begangen hat.[3] Insbesondere für einen Verstoß gegen die Grundsätze der Datenverarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Art. 5, 6, 7 und 9 DSGVO, sieht die Verordnung eine maximale Geldbuße in Höhe von bis zu 20 Mio. EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs vor, je nachdem, welcher der Beträge der höhere ist.[4] Diese Maximalstrafe sieht die Verordnung beispielsweise auch für Verstöße gegen die weiteren Kernelemente des Datenschutzrechts vor, namentlich für Verstöße gegen das präventive Verbot mit Erlaubnisvorbehalt gemäß Art. 6 DSGVO, gegen die Rechte der betroffenen Personen gemäß den Art. 12 bis 22 DSGVO, gegen die Vorgaben hinsichtlich der Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder eine internationale Organisation gemäß Art. 44 bis 49 DSGVO[5] sowie die Nichtbefolgung von Anweisungen der Aufsichtsbehörde im Sinne von Art. 58 Abs. 2 DSGVO.

Dieser Beitrag soll nachfolgend einen ersten Überblick darüber geben, inwiefern internationale sowie nationale Aufsichtsbehörden in Deutschland bislang von ihrer Möglichkeit der Verhängung empfindlicher Bußgelder im Sinne des Art. 83 DSGVO Gebrauch gemacht haben.[6]

II. Bußgelder

1. Bußgelder auf internationaler Ebene

Das wohl medienwirksamste Bußgeld im internationalen Bereich war das verhängte Bußgeld der französischen Aufsichtsbehörde Commission Nationale de l'Informatique et des Libertés („CNIL")[7]: Diese verhängte gegen Google LLC („Google") ein Bußgeld in Höhe von 50 Mio. EUR, da Google zum einen nicht transparent über die Datennutzung seiner Nutzer informiert hat und zum anderen der Konzern keine wirksame Einwilligung für die Verarbeitung der Daten für Werbezwecke vorweisen konnte.[8] Wie bereits aus dieser Kurzzusammenfassung der Entscheidung der CNIL erkennbar ist, ging es in diesem Fall nicht um besonders außergewöhnliche oder spezielle Verstöße gegen das Datenschutzrecht, sondern vielmehr um Verstöße gegen absolute Basics.

Hinsichtlich der Höhe des Bußgeldes lässt die Entscheidung der CNIL offen, welche Kriterien für die Bemessung ausschlaggebend waren. In der Literatur wird hinsichtlich der Höhe des Bußgeldes angemahnt, dass das von der Behörde bewusst öffentlichkeitswirksame Vorgehen nach der eigenen Auffassung der Behörde ein Teil der Sanktion sei, was schwerlich mit dem Maßnahmenkatalog des Art. 58 DSGVO zu vereinbaren sei.[9] Dem lässt sich nur zustimmen.

Die Behörde stellt in ihrer Entscheidung zunächst dar, dass der Verantwortliche[10], hier also Google, gemäß Art. 12 Abs. 1 S. 1 DSGVO dazu verpflichtet ist, geeignete Maßnahme zu ergreifen, um der betroffenen Person alle Informationen gemäß den Art. 13 und 14

1 Art. 99 Abs. 2 DSGVO.
2 Vgl. dazu *Kehr*, CB 2016, 421 ff. und *Wenzel/Wybitul*, ZD 2019, 290 ff.
3 Vgl. Art. 83 Abs. 4, 5 und 6 DSGVO. Siehe auch Art. 83 Abs. 2 DSGVO.
4 Art. 83 Abs. 5 DSGVO.
5 Vgl. dazu auch die Safe-Harbor-Entscheidung des EuGH v. 6.10.2015 – C-362/14, EWS 2015, 262 ff.
6 Einen ersten Überblick über Urteile der Gerichte zu Schadensersatzansprüchen wegen datenschutzrechtlicher Verstöße gibt *Wybitul*, NJW 2019, 3265 ff.
7 Die französische Aufsichtsbehörde CNIL wurde 1978 durch das Gesetz „loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés" gegründet. Ausführlich zur Praxis der Geldbußenzumessung der CNIL vgl. *Votteler*, ZD 2019, 431 ff.
8 CNIL, Deliberation of the Restricted Committee SAN-2019 –001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, Seite 11 ff.
9 Vgl. dazu *Wybitul*, ZD 2019, 97, 98.
10 Verantwortlicher ist nach der Legaldefinition des Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

DSGVO und alle Mitteilungen gemäß den Art. 15 bis 22 und Art. 34 DSGVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. In dem genannten Fall sah die französische Aufsichtsbehörde insbesondere die von Art. 12 Abs. 1 DSGVO geforderte leichte Zugänglichkeit und Transparenz als nicht gegeben an. Die Informationen, die Google nach Art. 13 DSGVO seinen Nutzern bereitzustellen habe, waren in mehreren Dokumenten verstreut und erst durch eine Vielzahl von Klicks erreichbar.[11] Hinsichtlich der Verständlichkeit der Informationen stellte die Behörde fest, dass die Formulierungen von Google zu vage und allgemein gehalten waren. Dem Nutzer war es mangels einer konkreten Angabe des Zwecks der Datenverarbeitung nicht möglich, die Konsequenzen der Datenverarbeitung zu erfassen.[12] Zudem stellte die Behörde fest, dass bei den Anforderungen des Art. 12 DSGVO auch zu berücksichtigen ist, dass Google in erheblichem Maße Daten verarbeitet. Sichtlich stellt die Behörde somit einen Zusammenhang zwischen der Intensität der Datenverarbeitung auf der einen Seite und den daraus resultierenden Anforderungen an die Informationspflicht des Verantwortlichen auf der anderen Seite her.[13]

In der Literatur wird zu Recht die Frage aufgeworfen, ob diese Anforderungen der CNIL an die Zweckbestimmung nicht überzogen seien und letztlich nur zu noch längeren Datenschutzerklärungen bzw. Datenschutzhinweisen führen.[14] Ob noch längere Dokumente gerade im Hinblick auf eine Verständlichkeit dieser Dokumente für Laien vorteilhaft ist, lässt sich bezweifeln. Das Transparenzgebot nach den Art. 12 ff. DSGVO wird in der Praxis durch Unternehmen insbesondere gegenüber Kunden, Beschäftigten und Bewerbern in Form eines Datenschutzhinweises sowie auf der Homepage gemäß Art. 13 DSGVO umgesetzt. Das betroffene Personen diese Dokumente, die grundsätzlich mehrere Seiten in kleiner Schrift umfassen, wirklich zur Kenntnis nehmen, ist zu hinterfragen und dürfte in den weitaus überwiegenden Fällen mit „nein" beantwortet werden. Eigentlich sollte in diesem Zusammenhang der Grundsatz „Weniger ist mehr" gelten, denn Betroffene würden sicherlich eher kürzere Dokumente lesen und auch verstehen als mehrere Seiten langatmiger datenschutzrechtlicher Dokumente. Rechtssicherste Variante für Unternehmen bleibt, bestehende Informationspflichten nach den Art. 13 ff. DSGVO ausführlich zu erfüllen.

Als weiteren Missstand stellte die französische Behörde fest, dass Google nicht über eine wirksame Einwilligungserklärung im Sinne von Art. 6 Abs. 1 S. 1 lit. a DSGVO hinsichtlich der Datenverarbeitung für Werbezwecke verfügt. Damit wird auf das auch unter Geltung der DSGVO vorherrschende und bereits nach dem BDSG a. F.[15] bekannte präventive Verbot mit Erlaubnisvorbehalt, wonach eine Datenverarbeitung vom Grundsatz her verboten ist, wenn sie nicht ausdrücklich durch Gesetz oder eine Einwilligung erlaubt ist, eingegangen. Eine Einwilligung in die Datenverarbeitung ist gemäß Art. 4 Nr. 11 DSGVO jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Dies lehnte die Behörde zum einen vollkommen zutreffend ab, da Erwägungsgrund 43 S. 2 vorsieht, dass eine Einwilligung nicht als freiwillig erteilt gilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann. Da jedoch die Einwilligung der Datenverarbeitung für Werbezwecke mit der Erstellung des Accounts und der Akzeptanz weiterer Regularien zusammenfiel, konnte nach Ansicht der Behörde im vorliegenden Fall keine wirksame Einwilligung auch für Werbemaßnahmen angenommen werden.[16]

Ebenso stellte die Behörde zu Recht fest, dass die Einwilligung der Datenverarbeitung auch deswegen unwirksam war, weil das hierfür vorgesehene Kästchen bereits mit einem Haken voreingestellt war. Es kann insoweit nicht von einer eindeutigen und unmissverständlichen Einwilligungserklärung ausgegangen werden.[17] Diese Ansicht deckt sich mit S. 3 des Erwägungsgrundes 32 der DSGVO, der bereits angehakte Kästchen nicht als wirksame Einwilligung genügen lässt. Ein „Opt-Out" ist daher nach den Vorgaben der DSGVO nicht ausreichend. Dies gilt aus datenschutzrechtlicher Sicht ganz generell und wurde jüngst auch höchstrichterlich vom Europäischen Gerichtshof („EuGH") so bestätigt[18].

Für Unternehmen drängt sich daher als Frage auf, wie sie im Hinblick auf Werbeeinwilligungen vorgehen sollen. Als praxisrelevantestes Beispiel ist sicherlich der Bezug eines Newsletters auf der Homepage eines Unternehmens zu nennen. Auf vielen Websites wird nämlich eine Möglichkeit angeboten, einen Newsletter des Unternehmens zu abonnieren. Der Begriff der Werbung ist nach deutschem Verständnis sehr weit gefasst, diesem unterfällt auch eine Versendung eines Newsletters. Da sich dieser Newsletter insbesondere an Interessenten und nicht (nur) an Kunden richtet, kann sich ein Unternehmen von vorne herein nicht auf eine Privilegierung nach § 7 Abs. 3 UWG stützen. Dies bedeutet im Ergebnis: Eine Einwilligungserklärung des Newsletter-Abonnenten ist sowohl aus datenschutzrechtlichen Gründen als auch aufgrund von Vorgaben des UWG erforderlich. Der Bundesgerichtshof („BGH") hat in ständiger Rechtsprechung klare Vorgaben an eine solche Einwilligungserklärung hinsichtlich Werbemaßnahmen aufgestellt.[19] Insbesondere muss der Betroffene wissen, dass seine Erklärung eine Einwilligungserklärung darstellt und welches Unternehmen welche Produkte und Dienstleistungen bewirbt.[20] Zudem müssen auch Angaben zur Art der Werbung, also dem Werbekanal, erfolgen (z. B. per E-Mail, per MMS/SMS, per Telefon etc.). In dem Zusammenhang hat der BGH jedoch ausgeführt, dass sich eine Einwilligungserklärung auch auf mehrere Werbekanäle beziehen kann.[21] Es ist folglich nicht notwendig, beispielsweise eine separate Einwilligungserklärung für Werbemaßnahmen per E-Mail (wie z. B. den Newsletterversand) und eine weitere separate Einwilligungserklärung für Werbung per Telefon einzuholen. Vielmehr kann sich eine Einwil-

11 CNIL, Deliberation of the Restricted Committee SAN-2019 –001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, Seite 14 Nr. 98 ff.

12 CNIL, Deliberation of the Restricted Committee SAN-2019 –001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, Seite 15, Nr. 105 ff.

13 Vgl. dazu auch *Wybitul*, ZD 2019, 97, 98.

14 *Seeger*, Newsdienst Compliance 2019, 13010.

15 Dort § 4 BDSG a. F.

16 CNIL, Deliberation of the Restricted Committee SAN-2019 –001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, Seite 23 Nr. 157.

17 CNIL, Deliberation of the Restricted Committee SAN-2019 –001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, Seite 23 Nr. 161.

18 EuGH v. 1.10.2019 – C-673/17, CB 2020, 39 ff. mit Kommentar und Praxishinweisen von *Kehr*, CB 2020, 44.

19 Vgl. dazu BGH v. 25.10.2012 – I ZR 169/10, NJW 2013, 2683; BGH v. 1.2.2018 – III ZR 196/17, NJW-RR 2018, 486.

20 BGH v. 1.2.2018 – III ZR 196/17, NJW-RR 2018, 486, 488.

21 Siehe BGH v. 1.2.2018 – III ZR 196/17, NJW-RR 2018, 486.

ligungserklärung auf mehrere dieser Werbekanäle beziehen. Dies wurde bisher in der Instanzrechtsprechung auch anders gesehen.[22] Im Ergebnis bestehen daher hinsichtlich der Ausgestaltung von Einwilligungserklärungen bezogen auf Werbemaßnahmen klare höchstrichterliche Vorgaben, die auch ohne größeren Aufwand eingehalten werden können, wenn man sich strikt an diesen orientiert, was in der Praxis jedoch nicht immer der Fall ist. Neben der Einholung der Einwilligungserklärung (1. Opt-In) ist auch eine Bestätigung dieser Einwilligung erforderlich, oftmals durch Versand einer E-Mail an den Abonnenten des Newsletters (2. Opt-In, daher auch „Doppel-Opt-In" Verfahren genannt). Auch wurde jüngst seitens des EuGH in der mit Spannung erwarteten Entscheidung zur Thematik „Cookies" ausdrücklich bestätigt, dass das Opt-In durch ein aktives Handeln des Betroffenen zu erfolgen hat.[23]

Auch in Italien wurde bereits ein Bußgeld in beträchtlicher Höhe von 2 Mio. EUR verhängt. Das betroffene Unternehmen hat im Rahmen einer telefonischen Kundenakquise die Kunden weder über ihre Rechte informiert noch lag eine schriftliche Einwilligung zur Erhebung und Verarbeitung personenbezogener Daten zu Marketingzwecken vor.[24] Auch diese Entscheidung zeigt, dass wieder das Thema „Datenschutzhinweis" sowie eine rechtskonforme Ausgestaltung der Einwilligung, wenn eine solche in der Praxis genutzt werden soll (oder muss), von besonderer Relevanz ist.

Beide Entscheidungen der Aufsichtsbehörden zeigen daher, dass es für Unternehmen unerlässlich ist, sich gerade im Hinblick auf das Vorhandensein einer Rechtsgrundlage nach Art. 6 DSGVO abzusichern und gleichzeitig bestehende Informationspflichten nach den Art. 12 ff. DSGVO datenschutzkonform zu erfüllen.

Rechtlich sicher umgesetzt werden kann dies insbesondere durch eine genaue Prüfung sämtlicher im Verzeichnis für Verarbeitungstätigkeiten aufgeführten Verarbeitungsvorgänge hinsichtlich des Vorhandenseins einer Rechtsgrundlage. Es bietet sich in diesem Zusammenhang, insbesondere auch unter Berücksichtigung der Dokumentationspflichten der DSGVO an, diese in einer separaten Spalte im Verzeichnis für Verarbeitungstätigkeiten, auch wenn dies gesetzlich nicht von Art. 30 DSGVO gefordert wird, darzustellen. Zudem sollte auch in dem Verzeichnis aufgeführt werden (auch wenn ebenfalls nicht zwingend gesetzlich erforderlich), durch welchen der in der Praxis vorhandenen Datenschutzhinweise entsprechende Informationspflichten gegenüber dem Betroffenen erfüllt werden. Eine solche Vorgehensweise erleichtert nicht nur den Überblick für den Verantwortlichen, sondern ist auch im Rahmen der bestehenden Dokumentationspflicht für Unternehmen ein großer Vorteil, sollte es zu einer Prüfung durch eine Aufsichtsbehörde kommen.

Hinsichtlich der Informationspflichten muss sichergestellt werden, dass diese für jeden Adressatenkreis anhand der Vorgaben des Art. 13 DSGVO bzw. des Art. 14 DSGVO erfüllt werden können. In der Praxis bedeutet dies, insbesondere einen Datenschutzhinweis für Kunden/Geschäftspartner/Lieferanten, für Beschäftigte/Bewerber und für eine Homepage zu verwenden und durch entsprechende Prozesse sicherzustellen, dass das Dokument dem Betroffenen auch vor dem Erheben seiner Daten zugänglich gemacht wird. Selbstverständlich kann diese Auflistung nicht abschließend sein, vielmehr ist in jedem Einzelfall zu prüfen, ob nicht weitere Datenschutzhinweise erforderlich sind, beispielsweise wenn eine Facebook-Fanpage[25] seitens des Unternehmens betrieben wird.

2. Bußgelder auf nationaler Ebene

Auch in Deutschland haben die Aufsichtsbehörden bereits Geldbußen wegen Verstößen gegen datenschutzrechtliche Vorgaben verhängt.[26]

a) Delivery Hero Germany GmbH

Im September 2019 wurde das zum damaligen Zeitpunkt höchste Bußgeld von einer deutschen Aufsichtsbehörde verhängt. Laut Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 19.9.2019 wurde ein Bußgeld in Höhe von 195.407 EUR gegen das Unternehmen Delivery Hero Germany GmbH erlassen.[27] Dieses Bußgeld umfasst laut der Pressemitteilung mehrere datenschutzrechtliche Einzelverstöße. Anknüpfungspunkt für dieses Bußgeld waren zum einen Verstöße gegen Betroffenenrechte nach den Art. 15 ff. DSGVO. In einer Mehrzahl von Fällen wurden personenbezogene Daten ehemaliger Kunden nicht gelöscht (Art. 17 DSGVO), obwohl diese jahrelang nicht mehr auf der Lieferdienst-Plattform des Unternehmens aktiv gewesen sind. Des Weiteren wurden auch Auskunftsersuchen nach Art. 15 DSGVO, das in der Praxis wohl am häufigsten geltend gemachte Betroffenenrecht, nicht datenschutzkonform erfüllt. Auf der anderen Seite wurden Werbe-E-Mails auf nicht datenschutzkonforme Weise versendet. In einem Fall sollen trotz Widerspruch gegen den Erhalt solcher Werbe-E-Mails weitere 15 solcher E-Mails an einen Betroffenen versendet worden sein.

b) Deutsche Wohnen SE

Im Oktober 2019 wurde dann auch in Deutschland das erste Millionenbußgeld erlassen.[28] Seitens der Berliner Beauftragten für Datenschutz und Informationsfreiheit wurde gegen das Unternehmen Deutsche Wohnen SE ein Bußgeld in Höhe von 14,5 Mio. EUR verhängt.

Damit war aufgrund der bisherigen deutschen Bußgeldpraxis der datenschutzrechtlichen Aufsichtsbehörden nicht unbedingt zu rechnen. Das bis dahin höchste Bußgeld hatte, wie oben beschrieben, noch nicht einmal 200.000 EUR betragen und blieb daher sogar klar hinter der Höhe der nach dem BDSG a. F. verhängten Bußgelder zurück.[29]

Hintergrund war ein datenschutzrechtlicher Verstoß gegen bestehende Löschpflichten der DSGVO. Seitens der Berliner Landesdatenschutzbeauftragten wurde bei Vor-Ort-Prüfungen in den Jahren 2017 und 2019 festgestellt, dass das Unternehmen Deutsche Wohnen SE im Hinblick auf eine Speicherung der personenbezogenen Daten seiner Kunden, in dem Fall von Mietern, ein IT System verwendet hatte, welches faktisch keine Möglichkeit vorsah, nicht mehr erforderliche personenbezogene Daten wieder zu löschen. Auch fanden keine

22 LG Berlin v. 9.12.2011 – 15 O 343/11, juris.
23 EuGH v. 1.10.2019 – C-673/17, CB 2020, 39 ff. mit Kommentar und Praxishinweisen von *Kehr*, CB 2020, 44.
24 Pressemitteilung der Garante per la Protezione die dati personali vom 30.5.2019, abrufbar unter: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9116516#3, zuletzt abgerufen am 18.2.2020.
25 Vgl. EuGH v. 5.6.2018 – C-210/16, juris.
26 Vgl. dazu auch *Braun*, ZD-Aktuell 2019, 06445.
27 Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 19.9.2019, 711.408.1, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf, zuletzt abgerufen am 18.2.2020.
28 Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 5.11.2019, 711.412.1, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf, zuletzt abgerufen am 10.2.2020.
29 Vgl. dazu *Kehr*, PStR 2015, 152, 157.

Überprüfungen seitens des Unternehmens statt, ob diese Daten überhaupt noch für den jeweiligen datenschutzrechtlichen Zweck erforderlich waren. Zum einen wurde hinsichtlich der Höhe des Bußgelds seitens der Aufsichtsbehörde berücksichtigt, dass teilweise auch sehr sensible Daten seitens des Unternehmens nicht gelöscht wurden. Neben Gehaltsnachweisen und Kopien von Arbeitsverträgen fanden sich darunter auch Steuer-, Sozial- und Krankenversicherungsdaten. Ohne dass aus der Pressemitteilung der Berliner Landesdatenschutzbeauftragten hervorgeht, um welche Daten es sich genau gehandelt hat, liegt es sehr nahe, dass damit auch besondere Kategorien von personenbezogenen Daten im Sinne von Art. 9 DSGVO, welche besonders schützenswert sind und daher nur unter strengen Vorgaben überhaupt verarbeitet werden dürfen, weiterhin gespeichert wurden, obwohl sie hätten gelöscht werden müssen. Zum anderen wurde sicherlich auch berücksichtigt, dass der datenschutzrechtliche Verstoß bereits in dem Jahr 2017, also noch unter dem damals geltenden BDSG a. F., aufgedeckt wurde. Der Verstoß wurde jedoch nicht abgestellt, sondern lediglich vorbereitende Maßnahmen seitens des Unternehmens getroffen, so dass auch im März 2019 noch kein datenschutzkonformer Zustand erreicht wurde.

Systematisch stützt der Berliner Landesdatenschutzbeauftragte das Bußgeld auf Verstöße gegen Art. 25 Abs. 1 DSGVO (Datenschutz durch Technikgestaltung)[30] und Art. 5 DSGVO (Allgemeine Grundsätze für eine Verarbeitung von personenbezogenen Daten)[31]. Aus diesen Vorschriften, insbesondere dem allgemeinen datenschutzrechtlichen Grundsatz der Datenminimierung, lässt sich auch unter Bezugnahme auf Art. 17 DSGVO ableiten, dass personenbezogene Daten dann gelöscht werden müssen, wenn sie zum Erfüllen des datenschutzrechtlichen Zwecks nicht mehr erforderlich sind. Ein Antrag des Betroffenen ist dazu nicht erforderlich. Vielmehr handelt es sich um eine gesetzliche Pflicht. Natürlich müssen in dem Zusammenhang auch anderweitige gesetzliche Vorgaben, insbesondere Aufbewahrungspflichten, berücksichtigt werden, zum Beispiel solche der AO oder des HGB. Es kann demnach eine Situation eintreten, wonach das Löschen aus datenschutzrechtlichen Gesichtspunkten zwingend ist, basierend auf den Vorgaben der gesetzlichen Aufbewahrungspflichten anderer Gesetze jedoch gar nicht vorgenommen werden darf. Gerade solche gegenläufigen Gesichtspunkte machen das Einhalten der datenschutzrechtlichen Vorgaben in der Praxis für Unternehmen sehr schwierig. Im Endeffekt kann hier eine Einschränkung der Verarbeitung nach Art. 18 DSGVO weiterhelfen.

Interessant ist auch, dass seitens der Berliner Landesdatenschutzbeauftragten ausgeführt wird, dass für den festgestellten Verstoß basierend auf dem Jahresumsatz des Unternehmens von über 1 Mrd. EUR der Bußgeldrahmen bei ca. 28 Mio. EUR lag. Das Bußgeld hätte daher noch höher ausfallen können. Ob seitens der Aufsichtsbehörden in dem Zusammenhang bereits das neue Bußgeldmodell der Datenschutzkonferenz[32] zugrunde gelegt wurde, lässt sich dem veröffentlichten Dokument leider nicht entnehmen.[33]

c) 1&1 Telecom GmbH

Das nächste Millionenbußgeld ließ nicht lange auf sich warten. Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit hat im Dezember 2019 bekanntgegeben, dass er ein Bußgeld in Höhe von 9,55 Mio. EUR gegen das Telekommunikationsunternehmen 1&1 Telecom GmbH verhangen hat.[34] Nach Ansicht des Bundesbeauftragten für Datenschutzschutz hatte das Unternehmen keine hinreichenden technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO getroffen, um seine Kundendaten zu schützen. Konkret ging es darum, dass unberechtigte Personen über den Kundenservice Auskünfte zu fremden Kundendaten erhalten konnten. Denn allein durch Angabe des Namens und des Geburtsdatums des (vermeintlichen) Kunden konnte der Anrufer weitergehende Informationen zu den über andere gespeicherte Kundendaten erhalten. Ein solcher Prozess ist natürlich insbesondere dann problematisch, wenn dadurch personenbezogene Daten von Betroffenen herausgegeben werden, die gar nicht selbst das Auskunftsverlangen gestellt haben. Seitens des Bundesbeauftragten für den Datenschutz wurde ausdrücklich darauf hingewiesen, dass durch eine solche Vorgehensweise eine Gefahr für den gesamten Kundenbestand des Unternehmens vorgelegen habe.

Ähnlich wie im oben gerade dargestellten Sachverhalt betreffend das Bußgeld gegen Deutsche Wohnen SE wurde auch hier von der Aufsichtsbehörde wieder explizit darauf hingewiesen, dass sich das Bußgeld im unteren Rahmen befände. Im Ergebnis hätte es demnach auch wesentlich höher ausfallen können. Da sich das Unternehmen jedoch im gesamten Prozess kooperativ zeigte, wurde seitens des Bundesbeauftragten für Datenschutz wohl von einer höheren Sanktion abgesehen.

Das oben dargestellte Authentifizierungsverfahren des Unternehmens, das lediglich auf dem Namen und dem Geburtsdatum basiert, ist nach Ansicht des Bundesbeauftragten für den Datenschutz keine geeignete technische und organisatorische Maßnahme im Sinne von Art. 32 DSGVO. Neben dem dogmatischen Anknüpfungspunkt der technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO hat dies auch anderweitige Konsequenzen für besonders praxisrelevante Bereiche des Datenschutzrechts. Das in der Praxis am häufigsten seitens der Betroffenen geltend gemachte Recht ist das Auskunftsrecht nach Art. 15 DSGVO. Auch in einem solchen Fall besteht eine vergleichbare Situation. Betroffene wenden sich an eine verantwortliche Stelle, um ihren Auskunftsanspruch geltend zu machen. Seitens der verantwortlichen Stelle werden dann dem Betroffenen weitreichende Informationen nach den Vorgaben des Art. 15 Abs. 1 und Abs. 2 DSGVO übermittelt. Falls noch nicht geschehen,

30 Art. 25 Abs. 1 DSGVO regelt: Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

31 Nach Art. 5 DSGVO muss eine Verarbeitung rechtmäßig, nach Treu und Glauben, nachvollziehbar, zweckgebunden, auf das notwendige Maß beschränkt, auf der Basis richtiger Daten, vor Verlust, Zerstörung und Schädigung geschützt und die Integrität und Vertraulichkeit wahrend stattfinden.

32 Konzept der unabhängigen Datenschutzaufsichtsbehörden der Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen vom 14.10.2019, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/20191016_bußgeldkonzept.pdf, zuletzt abgerufen am 10.2.2020.

33 Vgl. dazu ausführlich *Lang*, CB 2020, 20 ff.

34 Pressemitteilung des Bundesbeauftragten für Datenschutz und Informationsfreiheit vom 9.12.2019, „BfDI verhängt Geldbußen gegen Telekommunikationsdienstleister“, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html, zuletzt abgerufen am 10.2.2020.

sollten Unternehmen daher ihre Identifizierungsprozesse entsprechend überprüfen und ggf. verschärfen. Denn gerade der dargestellte Sachverhalt zeigt, dass man „lieber einmal mehr nachfragen sollte", damit eine Identität des Betroffenen auch zweifelsfrei geklärt werden kann, denn andernfalls kann es teuer werden.

d) Strategien, um Bußgelder zu vermeiden

Wie können sich deutsche Unternehmen vor solchen Bußgeldern schützen?[35]

Der vorliegende Beitrag soll keinen Überblick über sämtliche allgemeinen und besonderen Strategien liefern, um Bußgelder zu vermeiden. Vielmehr soll hier lediglich auf einige besonders praxisrelevante Aspekte der deutschen Bußgeldpraxis eingegangen werden.

Den dargestellten Sachverhalten hinsichtlich der erlassenen deutschen Bußgelder ist zu entnehmen, dass immer auch ein Bezug zu den technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO besteht. Gerade im Hinblick auf diese Anknüpfungspunkte ist daher eine rechtskonforme Ausgestaltung der technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DSGVO von besonderer Relevanz.

Mit dem Standard-Datenschutzmodell („SDM")[36] wird seitens der Datenschutzkonferenz, einem Zusammenschluss der datenschutzrechtlichen Aufsichtsbehörden des Bundes und der Länder, ein neues Werkzeug bereitgestellt, mit dem die Auswahl, Umsetzung und Bewertung technischer und organisatorischer Maßnahmen im Sinne von Art. 32 DSGVO unterstützt wird. Erklärtes Ziel der Datenschutzkonferenz ist es in diesem Zusammenhang, mit dem SDM einen Maßnahmenkatalog für datenschutzrechtliche Berater und Aufsichtsbehörden zur Verfügung zu stellen, um so eine einheitliche Beratungs- und Prüfungspraxis nach dem Inkrafttreten der DSGVO sicherzustellen. Dies bezieht sich jedoch ausschließlich auf technische und organisatorische Maßnahmen und nicht, wie der Name Standard-Datenschutzmodell vermuten lässt, auf sämtliche datenschutzrechtliche Vorgaben der DSGVO bzw. des BDSG. Mehr Rechtssicherheit kann durch das SDM folglich auch nur im Bereich der technischen und organisatorischen Maßnahmen erreicht werden, nicht jedoch darüber hinaus.

Das SDM setzt bei einer Strukturierung der in Art. 5 DSGVO genannten allgemeinen rechtlichen Vorgaben an (Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit). Für die systematische Darstellung dieser aus dem Datenschutzrecht resultierenden Anforderungen wird in dem SDM der Begriff „Gewährleistungsziel" verwendet, da eine datenschutzkonforme Verarbeitung unter Berücksichtigung der elementaren datenschutzrechtlichen Schutzziele durch technische und organisatorische Maßnahmen „gewährleistet" werden soll. Berücksichtigt werden nicht nur grundlegende datenschutzrechtliche Anforderungen, sondern auch klassische Schutzziele der Informationssicherheit. Aus den Vorgaben des Art. 5 DSGVO werden folgende Gewährleistungsziele abgeleitet: 1. Datenminimierung, 2. Verfügbarkeit, 3. Integrität, 4. Vertraulichkeit, 5. Nichtverkettung, 6. Transparenz und 7. Intervenierbarkeit.[37]

Das SDM bietet mit seinen Gewährleistungszielen folglich eine Übersetzungshilfe vom Recht (also den allgemeinen Grundsätzen des Art. 5 DSGVO) zur Technik.[38] Diese seitens der Aufsichtsbehörden entwickelte „Hilfestellung" sollte von Unternehmen durch eine Modifizierung der technischen und organisatorischen Maßnahmen unter Berücksichtigung der Vorgaben des SDM angenommen werden. Dies ist insbesondere deshalb von besonderer Relevanz, da nunmehr mit dem SDM ein Standard für datenschutzrechtliche Aufsichtsbehörden besteht, der in der Praxis bei Kontrollen angewendet wird und bei Nichtbeachtung durch Unternehmen seitens der Aufsichtsbehörden sanktioniert werden dürfte. Unternehmen ist daher anzuraten, ihren Ist-Zustand der technischen und organisatorischen Maßnahmen mit dem Soll-Zustand nach dem SDM abzugleichen und Schritt für Schritt erforderliche Modifizierungen vorzunehmen. Im Ergebnis dürfte dies, je nach Größe des Unternehmens, einen Prozess darstellen, der mindestens mehrere Monate dauern wird. Das SDM beinhaltet daneben jedoch auch vielfältige weitere Bausteine[39], die im Laufe der Zeit veröffentlicht werden sollen. Schon jetzt lässt sich nach Analyse der Bausteine jedoch bereits aussagen, dass diese sehr (vielleicht auch zu) umfangreich sind und zudem (zumindest aus Sicht der Unternehmen) mehr konkrete Vorgaben enthalten könnten.

Nach den Erfahrungen der Verfasser werden in der Praxis zudem Prüfungen der Aufsichtsbehörden insbesondere von unzufriedenen Kunden (teilweise auch aus „datenschutzfremden" Gründen) eingeleitet. Des Weiteren ist auch der Bereich Personal, insbesondere hinsichtlich gekündigter Arbeitnehmer und abgelehnter Bewerber mit besonderen Gefahren verbunden. Es ist für Unternehmen daher gerade im Auftritt nach außen im Hinblick auf diese Zielgruppen von besonderer Relevanz, sich nachweisbar datenschutzkonform zu verhalten.[40]

Vor allem sollten auch aktuelle gerichtliche, insbesondere höchstrichterliche, Urteile dringend berücksichtigt werden. Zu erwähnen sei an der Stelle nur das wegweisende Urteil des EuGH zum Thema Cookies.[41] Auch aktuell, also nach mehreren Monaten nach dem Urteil des EuGH, wurden daraus entstehende Modifikationen immer noch nicht von allen Unternehmen umgesetzt. Natürlich muss Unternehmen ein gewisser Zeitraum dafür gewährt werden. Gerade auch bei international tätigen Unternehmen oder bei Konzernen ist der Aufwand für den Umsetzungsakt auch nicht zu unterschätzen, da beispielsweise seitens eines Konzerns selbstverständlich eine konzernweite Vorgehensweise bevorzugt wird, was natürlich Zeit kostet. Problematisch für Unternehmen ist in dem Zusammenhang jedoch, dass

35 Vgl. dazu ausführlich *Wybitul*, ZD 2019, 290.

36 Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf Basis einheitlicher Gewährleistungsziele, Version 2.0a, Stand November 2019, abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/SDM-Methode_V2.0a_0.pdf, zuletzt abgerufen am 10.2.2020.

37 Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf Basis einheitlicher Gewährleistungsziele, Version 2.0a, Stand November 2019, abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/SDM-Methode_V2.0a_0.pdf, zuletzt abgerufen am 10.2.2020, Seite 24 ff.

38 Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf Basis einheitlicher Gewährleistungsziele, Version 2.0a, Stand November 2019, abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/SDM-Methode_V2.0a_0.pdf, zuletzt abgerufen am 10.2.2020, Seite 5.

39 Aktuell sind folgende Bausteine veröffentlich: Aufbewahrung, Planung und Spezifikation, Dokumentation, Protokollierung, Trennung, Löschen und Vernichten sowie Datenschutzmanagement. Diese können auf der Homepage des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern abgerufen werden unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/, zuletzt abgerufen am 10.2.2020.

40 Vgl. zu den strategischen Maßnahmen zur Vermeidung von Sanktionen auch *Wybitul*, ZD 2019, 290.

41 EuGH v. 1.10.2019 – C-673/17, CB 2020, 39 ff. mit Kommentar und Praxishinweisen von *Kehr*, CB 2020, 44.

ein einfacher Blick auf ihre Unternehmenshomepage genügt, um zu sehen, dass dort beispielsweise immer noch der alte Cookiebanner verwendet wird, kein Tool zur Abgabe von differenzierten Einwilligungen genutzt wird oder im Datenschutzhinweis noch auf das berechtigte Interesse im Sinne von Art. 6 Abs. 1 S. 1 lit. f DSGVO als Rechtsgrundlage für das Setzen von Cookies eingegangen wird. Da sich alle Missstände leicht auf der Homepage, also öffentlich von jedermann, betrachten lassen, überrascht es nicht, dass allein in Rheinland-Pfalz laut Aussage des dortigen Landesdatenschutzbeauftragten auf seiner Homepage insgesamt 15.000 Anzeigen vorliegen, die Verstöße bezüglich der Thematik „Cookies" betreffen.

III. Fazit

Es bleibt abzuwarten, wie sich die weitere Handhabung der internationalen und deutschen Aufsichtsbehörden entwickeln wird. Insbesondere wird spannend zu sehen sein, ob solche Bußgeldbescheide auch vor Gericht Bestand haben werden. Aufgrund der nunmehr aktuellen Höhe der Bußgelder ist davon auszugehen, dass seitens der betroffenen Unternehmen eine gerichtliche Überprüfung angestrebt wird.

Beide dargestellten „deutschen" Millionenbußgelder zeigen jedenfalls, dass auch in Deutschland nunmehr scharfe Sanktionen für Unternehmen drohen. Der vom europäischen Gesetzgeber in Art. 83 Abs. 1 DSGVO geforderte Abschreckungseffekt ist demnach auch in Deutschland eingekehrt.

Auch wenn es bereits in der Literatur vielfach wiederholt wurde, so gilt das Folgende nach den betrachteten Bußgeldern der Aufsichtsbehörden umso mehr: Der Bereich Datenschutzrecht muss nunmehr von jedem Unternehmen als wesentlicher Bestandteil eines effektiven Compliance-Management-Systems angesehen werden. Andernfalls drohen hohe Sanktionen.

AUTOREN

Dr. Thomas Kehr *ist Rechtsanwalt und Geschäftsführer der Dornbach GmbH Rechtsanwaltsgesellschaft. Er ist spezialisiert auf Gesellschaftsrecht, Datenschutzrecht und den Bereich Compliance und berät mittelständische Unternehmen und Konzerne.*

Benjamin Zapp *ist als Referendar jur. im Bezirk des Oberlandesgerichts Koblenz tätig und als wissenschaftlicher Mitarbeiter bei der Dornbach GmbH Rechtsanwaltsgesellschaft angestellt.*