Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

2
K&R

24. Jahrgang **Februar 2021** Seiten 73 – 144

dfv Mediengruppe · Frankfurt am Main

soll. Hierbei konnte offenbleiben, ob die Beklagte nach diesen Grundsätzen überhaupt berechtigt wäre, zugleich mit der Deaktivierung des – auch nach ihrem Vortrag zumindest nicht eindeutig rechtswidrigen – Beitrags des Klägers eine Sperre des Nutzers auszusprechen, oder, ob sie diese nicht erst androhen und ggf. nach Abwarten einer Beschwerdefrist hätte verhängen dürfen.

Nach alledem ist im hiesigen Fall von einem Wegfall der Wiederholungsgefahr nicht auszugehen.

Die Entscheidung über die Androhung eines Ordnungsmittels beruht auf § 890 ZPO.

3. Angesichts der Unzulässigkeit des Feststellungsantrages zu Ziffer 1., war der hilfsweise gestellte Antrag auf Berichtigung von Daten zu prüfen […]. Dieser ist jedoch unbegründet. […]

4. Der Kläger hat gegen die Beklagte keinen Anspruch auf Auskunft darüber, ob die Beklagte ein Unternehmen mit der Prüfung beauftragt hat […]

5. Der Kläger hat auch keinen Anspruch auf Auskunft, ob die Beklagte konkrete oder abstrakte Weisungen, Hinweise, Ratschläge oder sonst irgendwelche Vorschläge von der Bundesregierung oder nachgeordneten Dienststellen hinsichtlich der Löschung von Beiträgen und/oder der Sperrung von Nutzern erhalten hat, und ggf. welche […].

6. Der Kläger kann auch nicht die Zahlung von Schadensersatz verlangen […].

a) Für die Zuerkennung einer Geldentschädigung fehlt es an einer schwerwiegenden Beeinträchtigung des Klägers bei gleichzeitigem Vorliegen eines schweren Verschuldens der Beklagten (vgl. auch OLG Oldenburg, Urt. v. 27. 1. 2020 – 13 U 128/19). Der Kläger war durch die Löschung seines Beitrages und der zeitlich begrenzten Sperre seines Kontos lediglich in der Form seiner sozialen Kontaktaufnahme eingeschränkt. Ihm war es möglich, über andere Medien mit anderen Personen in Kontakt zu treten.

b) Soweit der Kläger seinen Zahlungsanspruch mit dem Eintritt eines materiellen Schadens infolge der fehlenden Nutzung des Netzwerkes während des Sperrzeitraums begründet und insoweit die Bezahlung einer fiktiven Lizenzgebühr in Höhe von 50 EUR täglich verlangt, dringt er hiermit nicht durch. Nach der sogenannten Differenzhypothese setzt die Annahme eines materiellen Schadens grundsätzlich voraus, dass der tatsächliche Wert des Vermögens des Geschädigten geringer ist als der Wert, den das Vermögen, ohne das die Ersatzpflicht begründende Ereignis haben würde. Danach liegt ersichtlich kein Schaden des Klägers vor, da er auch ohne Sperre keine Lizenzgebühr für die Nutzung seines F.-Profils und der dort gespeicherten Daten erhalten hätte (LG Frankfurt a. M., Urt. v. 5. 3. 2020 – 2-03 O 411/18; vgl. OLG Oldenburg, Urt. v. 27. 1. 2020 – 13 U 128/19; LG Hamburg, Urt. v. 31. 5. 2019 – 305 O 117/18, BeckRS 2019, 21755 Rn. 57).

c) Auch eine fiktive Schadensberechnung kommt nicht in Betracht. Diese wird nach der Rechtsprechung nur in Ausnahmefällen für zulässig gehalten. Eine Anwendung auf die Sperre eines F.-Accounts hält die Kammer für nicht angebracht (vgl. LG Hamburg, Urt. v. 31. 5. 2019 – 305 O 117/18, BeckRS 2019, 21755 Rn. 57; LG Traunstein, Urt. v. 13. 12. 2019 – 8 O 2622/18).

d) Der Anspruch des Klägers ergibt sich auch nicht aus Art. 82 Abs. 1 DSGVO. Es ist bereits nicht ersichtlich, dass die Beklagte die Daten des Klägers – jedenfalls in Bezug auf die hier streitgegenständliche Sperre – in datenschutzrechtswidriger Weise verarbeitet hätte. Nach den AGB der Beklagten darf die Beklagte solche Löschungen vornehmen und Sperren aussprechen. Dann ist aber auch die Verarbeitung der Daten für diesen Zweck von Art. 6 Abs. 1 lit. b DSGVO erfasst. Dass die Datenverarbeitung der Beklagten aus anderen Gründen rechtswidrig wäre, hat der Kläger nicht hinreichend substantiiert vorgetragen. Im Übrigen ist auch nicht ersichtlich, welcher Schaden dem Kläger durch die angeblich rechtswidrige Verarbeitung entstanden sein sollte.

7. Der Kläger hat einen Anspruch auf Ersatz von vorgerichtlichen Kosten […], jedoch nicht in der geltend gemachten Höhe. […]

Bußgeldhöhe bei unzureichenden Datenschutzmaßnahmen in Callcenter

LG Bonn, Urteil vom 11. 11. 2020 – 29 OWi 1/20

Volltext-ID: KuRL2021-133, www.kommunikationundrecht.de

ECLI:DE:LGBN:2020:1111.29OWI1.20.00

Art. 32 Abs. 1, 2, Art. 83 Abs. 1, 2, 4 DSGVO

1. Die Betroffene hat gegen Datenschutzvorgaben verstoßen, indem sie es im Regelfall in ihren Callcentern ausreichen ließ, dass durch die Callcenter-Agenten zur Authentifizierung des Anrufers Name und Geburtsdatum abgefragt wurden.

2. Eine Bemessung des Bußgeldes mit Fokussierung auf den Unternehmensumsatz ist problematisch. Sie mag bei Datenschutzverstößen von mittlerem Gewicht zu angemessenen Ergebnissen führen. Sie versagt jedoch bei schweren Datenschutzverstößen umsatzschwacher Unternehmen und leichten Datenschutzverstößen umsatzstarker Unternehmen. Hier haben die tatbezogenen Zumessungsgesichtspunkte Vorrang. (Leitsätze der Redaktion)

Sachverhalt

Die Betroffene K. C. GmbH gehört zum K. X. Konzern (im Folgenden: K. X.). Dieser zählt zu den fünf größten Telekommunikationsdienstleistern in Deutschland. Die Produkte des Konzerns werden in erster Linie über die Marke K. sowie daneben über Discount-Marken angeboten.

Die K. X. AG als börsennotierte Muttergesellschaft konzentriert sich auf die Holding-Aufgaben wie Geschäftsführung, Finanz- und Rechnungswesen, Cash-Management, Personalwesen und Risikomanagement. Das operative Geschäft wird im Wesentlichen von der K. G. SE und dabei insbesondere von der Betroffenen, der K. C. GmbH, sowie von der X. GmbH betrieben. Die Betroffene ist 100 %ige Tochter der K. B. GmbH, die ihrerseits eine 100 %ige Tochter der K. G. SE ist. Deren Anteile wiederum hält zu 100 % die Muttergesellschaft K. X. AG. Zwischen allen Gesellschaften des Konzerns bestehen umfassende Gewinnabführungs- und Beherrschungsverträge. K. X. hatte im Geschäftsjahr 2018 Umsatzerlöse von rund 3,63 Milliarden Euro, die im Jahre 2019 auf 3,76 Milliarden Euro stiegen. Der Gewinn des Konzerns betrug im Jahre 2018 rund 406 Millionen Euro, im Jahre 2019 rund 373 Millionen Euro.

Im Tatzeitraum seit Inkrafttreten der DSGVO am 25. 5. 2018 bis zum 8. 5. 2019 betrieb die Betroffene im Konzernverbund für die Marke K. Callcenter mit Callcenter-Serviceagenten. Diese betreuten rund […] Millionen Kunden.

Die Callcenter-Agenten der Betroffenen arbeiteten mit der sog. Z. (im Folgenden Z.), einer Benutzeroberfläche auf der Grundlage der Kundendatenbank des Unternehmens K. Diese stellte dem Callcenter-Agenten die für die Bearbeitung von Kundenanfragen erforderlichen Informationen zur Verfügung.

Im Einzelnen waren dies: Name und Kundenummer, Adresse des Kunden, Geburtsdatum des Kunden, Vertragsdaten (Art, Konditionen, Laufzeit und Vertragsstatus), Telefonnummer des Kunden, E-Mail-Adresse des Kunden, Werbeeinstellungen, Rechnungsdaten bzw. -status (d. h. offen bzw. beglichen), die Bankverbindung, die allerdings nach der „Need-to-know"-Regel nur Mitarbeitern vollständig angezeigt wurde, die damit arbeiteten (z. B. W., S., Forderungsmanagement), während den Callcenter-Agenten des First-Level-Support nur die letzten vier Ziffern der IBAN angezeigt wurden, Rechnungen, wobei die Kontonummer bis auf die vier letzten Ziffern technisch unkenntlich gemacht („ausgeixt") waren, die vergangene Korrespondenz mit dem Kunden.

Einzelverbindungsnachweise oder sonstige Verkehrsdaten wurden nicht in der Z. angezeigt und waren somit auch nicht für die Callcenter-Agenten einsehbar. Sie wurden den Kunden nur im Control-Center, einer Web-Anwendung zur Selbstverwaltung des Kundenkontos, zur Verfügung gestellt.

Anrufer erreichten im Callcenter in der Regel als erstes einen Serviceagenten des First-Level-Supports. Dieser musste den Anrufer zunächst identifizieren. Erfolgte der Anruf unter einer von K. vergebenen Telefonnummer wurde dem Serviceagenten der jeweilige Datensatz der Telefonnummer direkt angezeigt. Handelte es sich dagegen um einen Anruf von einer fremden oder unterdrückten Telefonnummer wurde der Kunde vom Serviceagenten anhand seines Namens und seines Geburtsdatums oder – alternativ – durch Angabe von Kunden-/Vertrags- bzw. Auftragsnummer identifiziert.

Der jeweilige Serviceagent war angehalten, den Anrufenden als Berechtigten zu authentifizieren. Hierzu wurde – soweit dies nicht bereits für den Aufruf des richtigen Datensatzes im Rahmen der Identifizierung erforderlich war – das Geburtsdatum abgefragt.

Nach der Authentifizierung waren die Callcenter-Agenten ermächtigt, dem Anrufer Auskünfte zu erteilen und Änderungswünsche entgegenzunehmen. Bei bestimmten Themen leiteten die Callcenter-Agenten des First-Level-Support auf der Grundlage eines Berechtigungskonzepts die Anrufer an andere Mitarbeiter weiter. So konnte etwa nur die Rechnungsstelle eine neue Bankverbindung eingeben. Eine nochmalige oder strengere Authentifizierung erfolgte gegenüber diesen weiteren Mitarbeitern nach der Authentifizierung durch den First-Level-Support nicht.

Für den Fall, dass für den Callcenter-Agenten erkennbar eine andere Person als der Kunde im Callcenter anrief, hatte die Betroffene keine umfassende Regelung getroffenen. Lediglich für den Umgang mit telefonischen Anfragen von gesetzlichen Betreuern gab es eine besondere Arbeitsanweisung. Im Übrigen entsprach es bei der Betroffenen gängiger Praxis, dass Personen, die sich als Familienangehörige des Kunden oder sonst nahestehende Personen vorstellten und zur Authentifizierung den Namen und das Geburtsdatum des Kunden nennen konnten, als legitimiert galten, für den Kunden zu handeln. Dies war unabhängig davon, ob diese Person vom Kunden als sog. weiterer Ansprechpartner im System hinterlegt worden war oder nicht. Nicht ausdrücklich geregelt war auch, wie die Callcenter-Agenten reagieren sollten, wenn ein anrufender Dritter im Rahmen des Authentifizierungsprozesses das Geburtsdatum des Kunden nicht nennen konnte.

Die Authentifizierung der Anrufer im Callcenter wurde bei der Betroffenen schon seit mehreren Jahren wie vorstehend beschrieben praktiziert. Eine Überprüfung dieser Praxis auf ihre Konformität mit der Datenschutzgrundverordnung erfolgte nicht.

Die Möglichkeit, als (vermeintliche) Familienangehörige eines Kunden anzurufen, machte sich die ehemalige Lebensgefährtin eines Kunden von K. zunutze. Ihr Ex-Partner hatte seine vorherige Mobilfunknummer bewusst geändert, um von ihr nicht mehr kontaktiert zu werden. Aufgrund einer offenen Forderung war es zu einer Sperrung des Mobilfunkanschlusses des K.-Kunden gekommen, was der ehemaligen Lebensgefährtin offenbar bekannt war. Am 23. 12. 2018 rief sie im Callcenter der Betroffenen an, gab sich als Ehefrau des Kunden aus und erklärte, dass sie die offene Forderung beglichen habe. Da sie den Namen und das Geburtsdatum ihres Ex-Partners nennen konnte, wurde sie durch die Callcenter-Agentin als Berechtigte behandelt. Im Zuge des Gesprächs wurde der Anruferin die neue Telefonnummer ihres Ex-Partners bekannt gegeben. Dies nutzte sie in der Folge für belästigende Anrufe, weswegen der Kunde von K. bei der Polizei M. Anzeige wegen Nachstellung erstattete.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – BfDI – erlangte durch eine Mitteilung der Polizei M. vom 31. 1. 2019 von dem Vorfall Kenntnis. Am 25. 3. 2019 leitete der BfDI ein Ordnungswidrigkeitenverfahren gegen die Betroffene ein. Mit Schreiben vom 8. 4. 2019, zugestellt am 11. 4. 2019, hörte er die Betroffene an. Mit Bußgeldbescheid vom 27. 11. 2019 verhängte der BfDI gegen die Betroffene wegen eines grob fahrlässigen Verstoßes gegen Art. 32 Abs. 1 DSGVO ein Bußgeld in Höhe von 9 550 000 EUR.

Eindeutige Anforderungen an den Authentifizierungsprozess in Callcentern waren zum damaligen Zeitpunkt nicht etabliert. Richtlinien oder Hinweise dazu wurden von dem BfDI nicht veröffentlicht. Auch in den halbjährlich stattfindenden Besprechungen der führenden Telekommunikationsunternehmen mit dem BfDI („N") war die Frage, wie in Callcentern die Identifizierung und Authentifizierung der Kunden erfolgen soll, nicht Gegenstand.

Als Reaktion auf die Ermittlungen des BfDI änderte die Betroffene die Authentifizierung im Callcenter. Als vorläufige Maßnahme wurde am 8. 5. 2019 eine Authentifizierung über die Kunden-/Vertrags- oder Auftragsnummer, das Geburtsdatum bzw. die E-Mail-Adresse und die letzten vier Ziffern der IBAN eingeführt.

Seit dem 9. 12. 2019 müssen sich die Anrufer in den Callcentern von K. mittels einer fünfstelligen Service-PIN authentifizieren, die den Kunden per E-Mail oder postalisch übermittelt wurde und bei Bedarf im Online Control Center in eine Wunsch-PIN geändert werden kann. Die IT-Struktur der Betroffenen musste angepasst und die Mitarbeiter im Callcenter entsprechend geschult werden.

Aus den Gründen

IV. Ein Prozesshindernis besteht nicht. Der Bußgeldbescheid des BfDI bildet eine tragfähige Grundlage für das gerichtliche Verfahren, so dass dem Antrag der Verteidigung auf Einstellung des Verfahrens nicht nachzukommen war.

1. In dem Bußgeldbescheid des BfDI wird der Datenschutzverstoß näher dargelegt und festgestellt, dass die Betroffene gegen Art. 83 Abs. 4 lit. a i. V. m. Art. 32 Abs. 1 der VO (EU) 2016/679 (DSGVO) verstoßen habe, indem sie es jedenfalls grob fahrlässig unterlassen habe, Prozesse zur hinreichenden Authentifizierung von Anrufern zu gewährleisten. Nicht näher beschrieben wird, welche natürlichen Personen im Unternehmen der Betroffenen durch welche Handlungen den Datenschutzverstoß begangen haben.

2. Damit beschreibt und umgrenzt der Bußgeldbescheid die Tat im prozessualen Sinne ausreichend (§ 41 Abs. 2 S. 1 BDSG, § 71 Abs. 1OWiG, § 264 StPO). […]

V. Die Betroffene hat als Datenverantwortliche schuldhaft gegen Art. 32 Abs. 1 DSGVO verstoßen und ist daher einer Ordnungswidrigkeit nach Art. 83 Abs. 4 lit. a DSGVO schuldig.

1. Gem. Art. 32 Abs. 1 S. 1 DSGVO haben Datenverantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um den mit der Datenverarbeitung einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen zu begegnen. Das zu gewährleistende Schutzniveau muss angemessen sein. Bei der Beurteilung, was angemessen ist, sind der Stand der Technik, die Implementierungskosten und Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Zu den Risiken, denen der Datenverantwortliche zu begegnen hat, gehören nach Art. 32 Abs. 2 DSGVO das Risiko der unbefugten Offenbarung personenbezogener Daten und der unbefugte Zugang zu personenbezogenen Daten.

2. Gegen diese Vorgaben hat die Betroffene verstoßen, indem sie es im Regelfall in ihren Callcentern ausreichen ließ, dass durch die Callcenter-Agenten zur Authentifizierung des Anrufers Name und Geburtsdatum abgefragt wurden. Dies genügte sogar, wenn erkennbar nicht der Kunde selbst, sondern ein Dritter für diesen anrief. Eine solche Authentifizierung gewährleistete unter Berücksichtigung der Kriterien des Art. 32 Abs. 1 DSGVO keinen ausreichenden Schutz der für die Callcenter-Agenten einsehbaren Kundendaten vor der Preisgabe an unberechtigte Anrufer.

a) Die Kommunikation über ein Callcenter ist weitgehend anonym. In der Regel kennen sich der Anrufer und der Callcenter-Agent nicht persönlich. Soweit es um Vertragsangelegenheiten geht und der Callcenter-Agent für die Bearbeitung des Anrufs auf Kundendaten zurückgreifen muss, muss er den Kunden zunächst identifizieren. Soweit bei dem Anruf personenbezogene Daten an den Anrufer preisgegeben werden, muss zudem sichergestellt werden, dass es sich bei dem Anrufer tatsächlich um den Kunden oder einen für diesen berechtigt auftretenden Dritten handelt. Es bedarf daher einer sicheren Methode zur Authentifizierung des Anrufers als an den Daten Berechtigten.

b) Für die Authentifizierung des Anrufers stehen verschiedene Methoden zur Verfügung, die eine unterschiedliche Sicherheit gewährleisten. Zur Auswahl der Methode ist eine Ermittlung und Bewertung der spezifischen Risiken auf der Grundlage der Eintrittswahrscheinlichkeit und der Schwere nachteiliger Folgen für die betroffenen natürlichen Personen durchzuführen. Je sensibler die Daten, je gravierender die möglichen Folgen der unbefugten Datenpreisgabe und je wahrscheinlicher solche Folgen sind, desto höher sind die Anforderungen an ihren Schutz.

c) Die Callcenter-Agenten der Betroffenen hatten keinen Zugriff auf besonders sensible Daten im Sinne von Art. 9 Abs. 1 DSGVO, die besonders zu schützen sind, weil sie höchstpersönlichen bzw. identitätsstiftenden Charakter haben und ihnen deswegen von vornherein ein hohes Schadens- und Diskriminierungspotential innewohnt (vgl. BeckOK, DatenschutzR/Albers/Veit, 33. Ed. 1. 5. 2020, DSGVO Art. 9 Rn. 17, Paal/Pauly/Frenzel, 2. Aufl. 2018, DSGVO Art. 9 Rn. 6). Dies sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Um solche Daten handelte es sich weder unmittelbar, noch ließen sich aus den für die Callcenter-Agenten verfügbaren Daten Rückschlüsse auf solche Daten ziehen.

d) Auch die Risiken für Rechte und Freiheiten natürlicher Personen, die in Erwägung 75 zur DSGVO besonders hervorgehoben werden (Diskriminierung, Identitätsdiebstahl oder -betrug, Rufschädigung etc.), standen vorliegend nicht im Vordergrund. Dies gilt auch, soweit dort Daten betreffend die wirtschaftliche Lage und die Zuverlässigkeit erwähnt sind. Zwar war es den Callcenter-Agenten möglich, in der Z. einzusehen, ob Anschlüsse wegen ausstehender Forderungen gesperrt sind, was Rückschlüsse auf die wirtschaftliche Lage des Kunden erlauben kann. Ungeachtet des Umstandes, dass auch andere Gründe dahinter stehen können als Zahlungsschwierigkeiten, hat Erwägungsgrund 75 den Anwendungsfall im Blick, dass die genannten Aspekte bewertet, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen. Dies erfolgte vorliegend jedoch nicht.

e) Betroffen waren nur wenig sensible Daten, allgemeine Kontaktdaten (Adresse, Telefonnummer und E-Mail-Adresse) sowie die Bankverbindung. Dabei handelt es sich um Daten, die üblicherweise bei Vertragsschlüssen, bei behördlichen Vorgängen oder aus sonstigen Gründen Dritten zur Verfügung gestellt werden. Daneben waren die Vertrags- und Rechnungsdaten sowie die Kundenkorrespondenz in der Z. gespeichert und daher vom Callcenter-Agenten einsehbar, also Daten, die unmittelbar aus dem Vertragsverhältnis mit der Betroffenen stammen und an deren Kenntnisnahme Dritte im Regelfall kein Interesse haben.

f) Die Wahrscheinlichkeit, dass Dritte über das Callcenter der Betroffenen versuchen würden, unberechtigt diese Daten in Erfahrung zu bringen, war dementsprechend gering. Ein massenweiser Zugriff auf die Daten einer Vielzahl von Kunden der Betroffenen durch Einsatz entsprechender Software war über die Kontaktaufnahme mittels Callcenter nicht zu erwarten. Zur Preisgabe der Informationen bzgl. eines Kunden musste der Callcenter-Agent jeweils durch eine geschickte Gesprächsführung überhaupt erst einmal veranlasst werden. Im Vordergrund stand also die Gefahr eines Angriffs auf die Daten individueller Kunden. Insbe-

sondere bestand das Risiko, dass Dritte aus persönlichen Motiven heraus versuchen würden, über das Callcenter Informationen über eine ihnen bekannte Person in Erfahrungen zu bringen.

g) Das Risiko für die Rechte und Freiheiten bestimmter natürlicher Personen ist indes derart erheblich, dass die Daten wirksam geschützt werden mussten.

Gefährdet waren etwa Personen, bei denen ganz allgemein die Gefahr einer unerwünschten Kontaktaufnahme besteht, beispielsweise Personen des öffentlichen Lebens. Es geht aber insbesondere auch um Personen, bei denen ein reelles Risiko besteht, dass sie Opfer von Straftaten werden, sei es durch Nachstellung („Stalking"), Bedrohung oder Freiheitsberaubung. Jenseits dieser persönlichen Gefahren besteht auch stets das Risiko einer Schädigung durch unberechtigten Datengebrauch. So ist denkbar, dass Betrüger über das Callcenter persönliche Informationen, etwa die letzten vier Ziffern der IBAN eines Kunden, in Erfahrung bringen, um diese Daten an anderer – schadensträchtiger – Stelle wiederum zur Authentifizierung zu verwenden. Die insoweit drohenden Gefahren reichen über den Bereich des Lästigen hinaus. Es sind im Einzelfall gravierende materielle und insbesondere immaterielle Schäden denkbar.

Das Risiko, Opfer eines Datenmissbrauchs durch Dritte zu werden, bestand zwar relativ betrachtet nur für einen geringen Anteil der Kunden von K. X. Aufgrund der […] Millionen Kunden war dies jedoch eine durchaus relevante absolute Anzahl. Da K. X. zudem zu den fünf größten Telekommunikationsdienstleistern in Deutschland gehört und nahezu jeder Erwachsene einen Festnetz- und/oder Mobilfunkanschluss hat, musste ein Dritter auch nicht notwendig wissen, dass das avisierte Opfer Kunde von K. ist. Es bestand eine realistische Chance durch „Abtelefonieren" der großen Telekommunikationsunternehmen bei der Betroffenen an die gewünschten Kontaktdaten zu gelangen. Dies unterscheidet die Risikolage für die bei der Betroffenen verarbeiteten Daten von denjenigen kleinerer regionaler Telekommunikationsunternehmen oder denen anderer Branchen.

h) Das zur Tatzeit angewendete Authentifizierungsverfahren der Betroffenen durch Abfrage von Name und Geburtsdatum trug den dargelegten Risiken nicht ausreichend Rechnung.

aa) Name und Geburtsdatum des Kunden stehen einem unüberschaubar großen Personenkreis zur Verfügung. Sie sind im Familien-, Bekannten- und Kollegenkreis vielfach bekannt oder verfügbar. Bei vielen Personen sind Name und Geburtsdatum darüber hinaus auch einfach zu ermitteln, beispielsweise im Internet zu finden, etwa bei Prominenten über C2 oder über soziale Netzwerke wie etwa Y2. Da Name und Geburtsdatum daher nicht nur im Wissens- oder Zugriffsbereich des Kunden stehen, ist das Erfragen dieser Informationen nicht ausreichend, um sicherzustellen, dass der Anrufende der im System erfasste Vertragspartner ist.

bb) Erst Recht sind die Daten ungeeignet, eine Vermutung für eine Berechtigung/Vertretungsmacht des Anrufenden zu begründen, wenn Anrufender und Kunde erkennbar personenverschieden sind, weil ein Dritter im Namen des Kunden anruft. Dass andere Personen Kenntnis von Namen und Geburtsdatum des Kunden haben, impliziert schon nicht, dass diesen die Informationen bewusst preisgegeben wurden, und selbst eine bewusste Weitergabe des Geburtsdatums beinhaltet – auch im Familien- und Freundeskreis – keine Erteilung einer Vertretungsmacht. Die Betroffene hatte aus ihrer vertraglichen Beziehung zum Kunden heraus auch keinerlei Informationen über die jeweiligen familiären Verhältnisse, weswegen es den Agenten im Callcenter nicht möglich war, zu verifizieren, ob der behauptete Angehörige nach der Familienstruktur des Kunden überhaupt existiert. Durch die Möglichkeit von Anrufen durch Dritte war die Gefahr eines Missbrauch zudem erhöht, weil es diesen besonders leicht möglich war, durch das Vorgeben von Wissenslücken und Unsicherheiten den Callcenter-Agenten zur Preisgabe der hinterlegten Informationen zu veranlassen, ohne bei diesen damit einen Missbrauchsverdacht zu erregen.

i) Der Betroffenen wäre es ohne nennenswerten Aufwand möglich gewesen, den Sicherheitsstandard zu erhöhen. Bereits durch das zusätzliche Abfragen von Spezialwissen, etwa der Kunden- oder Rechnungsnummer, wäre die Annahme, dass der Anrufende tatsächlich der Kunde oder ein Berechtigter ist, belastbarer gewesen. Denn auf diese Daten haben regelmäßig nur der Kunde selbst oder sein nahes Umfeld Zugriff. Der Kreis derjenigen, die sich unberechtigt beim Callcenter authentifizieren konnten, wäre damit bereits erheblich verkleinert worden. Da diese Daten für die Callcenter-Agenten bereits seinerzeit einsehbar waren, hätte es lediglich einer Information der Callcenter-Agenten und einer Überarbeitung der entsprechenden Schulungsunterlagen oder Schulungen bedurft, um das Schutzniveau zu erhöhen. Dies wäre mit einem einmaligen und äußerst geringen finanziellen Aufwand möglich gewesen.

2. a) Bei der Betroffenen kannte man das konkrete Schutzniveau im Callcenter und unterlag keiner Fehlvorstellung in tatsächlicher Hinsicht. Im Sinne einer Tatsachenkenntnis handelte das Unternehmen K. X. vorsätzlich. Indes geht die Kammer nicht davon aus, dass die zuständigen Mitarbeiter des Unternehmens sich der Zuwiderhandlung gegen Art. 32 DSGVO oder deren Möglichkeit bewusst waren. Denn in der Vergangenheit hatte es keine Beanstandungen durch Aufsichtsbehörden oder Dritte gegeben. Ein Missbrauch ihrer Callcenter war K. X. auch nicht bekannt geworden. Zudem waren in Fachzeitschriften oder Büchern zum Datenschutzrecht die Anforderungen an die Authentifizierung im Callcenter nicht näher behandelt worden.

b) Der darin liegende Verbotsirrtum und damit der Datenschutzverstoß waren für das Unternehmen K. X. jedoch vermeidbar.

aa) Bei einem Telekommunikationsunternehmen wie der Betroffenen ist das Callcenter für den persönlichen Kontakt mit dem Kunden die primäre Anlaufstelle. Es ist daher erforderlich, das Datenschutzniveau im Bereich des Callcenters anlassbezogen und zudem in regelmäßigen Abständen auf den Prüfstand zu stellen. Dies ergibt sich bereits daraus, dass das Datenschutzrecht nicht statisch ist, sondern sich der Stand der Technik auch und gerade im Hinblick auf neue Risiken fortentwickelt. In Art. 32 Abs. 1 lit. d DSGVO wird dementsprechend nunmehr auch ausdrücklich eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung verlangt. Erst recht gab die Reform des europäischen Datenschutzrechtes durch die Einführung der DSGVO Anlass, die Datenverarbeitungsprozesse auf Konformität mit dem neuen Gesetz zu überprüfen. Dafür stand eine fast zweijährige Übergangsphase zur Verfügung. Im Zuge dessen hätte die Betroffene überprü-

fen müssen, ob das Datenschutzniveau im Callcenter ausreichend ist oder ob Anpassungs- und Nachbesserungsbedarf besteht. Die Authentifizierung von Anrufern war dabei eine der zentralen Fragestellungen.

bb) Die Übergangsphase zur Einführung der DSGVO hat K. X. nicht genutzt. Bei einer entsprechenden Überprüfung hätte das Unternehmen die gleichen Erwägungen anstellen müssen wie die Kammer. Eine ähnlich gewissenhafte Prüfung anhand der Kriterien des Art. 32 DSGVO hätte zu dem Ergebnis geführt, dass der Authentifizierungsprozess nachzubessern ist. Die hierfür notwendige Sachkunde bestand auf Seiten von K. X. Das Unternehmen verfügt über eine eigene Rechtsabteilung, ist als Telekommunikationsunternehmen täglich mit Fragen des Datenschutzes befasst und muss in diesem Bereich besondere Kompetenzen haben. Wären Zweifel verblieben, hätte der BfDI als zuständige Aufsichtsbehörde zur Verfügung gestanden, um die Zweifelsfragen verlässlich zu klären. Der Verstoß wäre dadurch vermieden worden.

V. Bei der Bußgeldbemessung hat sich die Kammer von folgenden Erwägungen leiten lassen:

1. Der Bußgeldrahmen ist Art. 83 Abs. 4 DSGVO zu entnehmen. Gem. dessen lit. a kann bei einem Verstoß gegen Art. 32 DSGVO eine Geldbuße von bis zu 10 Millionen Euro verhängt werden. Im Fall eines Unternehmens ist zudem eine Geldbuße von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs möglich, falls dieser Betrag höher ist.

a) Dabei ist nach dem Erwägungsgrund 150 zur DSGVO der funktionale Unternehmensbegriff des europäischen Kartellrechts in Art. 101 und 102 AEUV zugrunde zu legen. Daher kommt es bei der Bestimmung der Obergrenze einer möglichen Geldbuße auf den Gesamtumsatz des K. X. Konzerns als Unternehmen im funktionalen Sinne und nicht auf den Umsatz der K. C. GmbH als formaler Bußgeldadressatin an.

In der deutschen Sprachfassung der DSGVO scheint dieser Auslegung der Art. 4 Nr. 18 DSGVO entgegenzustehen. Dort wird der Begriff „Unternehmen" dahin legal definiert, dass es sich um die natürliche oder juristische Person handele, die eine wirtschaftliche Tätigkeit ausübt. Diese Definition des Begriffs „Unternehmen" im Sinne des einzelnen Rechtsträgers ist für Art. 83 DSGVO nicht einschlägig. Dies zeigt ein Vergleich mit anderen Sprachfassungen. In der englischen Sprachfassung wird in Art. 4 Nr. 18 das Unternehmen als „enterprise" legaldefiniert und in Art. 83 Abs. 5 mit „undertaking" ein anderer Begriff verwendet, der mit dem englischsprachigen Erwägungsgrund 150 übereinstimmt. Auch im Bulgarischen, Dänischen, Gälischen, Kroatischen und Slowenischen wird bei Art. 83 DSGVO nicht auf den legaldefinierten Begriff des Unternehmens aus Art. 4 Nr. 18 zurückgegriffen (vgl. hierzu weitergehend BeckOK DatenschutzR/Holländer, 32. Ed. 1. 11. 2019, DSGVO Art. 83 Rn. 13 - 13.3; Cornelius, Die „datenschutzrechtliche Einheit" als Grundlage des bußgeldrechtlichen Unternehmensbegriff nach der EU-DSGVO, NZWiSt 2016, 421, 423 f.). Daraus ergibt sich, dass der Verordnungsgeber im hiesigen Kontext den Begriff des Unternehmens im Sinne des Erwägungsgrundes 150 versteht.

b) Die Frage, an welches Ereignis das vorangegangene Geschäftsjahr anknüpft, dessen Umsatz die Obergrenze der möglichen Geldbuße bestimmt, ist nicht ausdrücklich geregelt.

Nach der Rechtsprechung des EuGH im Kartellrecht zu dem nahezu gleichlautenden Art. 23 VO Nr. 1/2003 ist der Bezugszeitraum das der Sanktionsverhängung vorausgegangene Geschäftsjahr (EuGH, Urt. v. 26. 1. 2017 – C-637/13 P – Badezimmerkartell Laufen Austria, Rn. 49; EuGH, Urt. v. 4. 9. 2014 – C-408/12 P – YKK u. a. Rn. 90).

Da Art. 83 DSGVO die kartellrechtliche Regelung zum Vorbild hat, ist mithin die Höhe des Jahresumsatzes im letzten abgeschlossenen Geschäftsjahr vor Erlass des Bußgeldbescheides maßgebend. Auf den Zeitpunkt der gerichtlichen Entscheidung kommt es ebenso wenig an wie auf den Zeitpunkt des maßgeblichen Verstoßes.

Da der Bußgeldbescheid am 27. 11. 2019 erlassen wurde, ist mithin der Jahresumsatz für 2018 maßgebend. Auf der Grundlage eines Umsatzes für 2018 von 3,63 Milliarden Euro ergibt sich daraus eine zweiprozentige Obergrenze für die Geldbuße von 72,6 Millionen Euro. Da dieser Betrag höher ist als die alternativ in Art. 83 Abs. 4 DSGVO genannten 10 Millionen Euro, ist diese Obergrenze zugrunde zu legen.

2. Bei der Bemessung der Geldbuße innerhalb dieses Bußgeldrahmens war für die Kammer folgendes maßgebend:

a) Nach Art. 83 Abs. 1 DSGVO stellt jede Aufsichtsbehörde sicher, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. In Art. 83 Abs. 2 S. 2 DSGVO sind Zumessungskriterien aufgeführt, die bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag in jedem Einzelfall „gebührend" zu berücksichtigen sind. Relevant sind danach insbesondere Art, Schwere und Dauer des Verstoßes, die Zahl der von der Verarbeitung betroffenen Personen, das Ausmaß des Schadens, die Kategorie der betroffenen personenbezogenen Daten, das Bemühen des Unternehmens, den Schaden zu begrenzen, Art und Umfang der Kooperation mit den Datenschutzbehörden und der Grad der Verantwortlichkeit.

Der Umsatz des Unternehmens ist in Art. 83 Abs. 2 S. 2 DSGVO nicht als Zumessungsgesichtspunkt genannt. Daraus folgt nicht, dass dem Umsatz des Unternehmens bei der Bemessung der Geldbuße keine Bedeutung zukommt. Zum einen bestimmt der Umsatz bei umsatzstarken Unternehmen die Bußgeldobergrenze und spannt dadurch erst den Rahmen auf, in den der konkrete Datenschutzverstoß einzuordnen und einzupassen ist. Der Bußgeldrahmen gibt der konkreten Zumessung die notwendige Orientierung. Zum anderen müssen Geldbußen gegen Unternehmen gem. Art. 83 Abs. 1 DSGVO wirksam und abschreckend sein. Dies richtet sich auch nach der Ahndungsempfindlichkeit des jeweiligen Unternehmens. Je größer das Unternehmen ist, desto geringer ist regelmäßig die Ahndungsempfindlichkeit und desto höher ist im Regelfall das Bußgeld zu bemessen, damit es seine spezialpräventive Wirkung entfalten kann. Die Höhe des Umsatzes ist für die Unternehmensgröße und damit für die Ahnungsempfindlichkeit ein geeigneter Indikator; der Bilanzgewinn und sonstige Kennzahlen der wirtschaftlichen Leistungsfähigkeit des Unternehmens können zusätzlich berücksichtigt werden.

b) Es darf jedoch nicht aus dem Blick geraten, dass die DSGVO in Art. 83 Abs. 2 S. 2 in erster Linie tatbezogene Gesichtspunkte für die Bemessung aufführt. Eine Bemessung des Bußgeldes durch Ermittlung eines sich nach dem Umsatz richtenden Grundwertes für das Bußgeld, welcher je nach Schwere des Datenschutzverstoßes mit einem Fak-

tor multipliziert wird, ist aus diesem Grund und wegen der damit einhergehenden Fokussierung auf den Unternehmensumsatz problematisch. Einen solchen Ansatz hat der BfDI in Anlehnung an das Bußgeldkonzept der Datenschutzkonferenz vom 19. 10. 2019 bei der Bußgeldbemessung verfolgt. Eine solche Bemessungsmethode mag bei Datenschutzverstößen von mittlerem Gewicht zu angemessenen Ergebnissen führen. Sie versagt jedoch bei schweren Datenschutzverstößen umsatzschwacher Unternehmen und leichten Datenschutzverstößen umsatzstarker Unternehmen, also in denjenigen Fällen, in denen eine maßgeblich am Umsatz orientierte Zumessung in Widerstreit gerät zu der Zumessung anhand der Kriterien in Art. 83 Abs. 2 S. 2 DSGVO. Hier haben die tatbezogenen Zumessungsgesichtspunkte in Art. 83 Abs. 2 S. 2 DSGVO Vorrang. Der Umsatzhöhe kommt zwar weiterhin Bedeutung zu. Im Verhältnis zur Tatschuld verliert der Umsatz jedoch umso mehr an Bedeutung, desto eindeutiger die Bewertung der Schwere des Datenschutzverstoßes anhand der tatbezogenen Umstände in die eine oder andere Richtung ausfällt.

c) Für schwere Datenschutzverstöße umsatzschwacher Unternehmen ergibt sich dies aus Art. 83 Abs. 4 DSGVO selbst. Dieser enthält gerade keine allgemein am Umsatz orientierte Bußgeldobergrenze. Vielmehr ist eine Obergrenze von 10 Millionen Euro vorgesehen, die bei sehr umsatzstarken Unternehmen erhöht wird. Der europäische Gesetzgeber ermöglicht es daher den Aufsichtsbehörden und Gerichten, bei schweren Datenschutzverstößen auch gegen umsatzschwache Unternehmen hohe, gegebenenfalls auch existenzbedrohende Geldbußen zu verhängen.

d) Bei gering gewichtigen Datenschutzverstößen umsatzstarker Unternehmen ist eine maßgebliche Orientierung am Umsatz bei der Zumessung der Geldbuße in gleicher Weise nicht sachgerecht. Eine Geldbuße muss gem. Art. 83 Abs. 1 DSGVO zwar wirksam und abschreckend sein. Beide Gesichtspunkte verlieren bei Datenschutzverstößen von geringem Gewicht aber an Bedeutung. Zudem muss die Geldbuße nach Art. 83 Abs. 1 DSGVO stets auch verhältnismäßig sein. Mit anderen Worten: Die Geldbuße muss spürbar sein; sie darf jedoch nicht als unangemessene Härte im Sinne einer überzogenen Reaktion auf den konkreten Verstoß erscheinen.

e) Bei dem Verstoß der Betroffenen gegen Art. 32 DSGVO handelt es sich um einen Datenschutzverstoß mit einem deutlichen Überwiegen mildernder Gesichtspunkte. Denn es ist zu berücksichtigt, dass

- keine sensiblen Daten betroffen waren;
- es nur in dem einen Fall nachweisbar zu der Schädigung eines Kunden gekommen ist, wobei allerdings relativierend zu berücksichtigen ist, dass Fälle eines Datendiebstahls über das Callcenters nicht stets bekannt werden;
- K. nicht absichtlich, bewusst oder auch nur bedingt vorsätzlich gegen das Datenschutzrecht verstoßen hat;
- man vielmehr davon ausgegangen ist, dass der Authentifizierungsprozess gesetzeskonform ist, auch wenn diese Fehlvorstellung vermeidbar war;
- es keine Vorgaben für die Authentifizierung in Callcentern gab;
- ein niedriges Sicherheitsniveau auch deswegen bestand, damit die Kunden ohne größere Hindernisse mit dem Callcenter in Kontakt treten konnten;
- die Betroffene umfassend mit dem BfDI kooperiert hat und unverzüglich das Schutzniveau des Authentifizierungsprozesses erhöht und in Abstimmung mit dem BfDI letztendlich eine Service-PIN eingeführt hat;
- gegen K. erstmals wegen eines Datenschutzverstoßes eine Geldbuße verhängt wird.

Zwar waren abstrakt […] Millionen Kundendaten von K. betroffen. Es drohte jedoch kein Massendiebstahl von Kundendaten, sondern die Daten konnten von Angreifern nur im Einzelfall durch eine geschickte Gesprächsführung über das Callcenter in Erfahrung gebracht werden. Im Vordergrund standen dabei persönliche Motive. Real drohten nur einer geringen, wenn auch angesichts der Größe des Kundenstamms von K. relevanten Anzahl von Kunden durch die schwache Authentifizierung Nachteile.

Auch ist zu berücksichtigen, dass durch den öffentlichkeitswirksamen Erlass des Bußgeldbescheides ein Reputationsschaden bei K. eingetreten ist. Aufgrund der Höhe des zunächst verhängten Bußgeldes ist in der Öffentlichkeit der Eindruck entstanden, als handele es sich um einen – auch und gerade was das Verschulden anbelangt – gewichtigen Datenschutzverstoß. Dies ist indes nicht der Fall.

Unter umfassender Abwägung aller zumessungserheblichen Umstände hat die Kammer trotz des hohen Bußgeldrahmens eine gegenüber dem Bußgeldbescheid deutlich geringere Geldbuße in Höhe von 900 000 Euro als tat- und schuldangemessen angesehen. Diese ist wirksam, verhältnismäßig und bei Kenntnis der vielen mildernden Gesichtspunkte auch ausreichend abschreckend. […]

Kommentar

DSGVO-Geldbuße unverhältnismäßig

Sandra Brechtel und RA Dr. Hauke Hansen, LL. M.*

I. Einleitung

Mit großer Spannung wurde das erste Urteil eines deutschen Gerichtes zu einem DSGVO-Millionenbußgeld erwartet. Nachdem die Datenschutzbehörden der europäischen Nachbarstaaten[1] bereits früh empfindliche Bußgelder gegen Unternehmen verhängten, hielten sich die deutschen Datenschutzbehörden bei der Bemessung von Bußgeldern zunächst zurück.[2]

* Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 7. 1. 2020.

1 Frankreich: 50 Mio. EUR gegen Google, https://www.zeit.de/digital/datenschutz/2019-01/frankreich-datenschutzbehoerde-cnil-google-strafe-dsgvo?utm_referrer=https%3A%2F%2Fwww.google.com%2F; Großbritannien: 110 Mio. EUR gegen die Hotelkette Marriott, https://www.spiegel.de/netzwelt/netzpolitik/dsgvo-hotelkette-marriott-drohen-110-millionen-euro-bussgeld-a-1276615.html und 204 Mio. EUR gegen British Airways, https://www.manager-magazin.de/unternehmen/industrie/dsgvo-british-airways-soll-200-millionen-zahlen-a-1276303.html.

2 20 000 EUR gegen Knuddels, https://www.lto.de/recht/nachrichten/n/knuddels-datenschutz-hacker-bussgeld-kooperation/#:~:text=Das%20Chat%2DPortal%20Knuddels.de,der%20Datenschutzbeh%C3%B6rde%20zu%20verdanken%20ist; knapp 200 000 EUR gegen DeliveryHero, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf.

II. Das Konzept der DSK zur Zumessung von Bußgeldern wegen Datenschutzverstößen

Dies änderte sich, nachdem die Datenschutzkonferenz, ein Zusammenschluss aller unabhängigen Datenschutzbehörden des Bundes und der Länder (kurz: DSK), im Oktober 2019 ein Konzept zur Berechnung von Bußgeldern bei Datenschutzverstößen[3] veröffentlichte. In der Folgezeit hat sich auch in Deutschland die Höhe der verhängten Bußgelder drastisch erhöht.[4]

1. Die Formel

Das Modell sieht die Zumessung der Bußgeldhöhe in fünf Schritten vor:

(1) Zuordnung des betroffenen Unternehmens in eine von vier Größenklassen (Gruppe A: bis 2 Mio. EUR weltweiter Umsatz im Vorjahr bis Gruppe D: über 50 Mio. EUR Jahresumsatz); innerhalb dieser vier Gruppen erfolgt noch eine Zuordnung in Untergruppen.

(2) Bestimmung des mittleren Jahresumsatzes der jeweiligen Untergruppe.

(3) Ermittlung des wirtschaftlichen Grundwertes: Hierbei handelt es sich um einen Tagessatz, der sich aus dem mittleren Jahresumsatz geteilt durch 360 (Tage) ergibt.

(4) Multiplikation des Grundwertes mit einem Faktor. Anhand der konkreten Umstände des Einzelfalls erfolgt eine Einordnung der Tat in leicht, mittel, schwer oder sehr schwer (vgl. Art. 83 Abs. 2 S. 2 DSGVO). Diesen vier Schweregraden werden abhängig von der Art des Verstoßes Faktoren zugeordnet: 1 bis 6 bei formellen Verstößen gemäß Art. 83 Abs. 4 DSGVO, 1 bis 12 bei materiellen Verstößen gemäß Art. 83 Abs. 5 und 6 DSGVO; beides mit der Option, im Falle sehr schwerer Verstöße den Faktor nochmals zu erhöhen.

(5) Anpassung des unter Ziffer vier errechneten Bußgeldes anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände, z. B. die Kriterien aus Art. 83 Abs. 2 DSGVO oder die drohende Zahlungsunfähigkeit des Unternehmens.

2. Problem der Verhältnismäßigkeit

Das auf der Grundlage dieses Berechnungsmodells verhängte Millionen-Bußgeld wurde vom LG Bonn zwar im Grundsatz bestätigt, aber erheblich reduziert. Die Bonner Richter kritisierten die maßgebliche Orientierung am Umsatz bei der Bemessung der Geldbuße (vgl. oben Ziffer (1) des Konzeptes). Denn insbesondere bei leichten Datenschutzverstößen umsatzstarker Unternehmen sowie bei schweren Datenschutzverstößen umsatzschwacher Unternehmen führe diese nicht zu sachgerechten Ergebnissen. Das Bußgeld sei in erster Linie an den tatbezogenen Kriterien des Art. 83 Abs. 2 S. 2 DSGVO zu messen. Nur so könne die Verhältnismäßigkeit des Bußgeldes gewahrt werden.

Trotz dieser Kritik sah sich der Bundesdatenschutzbeauftragte durch das vorliegende Urteil bestätigt und formuliert in seiner Pressemitteilung[5] kämpferisch: „Ich bin überzeugt, dass diese Entscheidung in den Chefetagen von Unternehmen wahrgenommen wird. Ich warte noch auf die schriftliche Begründung des Urteils, aber klar ist schon jetzt: Kein Unternehmen kann es sich mehr leisten, den Datenschutz zu vernachlässigen." Allerdings wird er Presseberichten zufolge das Urteil zum Anlass nehmen, zusammen mit den übrigen Datenschutzbehörden das Bußgeldberechnungsmodell zu überarbeiten.

III. Reichweite der Unternehmenshaftung

Mit dem vorliegenden Urteil wurde nicht nur das Berechnungsmodell der DSK erheblich entschärft. Das Landgericht positionierte sich gleichzeitig zu der sehr umstrittenen Frage der Reichweite der Unternehmenshaftung für Datenschutzverstöße: Im Datenschutzrecht gelte die unmittelbare Verbandshaftung, die sich aus den Grundsätzen des supranationalen Kartellsanktionsrechts (Artt. 101, 102 AEUV) ableite. Das Unternehmen hafte demnach uneingeschränkt. Auf das nachweisbare Fehlverhalten eines leitenden Angestellten, wie es das Ordnungswidrigkeitenrecht in § 30 Abs. 1 OWiG vorsieht, komme es nicht an.

1. Unmittelbare Verbandshaftung des EU-Kartellsanktionsrechts

Im EU-Kartellsanktionsrecht (Artt. 101, 102 AEUV) wird der Unternehmensbegriff funktional verstanden.[6] Umfasst wird nach st. Rspr. jede, eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung.[7] Damit kann ein Unternehmen im kartellsanktionsrechtlichen Sinn aus mehreren natürlichen oder juristischen Personen, Verbänden oder auch Unternehmensvereinigungen bestehen, soweit sie wirtschaftlich tätig sind.[8] Unter den Unternehmensbegriff fallen demnach nicht nur die Einzelunternehmen eines Konzerns, sondern der Konzern als Ganzes. Muttergesellschaften haften gemeinsam mit ihren untergeordneten Gesellschaften gesamtschuldnerisch für Kartellrechtsverstöße.[9] Für die Haftung des Unternehmens ist danach jedes Fehlverhalten einer für das Unternehmen handelnden Person ausreichend. Die für das Unternehmen konkret handelnde Person muss nicht identifiziert werden.[10] Ausgenommen ist die Haftung des Unternehmens lediglich dann, wenn die für das Unternehmen handelnde Person klar die Grenzen ihrer Kompetenzen überschreitet und dieses Verhalten dem Unternehmen

3 https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf.

4 14,5 Mio. EUR gegen die Deutsche Wohnen, https://www.lto.de/recht/kanzleien-unternehmen/k/dsgvo-verstoss-deutsche-wohnen-bussgeld-datenschutz-berlin/; 9,55 Mio. EUR gegen die 1&1 Telecom GmbH, https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html; 35,3 Mio. EUR gegen H&M, https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren; 1,24 Mio. EUR gegen AOK, https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung/.

5 https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/28_Urteil-1und1.html.

6 *Kersting*, WuW 2014, 1156; *Cornelius*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XIV., Rn. 90; *Weiß*, in: Calliess/Ruffert, Kommentar AEUV, 5. Aufl. 2016, Art. 101 Rn. 25.

7 EuGH, 10. 4. 2014 – C-231/11 P und C-233/11 P, NZKart 2014, 177, Rn. 43 – Kommission/Siemens m. w. N.; EuGH, 20. 1. 2011 – C-90/09 P, BeckRS 2011, 80061, Rn. 34 – General Quimica; EuG, 4. 3. 2003 – Rs. T-319/99, BeckRS 9998, 155908 Rn. 35 – FENIN m. w. N.

8 EuGH, 10. 4. 2014 – C-231/11 P und C-233/11 P, NZKart 2014, 177, Rn. 43 – Kommission/Siemens; EuGH, 20. 1. 2011 – C-90/09 P, BeckRS 2011, 80061, Rn. 35 – General Quimica.

9 EuGH, 10. 4. 2014 – C-231/11 P und C-233/11 P, NZKart 2014, 177, 178, Rn. 46 – Kommission/Siemens; EuGH, Schlussanträge der Generalanwältin v. 29. 11. 2012 – C-440/11 P, NZKart 2013, 28, Rn. 23 – Kommission/Stichtig Administratiekantoor Portielje; Kersting, WuW 2014, 1156.

10 *Faust/Spittka/Wybitul*, ZD 2016, 120, 121 m. w. N. *Weiß*, in: Calliess/Ruffert (Fn. 6), Rn. 72; *Holländer*, in: Wolff/Brink, BeckOK DatenschutzR, 34. Ed. 1. 8. 2020, DSGVO Art. 83, Rn. 11.

nicht anderweitig, etwa durch Duldung, zugerechnet werden kann.[11]

2. Abgrenzung zur Haftung im Ordnungswidrigkeitenrecht

Deutlich höhere Anforderungen stellt das deutsche Ordnungswidrigkeitenrecht an die Haftung von Unternehmen für Rechtsverstöße von Personen, die für das Unternehmen handeln. Die Haftung knüpft hier an ein Fehlverhalten einer Leitungsperson an (vgl. § 30 Abs. 1 OWiG). Eine umfassende Haftung von Unternehmen für Rechtsverstöße von allen für das Unternehmen tätig werdenden Personen, wie es die Artt. 101, 102 AEUV vorsehen, besteht nicht.

Der Nachweis des Fehlverhaltens einer Leitungsperson ist in aller Regel mit erheblichen Schwierigkeiten verbunden. Ohne diesen Nachweis dürf(t)en Aufsichtsbehörden keine Bußgelder gegen das betroffene Unternehmen verhängen. Damit würden die Bußgeldvorschriften der DSGVO ihren Sanktionsdruck einbüßen.

3. EU-Kartellsanktionsrecht vs. Ordnungswidrigkeitenrecht

Die Reichweite der Unternehmenshaftung und damit die Frage, ob bei der Verhängung von Geldbußen nach Art. 83 Abs. 4 - 6 DSGVO der § 30 Abs. 1 OWiG und das deutsche Rechtsträgerprinzip oder die Grundsätze des EU-Kartellsanktionsrechts zur Anwendung kommen, ist rechtlich umstritten.[12] Der deutsche Gesetzgeber hat diese Frage nicht eindeutig beantwortet: Nach § 41 Abs. 1 BDSG gelten für Verstöße nach Art. 83 Abs. 4 - 6 DSGVO die materiell-rechtlichen Vorschriften des OWiG „sinngemäß". Der Gesetzgeber hat den Anwendungsvorrang der DSGVO zwar einerseits anerkannt, indem nur eingeschränkt auf die Vorschriften des OWiG verwiesen wird – nämlich „soweit dieses Gesetz nichts anderes bestimmt". Andererseits hat der Gesetzgeber in § 41 Abs. 1 S. 2 BDSG bestimmte Vorschriften ausdrücklich von der Verweisung ausgenommen. § 30 OWiG wurde dort entgegen der Anregung der DSK und entgegen der ersten Fassungen des Referentenentwurfs nicht ausgenommen. Daraus könnte der Schluss zu ziehen sein, der deutsche Gesetzgeber sei von einer Geltung des § 30 OWiG ausgegangen.

Das LG Bonn hat sich dennoch für die Anwendung der Artt. 101, 102 AEUV entschieden. Insbesondere würde die Anwendung des nationalen Ordnungswidrigkeitenrechts zu einer unterschiedlichen Sanktionspraxis innerhalb der EU führen und damit der vom europäischen Gesetzgeber vorgesehenen einheitlichen und effektiven Sanktionierung von Datenschutzverstößen entgegenstehen.[13]

Mit der zum Unternehmensbegriff vertretenen Kritik auf gesellschafts- und verfassungsrechtlicher Ebene[14] und deren Auswirkungen auf die Anwendbarkeit des Begriffes im Datenschutzrecht hat sich das Gericht allerdings nicht auseinandergesetzt.

IV. Prozessuales

Gemäß Art. 58 Abs. 2 lit. i DSGVO sind die Aufsichtsbehörden zur Verhängung von Geldbußen nach Art. 83 DSGVO befugt. Die Aufsichtsbehörde ist damit zugleich nach § 35 Abs. 1 OWiG als Verwaltungsbehörde für die Verfolgung von datenschutzrechtlichen Ordnungswidrigkeiten zuständig. Für das datenschutzrechtliche Bußgeldverfahren gelten dennoch andere Regeln als für das herkömmliche Verwaltungsverfahren. Gemäß §§ 41 Abs. 2 S. 1 BDSG-2018 sind auf datenschutzrechtliche Bußgeldverfahren die Bestimmung des OWiG und der StPO anwendbar. Einsprüche richten sich gemäß § 71 Abs. 1 OWiG nach den Vorschriften der StPO. Dem Betroffenen stehen damit besondere Verfahrensrechte, z. B. das Recht, sich vor dem Abschluss des Verfahrens zu äußern (§ 55 Abs. 1 OWiG i. V. m. § 163a Abs. 1 StPO), ein Akteneinsichtsrecht (§ 49 Abs. 1 S. 1 OWiG) sowie ein umfassendes Schweigerecht (§ 55 Abs. 1 OWiG i. V. m. §§ 163a S. 2, 136 Abs. 1 S. 2 StPO), zu. Über den Einspruch entscheiden gemäß §§ 41 Abs. 1 S. 3 BDSG-2018 i. V. m. 68 OWiG die Amts- bzw. Landgerichte, abhängig von der Höhe der festgesetzten Geldbuße (Grenze: 100 000 EUR). Die örtliche Zuständigkeit richtet sich gemäß § 68 Abs. 1 S. 1 OWiG nach dem Gerichtsbezirk, in dem die Aufsichtsbehörde ihren Sitz hat. Gegen die Entscheidung über den Einspruch ist die Rechtsbeschwerde nach § 79 OWiG der einzige Rechtsbehelf.

In § 41 BDSG werden einige weitere Normen des OWiG genannt, die beim Vorgehen gegen Bußgelder wegen DSGVO-Verstößen entweder keine oder nur eingeschränkte Anwendung finden. So werden die Akten an das Gericht übermittelt, wenn die Datenschutzaufsichtsbehörde nach dem Einspruch an dem von ihr verhängten Bußgeld festhält. Die Übersendung der Akten erfolgt jedoch nicht direkt an den zuständigen Spruchkörper, sondern gemäß § 69 Abs. 3 S. 1 OWiG zunächst an die Staatsanwaltschaft.

Erst wenn die Staatsanwaltschaft das Verfahren nicht einstellt und auch keine weiteren Ermittlungen durchführt, legt sie die Akten anschließend dem Strafrichter oder der großen Strafkammer vor (§ 69 Abs. 4 S. 2 OWiG). Bei Bußgeldern wegen DSGVO-Verstößen sieht § 41 Abs. 2 S. 3 BDSG allerdings die Besonderheit vor, dass eine Verfahrenseinstellung durch die Staatsanwaltschaft nur mit Zustimmung der Datenschutzaufsichtsbehörde erfolgen kann.

V. Ausblick

Es bleibt abzuwarten, ob sich andere deutsche Gerichte der Entscheidung des LG Bonn anschließen. Auf die nächste Entscheidung wird vermutlich nicht mehr lange zu warten sein. Auch wenn H&M, gegen die das deutschen Rekord-Bußgeld von 35,3 Mio. EUR verhängt wurde,[15] bereits auf Rechtsbehelfe verzichtet hat, hat die Deutsche Wohnen, die bereits im Oktober 2019 von der Berliner Datenschutzbeauftragten ebenfalls mit einem Millionen-Bußgeld belegt wurde,[16] Medienberichten zufolge Einspruch gegen den Bußgeldbescheid erhoben.

---

11 *Faust/Spittka/Wybitul*, ZD 2016, 120, 121 m. w. N.; *Weiß*, in: Calliess/Ruffert (Fn. 6), Rn. 72.

12 Siehe zum Streitstand die Ausführungen des LG Bonn, 11. 11. 2020 – 29 OWi 1/20, K&R 2021, 133, 135, IV. 2. d) m. w. N.

13 LG Bonn, 11. 11. 2020 – 29 OWi 1/20, K&R 2021, 133, 135, IV. 2. e).

14 Vgl. *Kersting*, WuW 2014, 1156 m. w. N.

15 Vgl. Pressemitteilung des Hamburgischen Beauftragten für Datenschutz und Informationssicherheit vom 1. 10. 2020, https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren.

16 Vgl. Pressemitteilung der Berliner Beauftragten für Datenschutzinformationssicherheit vom 5. 11. 2019, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf.