Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

10
K&R

23. Jahrgang Oktober 2020 Seiten 637 – 708

dfv Mediengruppe · Frankfurt am Main

mit in anderen Datenbanken des Verantwortlichen gespeicherten Klarinformationen verglichen werden. Ein derartiger Aufwand ist einem Verantwortlichen – auch bei Berücksichtigung des großen Interesses des jeweiligen Betroffenen an der Umsetzung der durch den Betroffenen geltend gemachten Rechte – kaum zumutbar. Außerdem ist zu berücksichtigen, dass auch in dem beschriebenen Sachverhalt die tatsächliche Vornahme einer Verknüpfung der pseudonymisierten Daten mit über den Betroffenen gespeicherten Klardaten unwahrscheinlich ist, da eine solche mittels rein automatisierter Prozesse zumeist nicht einfach umsetzbar ist.

III. Abschließende Bewertung der Vorschrift

Der Europäische Gesetzgeber hat mit der Vorschrift in Art. 11 Abs. 2 DSGVO eine sehr sinnvolle Regelung mit großer Praxisrelevanz geschaffen. Diese berücksichtigt sowohl das Interesse der Betroffenen an der Umsetzung der von ihnen geltend gemachten Betroffenenrechte als auch die im Rahmen dieser Umsetzung auf Seiten der Verantwortlichen bestehenden Herausforderungen. Im Online-Bereich kommt eine Anwendbarkeit der Regelung in Art. 11 Abs. 2 DSGVO insbesondere bei einer Verarbeitung pseudonymer Daten in Betracht. Durch die Vornahme von Pseudonymisierungen können die Grundrechte und Grundfreiheiten von Betroffenen in einem erheblichen Maße geschützt werden. Die Vorschrift in Art. 11 Abs. 2 DSGVO soll einen Anreiz für eine (gegebenenfalls über das Gesetz hinaus gehende) Pseudonymisierung von Daten schaffen. Ein solcher Anreiz wäre bei einer (zu) restriktiven Auslegung der Vorschrift in Art. 11 Abs. 2 DSGVO nicht gegeben. Diesbezüglich ist auch zu berücksichtigen, dass die Praxis gezeigt hat, dass es insbesondere aus Sicht der Betroffenen sinnvoller ist, dass Verantwortliche Datenverarbeitungen z. B. auf die Rechtsgrundlage in Art. 6 Abs. 1 lit. f DSGVO stützen und die hierbei vorzunehmende Interessenabwägung aufgrund der Verarbeitung pseudonymer Daten zu ihren Gunsten ausfällt,[22] als dass die Verantwortlichen für die Rechtfertigung der Datenverarbeitungen eine Einwilligung einholen. Insbesondere für den Online-Bereich ist nämlich festzustellen, dass Betroffene die Inhalte von Einwilligungen – z. B. für die Erhebung/Verarbeitung von Trackingdaten – gar nicht ausreichend wahrnehmen, bevor sie eine Einwilligung erteilen („click-fatigue“).

22 Dazu, dass die Vornahme von Pseudonymisierungen zur Folge haben kann, dass eine vorzunehmende Interessenabwägung zugunsten des Verantwortlichen ausfällt, vgl. beispielhaft die Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (Stand Mai 2019), Seite 14.

RA Stefan Hessel und Dipl.-Jur. Karin Potel, Saarbrücken*

Catch Me If You Can – Die Widersprüche der DSGVO bei Verantwortlichkeit und Bußgeldbemessung im Konzernkontext

Datenschutzaufsichtsbehörden verhängen gegen Unternehmen immer wieder Bußgelder wegen Verstößen gegen die DSGVO. Gerade im Konzernkontext erreichen die Bußgelder dabei wegen einer Anwendung des Funktionsträgerprinzips schnell ein Rekordniveau. Rechtlich ist dessen Anwendung jedoch, wie der folgende Beitrag zeigt, keineswegs unproblematisch, da innerhalb der DSGVO Widersprüche zwischen Bußgeldadressat und Bemessungskriterien bestehen.

I. Problemstellung

Ob das 200 Millionen Euro Bußgeld gegen British Airways oder die 50 Millionen Euro gegen Google – immer wieder werden von den Aufsichtsbehörden Rekordbußgelder wegen Datenschutzverstößen verhängt. Rechtsgrundlage für die Verhängung von Bußgeldern gegen Verantwortliche oder Auftragsverarbeiter ist Art. 83 DSGVO. Abhängig von der Art und Schwere des Verstoßes können diese bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes des Unternehmens betragen. Regelungen zu ihrer Bemessung finden sich unter anderem in Art. 83 Abs. 2 DSGVO. Hinweise zur Umsatzermittlung, welche für die Bußgeldhöhe besonders relevant ist, finden sich in ErwGr. 150 DSGVO. Danach ist der funktionale Unternehmensbegriff der Art. 101 und 102 AEUV als Grundlage für die Ermittlung des Jahresumsatzes heranzuziehen. Dies stellt insbesondere Konzerne, als Zusammenschlüsse von Unternehmen im Sinne des Art. 4 Nr. 19 DSGVO i. V. m. ErwGr. 37 DSGVO, vor Herausforderungen. So kann, wie der folgende Beitrag zeigt, eine Tochtergesellschaft Verantwortlicher und damit Adressat eines Bußgeldes sein, während für die Bußgeldbemessung der Jahresumsatz der Konzernmutter herangezogen wird.

II. Datenverarbeitung im Konzern

1. Grundlagen der datenschutzrechtlichen Verantwortlichkeit

Anlass für die Verhängung eines Bußgeldes nach Art. 83 Abs. 4 bis Abs. 6 DSGVO ist stets eine Verletzung des Datenschutzrechts. Dessen Einhaltung obliegt nach Art. 5 Abs. 2 DSGVO i. V. m. Art. 24 Abs. 1 DSGVO in erster Linie dem Verantwortlichen. Neben dem Verantwort-

* Die Grundlagen für diesen Beitrag wurden durch das Projekt „EVAREST“ im Rahmen einer strategischen Einzelförderung des Bundeswirtschaftsministeriums finanziert. Weitere Informationen zum Forschungsvorhaben finden Sie unter www.evarest.de. Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 14. 9. 2020.

lichen können nach Art. 28 Abs. 1 DSGVO auch den Auftragsverarbeiter datenschutzrechtliche Verpflichtungen treffen. Diesem kommt innerhalb der DSGVO jedoch – insbesondere bei seiner Inanspruchnahme durch die Aufsichtsbehörden – eine untergeordnete Rolle zu.[1] Bezugspunkt für die Beurteilung, wer verantwortlich für die Datenverarbeitung ist und wer gegebenenfalls Daten im Auftrag verarbeitet, ist der jeweilige Verarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DSGVO.[2]

2. Anwendung der Grundsätze auf den Konzern

Bei der Anwendung der dargestellten Grundsätze auf den Konzern ergibt sich zunächst, dass eine ausschließliche Verantwortlichkeit der Muttergesellschaft für die gesamte Datenverarbeitung im Konzern regelmäßig nicht in Betracht kommt.[3] Dies folgt daraus, dass die Tochtergesellschaften zwar von der Konzernmutter beherrscht werden, letztere aber gleichwohl nicht in jedem Fall über die Zwecke und Mittel der Datenverarbeitung entscheidet.[4] Stattdessen ergeben sich bei Konzernen abhängig vom jeweiligen Verarbeitungsvorgang unterschiedliche Konstellationen.[5] Für eine Datenübermittlung innerhalb des Konzerns existiert grundsätzlich kein Privileg. Aus Art. 6 Abs. 1 S. 1 lit. f DSGVO i. V. m. ErwGr. 48 DSGVO kann jedoch im Rahmen eines berechtigten Interesses ein sog. kleines Konzernprivileg abgeleitet werden. Neben diesem können auch andere Rechtsgrundlagen, etwa eine Einwilligung des Betroffenen zur Weitergabe oder auch zur Erfüllung eines Vertrages, einen Datenaustausch erlauben. Besteht eine Rechtsgrundlage zur Übermittlung, sind abhängig von der jeweiligen datenschutzrechtlichen Konstellation bestimmte formelle Voraussetzungen, beispielsweise ein Vertrag zur Auftragsverarbeitung, zu erfüllen. Insgesamt lässt sich festhalten, dass datenschutzrechtliche Verantwortung und die damit einhergehenden Verpflichtungen innerhalb eines Konzerns abhängig vom Verarbeitungsvorgang höchst unterschiedlich ausgestaltet sein können.

3. Zurechnung des Handelns von natürlichen Personen

Darüber hinaus ist innerhalb der Mutter- und Tochtergesellschaften eine Klärung der Verantwortlichkeit erforderlich.[6] Juristische Personen können nicht selbst handeln, sodass es der Zurechnung des Handelns ihrer Mitarbeiter und Angestellten bedarf. Eine Zurechnung des Handelns natürlicher Personen gegenüber einer juristischen Person ist nicht anlasslos möglich, sondern bedarf einer rechtlichen Grundlage, etwa einer gesetzlichen Regelung oder eines Rechtsscheins.

a) Zurechnung über das OWiG

Dazu wird teilweise vertreten, dass die DSGVO selbst keine Zurechnungsvorschriften enthält, sondern über Art. 83 Abs. 8 DSGVO auf das nationale Recht verweist. Für Verstöße nach Art. 83 Abs. 4 bis Abs. 6 DSGVO beinhaltet das deutsche Recht in § 41 Abs. 1 S. 1 BDSG einen Verweis auf das Gesetz über Ordnungswidrigkeiten (OWiG).[7] Dieses enthält in den §§ 30 und 130 OWiG Regelungen zur Zurechnung des Handelns natürlicher Personen. Nach § 30 OWiG kann juristischen Personen das Handeln einer Leitungsperson zugerechnet werden, wenn diese in ihrer Rolle gegen Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verstößt oder durch eine Straftat oder Ordnungswidrigkeit eine Bereicherung der juristischen Person herbeigeführt wird.[8] § 130 OWiG normiert eine generelle Haftung der juristischen Person für Aufsichtspflichtverletzungen.[9] Folgt man dieser Ansicht, würden nur die Tätigkeiten von Leitungspersonen sowie Aufsichtspflichtverletzungen eine Zurechnung des Handelns zulassen. Eine Verantwortlichkeit der juristischen Person würde demnach bei Datenschutzverletzungen durch Mitarbeiter, die keine Leitungspersonen sind, ausscheiden, solange nicht zugleich eine Aufsichtspflichtverletzung vorliegt.

b) Zurechnung über das Funktionsträgerprinzip

Dem lässt sich allerdings zu Recht entgegenhalten, dass der Verweis des Art. 83 Abs. 8 DSGVO eine Öffnung ausschließlich für Verfahrensvorschriften erlaubt. Die Frage der Zurechnung von Handlungen ist jedoch eine Frage des materiellen Rechts. Überwiegend wird eine Anwendung der §§ 30 und 130 OWiG daher abgelehnt.[10] Stattdessen wird teilweise vertreten, dass der kartellrechtliche Unternehmensbegriffs im Rahmen von Art. 83 DSGVO i. V. m. ErwGr. 150 DSGVO auch für die Frage der Zurechnung des Handelns von natürlichen Personen herangezogen werden muss.[11] Demnach werden einer juristischen Person über das Funktionsträgerprinzip die Handlungen aller ihr zugeordneten natürlichen Personen, insbesondere ihrer Mitarbeiter, zugerechnet.[12] Eine Haftung des einzelnen Mitarbeiters wäre allenfalls über Heranziehung von § 9 Abs. 1 OWiG möglich.[13]

c) Zurechnung durch Anwendung von Art. 4 Nr. 7 DSGVO

Eine Anwendung des Funktionsträgerprinzips im Rahmen der Zurechnung des Handelns natürlicher Personen widerspricht jedoch der DSGVO. Die Anwendung des Funktionsträgerprinzips wird lediglich im Rahmen der Bußgeldbemessung angeordnet, jedoch gerade nicht für die Frage der Verantwortlichkeit. Diese knüpft Art. 4 Abs. 7 DSGVO an die Entscheidung über Zwecke und Mittel der Datenverarbeitung. Eine Entscheidung über Zwecke und

1 *Hessel/Leffer/Potel*, in: Verantwortungsbewusste Digitalisierung, Tagungsband des 23. Internationalen Rechtsinformatik Symposions, IRIS 2020, Die Inanspruchnahme des Auftragsverarbeiters durch die Aufsichtsbehörde – Der datenschutzrechtliche Satz des Pythagoras, S. 207, S. 210 ff.

2 *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 4 Nr. 7 DSGVO, Rn. 22.

3 *Voigt/v. d. Bussche*, in: v. d. Bussche/Voigt (Hrsg.), Konzerndatenschutz, 2. Aufl. 2019, Teil 3, Kapitel 1. Einleitung: Fehlendes Konzernprivileg, Rn. 3.

4 *Raschauer*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 4 DSGVO, Rn. 133.

5 Siehe dazu und zum Folgenden die gelungene Darstellung von *Diercks*, Datenübermittlung im Konzern – Rechtsgrundlagen und formelle Anforderungen, Diercks Digital Recht, 10. 5. 2020, abrufbar unter: https://diercks-digital-recht.de/wp-content/uploads/2020/05/Diercks-Daten%C3%BCbermittlung-im-Konzern-Diercks-Digital-Recht-Blog-10-Mai-2020.pdf.

6 *Schild*, in: BeckOK Datenschutzrecht, 32. Edition, Stand: 1. 5. 2020, Art. 4 DSGVO Rn. 88 c.

7 *Gola*, in: Gola (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 83 DSGVO Rn. 16.

8 *Meyberg*, in: Graf (Hrsg.), BeckOK OWiG, 26. Ed., Stand: 1. 4. 2020, § 30 OWiG Rn. 67 ff.

9 *Beck*, in: Graf (Fn. 8), § 130 OWiG Rn. 4.

10 *Born*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 8 Datenschutz und Straf- und Ordnungswidrigkeitenrecht, Rn. 22; *Holländer*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 31. Ed., Stand: 1. 11. 2019, Art. 83 DSGVO, Rn. 11; DSK, Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten! – Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 3. 4. 2019, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf; Der Hessische Beauftragte für Datenschutz, 47. Tätigkeitsbericht zum Datenschutz, S. 170, abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2018_47_TB.pdf.

11 *Ambrock/Karg*, in: v. d. Bussche/Voigt (Fn. 3), Teil 8, Aufsichtsbehördlicher Vollzug und Sanktionen, Rn. 102 f.

12 *Ambrock/Karg*, in: v. d. Bussche/Voigt (Fn. 3), Teil 8, Aufsichtsbehördlicher Vollzug und Sanktionen, Rn. 102 f.

13 *Ambrock/Karg*, in: v. d. Bussche/Voigt (Fn. 3), Teil 8, Aufsichtsbehördlicher Vollzug und Sanktionen, Rn. 102 f.

Mittel kann zunächst aus nationalen Rechtsnormen, etwa § 278 BGB, folgen.[14] Darüber hinaus können auch natürliche Verantwortlichkeiten (z. B. die Verantwortung des Arbeitgebers für Daten der Mitarbeiter) oder faktische Umstände (z. B. tatsächliche Kontrolle über Daten) sowie weitere Faktoren Berücksichtigung finden.[15] Eine Haftung eines einzelnen Mitarbeiters kommt nach dieser Ansicht nur in Betracht, wenn ein Exzess vorliegt und der Mitarbeiter selbst über die Zwecke und Mittel der Datenverarbeitung entscheidet.[16] Welchen Umfang diese Entscheidung haben muss, ist bisher nicht abschließend geklärt. Es dürfte jedoch klar sein, dass ähnlich wie bei Auftragsverarbeitern nicht jede Entscheidung zu einem Exzess führen kann. Diesbezüglich hat bereits die Artikel-29-Datenschutzgruppe festgestellt, dass ein Auftragsverarbeiter durchaus über Mittel einer Datenverarbeitung entscheiden kann, ohne dadurch zum Verantwortlichen zu werden.[17] Hierbei ist zu beachten, dass die Artikel-29-Datenschutzgruppe bevorzugt das Unternehmen als Verantwortlichen betrachtet und nicht einzelne handelnde Personen.[18] Am Beispiel der heimlichen Überwachung von Mitarbeitern weist sie darauf hin, dass Datenschutzverletzungen durch einen Funktionsträger des Unternehmens oder durch einen Mitarbeiter „als Ergebnis unzureichender Sicherheitsmaßnahmen angesehen werden" können.[19] Dies soll sogar unabhängig von der Frage gelten, ob die betreffende Person „später sowohl unter zivilrechtlichen Aspekten – auch gegenüber dem Unternehmen – als auch unter strafrechtlichen Aspekten" haftbar gemacht werden kann.[20] Darüber hinaus soll ein Hinwegsetzen über die Weisung des Auftraggebers durch den Auftragsverarbeiter nicht nur eine Verletzung der Vertraulichkeit herbeiführen, sondern auch unbefugt und damit regelmäßig rechtswidrig sein.[21] Die DSK geht in ihrer Entschließung zur Haftung von Unternehmen für Datenschutzverstöße ihrer Beschäftigten sogar so weit, einen Exzess nur anzunehmen, wenn die Handlungen von Beschäftigten „bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können".[22] Der Maßstab für einen Exzess liegt damit vergleichsweise hoch. Er soll nach der Literatur beispielsweise bei einer Einsicht in behördliche Datenbanken für private Zwecke oder der Entwendung von Kundendaten gegeben sein.[23] Letztlich wird man auch unter Rückgriff auf die Grundsätze zum innerbetrieblichen Schadensausgleich[24] mindestens davon ausgehen können, dass eine Verantwortlichkeit des Mitarbeiters ausscheidet, wenn diesen nur eine geringe Schuld am Datenschutzverstoß trifft. Eine eigene Verantwortlichkeit des Mitarbeiters kommt demnach insbesondere bei Vorsatz und grober Fahrlässigkeit bzw. bei ausdrücklichem Missbrauch und bewussten Verstößen gegen Weisungen[25] in Betracht. Für Unternehmen besteht jedoch die Möglichkeit, durch technisch-organisatorische Maßnahmen die Schwelle für eine eigene Verantwortlichkeit des Mitarbeiters herabzusenken. Kann durch ein enges Konzept von Weisungen und technischen Schutzmaßnahmen demnach ein Datenschutzverstoß weitestgehend ausgeschlossen werden, wird man im Einzelfall eher von einer vorsätzlichen Handlung des Mitarbeiters ausgehen können. Hierbei ist zu berücksichtigen, dass der Weisung als solche aufgrund der Besonderheiten des Arbeitsverhältnisses im Vergleich zur Auftragsverarbeitung eine geringere Wirkung zukommen dürfte.

4. Zwischenfazit

Die zentrale Regelung der DSGVO für die Zuordnung und Verteilung von Verantwortlichkeit ist Art. 4 Nr. 7 DSGVO. Die datenschutzrechtliche Verantwortung leitet sich folglich primär aus einer Entscheidung über die Zwecke und Mittel ab. Ob diese auf Ebene der Muttergesellschaft, bei einer Tochtergesellschaft oder – im Falle des Exzesses – bei einzelnen Mitarbeitern stattfindet, bedarf einer Betrachtung des Einzelfalls.

III. Rechtsrahmen für die Verhängung von Bußgeldern

Hinsichtlich des Rechtsrahmens für die Verhängung von Bußgeldern kann zwischen dem Adressaten des Bußgeldes bzw. des Bußgeldtatbestands und der Bemessung des Bußgeldes unterschieden werden.

1. Adressat des Bußgeldes

Die zentralen Vorschriften für die Verhängung von Bußgeldern finden sich in Art. 83 Abs. 4 bis 6 DSGVO. Im Gegensatz zum Entwurf der DSGVO richtet sich das Bußgeld nicht gegen jeden, dem ein Verstoß nach der Vorschrift zur Last gelegt wird.[26] Vielmehr ergibt sich der Adressat des Bußgeldes aus dem jeweiligen Tatbestand der Norm.[27] Nach Art. 83 Abs. 4 lit. a DSGVO kann demnach ein Bußgeld gegen den Verantwortlichen oder Auftragsverarbeiter verhängt werden. Ob es sich beim Verantwortlichen oder Auftragsverarbeiter um eine natürliche oder juristische Person handelt, ist unbeachtlich.[28] Für die Bußgelder nach Art. 83 Abs. 5 und 6 DSGVO gilt dem Grunde nach nichts anderes, da sich die zugrundeliegenden Vorschriften nicht an jedermann, sondern an den Verantwortlichen oder Auftragsverarbeiter richten.[29]

2. Bußgeldbemessung

Losgelöst von der Frage des Adressaten ist die Frage nach der Bemessung des Bußgeldes. Ausschlaggebend für diese ist zunächst – unabhängig davon, ob das Bußgeld gegen ein Unternehmen, eine andere juristische Person oder eine

14 *Hartung*, in: Kühling/Buchner (Hrsg.), DSGVO BDSG, 2. Aufl. 2018, Art. 4 Nr. 7 DSGVO, Rn. 9.
15 *Arning/Rothkegel*, in: Taeger/Gabel (Hrsg.), DSGVO BDSG, 3. Aufl. 2019, Art. 4 DSGVO, Rn. 169.
16 *Moos/Schefzig*, in: Taeger/Gabel (Fn. 15), Art. 83 DSGVO, Rn. 92.
17 Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 00264/10/DE, WP 169, angenommen am 16. 2. 2010, S. 18, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf.
18 Artikel-29-Datenschutzgruppe (Fn. 17), S. 20.
19 Artikel-29-Datenschutzgruppe (Fn. 17), S. 21.
20 Artikel-29-Datenschutzgruppe (Fn. 17), S. 21.
21 *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 2), Art. 29 DSGVO Rn. 16 ff.
22 DSK, Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten! – Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 3. 4. 2019, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf.
23 *Schantz*, in: Schantz/Wolff (Hrsg.), Das neue Datenschutzrecht, 2017, Rn. 360.
24 Vgl. dazu: *Joussen*, in: Rolfs/Giesen/Kreikebohm/Udsching (Hrsg.), BeckOK Arbeitsrecht, 56. Ed., Stand: 1. 6. 2020, § 611 a BGB Rn. 424 ff.
25 Vgl. zur Auftragsverarbeitung: *Hartung*, in: Kühling/Buchner (Fn. 14), Art. 29 DSGVO, Rn. 17.
26 Vgl. Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25. 1. 2012, KOM/2012/011 endgültig – 2012/0011 (COD), S. 105 f., abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52012PC0011.
27 *Moos/Schefzig*, in: Taeger/Gabel (Fn. 15), Art. 83 DSGVO, Rn. 81.
28 *Gola*, in: Gola (Fn. 7), Art. 83 DSGVO, Rn. 16.
29 *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2017, Art. 83 DSGVO, Rn. 47; *Eckhardt*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, Art. 83 DSGVO, Rn. 65; a. A.: *Bergt*, in: Kühling/Buchner (Fn. 14), Art. 83 DSGVO, Rn. 11.

natürliche Person verhängt wird – die Art des Verstoßes. Demnach kann bei Verstößen gegen Art. 83 Abs. 4 DSGVO maximal ein Bußgeld von 10 Millionen Euro oder im Falle eines Unternehmens ein Bußgeld von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes verhängt werden. Bei Verstößen gegen Art. 83 Abs. 5 bzw. Abs. 6 DSGVO beträgt das mögliche Bußgeld bis zu 20 Millionen Euro oder – bei Unternehmen – 4 % des gesamten weltweit erzielten Jahresumsatzes.

In einem zweiten Schritt ist zur Bestimmung der Obergrenze des Bußgeldes relevant, ob ein Unternehmen Adressat des Bußgeldes ist. Ist dies der Fall, stellt sich im Zusammenhang mit Konzernbußgeldern sodann die Frage, ob für die Bestimmung der Obergrenze im Einzelfall der Jahresumsatz des Tochterunternehmens oder des Konzerns heranzuziehen ist. Hierfür ist nach ErwGr. 150 DSGVO der aus dem Kartellrecht stammende funktionale Unternehmensbegriff der Art. 101 und 102 AEUV heranzuziehen. Nach der Rechtsprechung des EuGH ist unter einem Unternehmen in diesem Kontext „jede eine wirtschaftliche Tätigkeit ausübende Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung" zu verstehen.[30] Ob eine wirtschaftliche Einheit vorliegt, ist aus dem europäischen Recht heraus zu bestimmen.[31] Entscheidendes Kriterium ist insoweit die Abhängigkeit der Beteiligten sowie irgendein Angebot von Waren oder Dienstleistungen gegen Entgelt innerhalb des Binnenmarkts.[32] Übertragen auf den Konzern bedeutet die Anwendung dieser Grundregel, dass stets danach zu fragen ist, ob eine Abhängigkeit einzelner Konzernunternehmen untereinander und insbesondere zur Muttergesellschaft in einer Form besteht, die eine autonome Bestimmung des Verhaltens nicht mehr zulässt.[33] Dies ist jedenfalls bei einer 100%igen oder fast 100%igen Beteiligung der Fall.[34] Es ist jedoch auch ausreichend, dass im Fall einer Mehrheitsbeteiligung weitere Einflussmöglichkeiten, etwa personelle Überschneidungen, oder eine Weisungsbefugnis bestehen.[35]

In einem dritten Schritt sind letztlich die weiteren Bemessungskriterien nach Art. 83 Abs. 2 DSGVO heranzuziehen, um das Bußgeld innerhalb des zuvor ermittelten Bußgeldrahmens festzusetzen (Bußgeldbemessung im engeren Sinne).[36] Hierbei spielen tatbezogene Umstände, wie etwa die Art, Schwere und Dauer des Verstoßes, aber auch täterbezogene Umstände eine Rolle. Zu letzteren zählt beispielsweise, ob der Bußgeldadressat vorsätzlich oder fahrlässig gehandelt hat.

3. Auswirkungen im Konzernzusammenhang

Vergleicht man die hier erarbeiteten Schritte zur Bemessung von Bußgeldern mit dem Bußgeldkonzept der DSK,[37] lässt sich zunächst feststellen, dass dieses den dargestellten Grundsätzen nicht folgt. Vielmehr zieht die DSK das eigentlich zur Ermittlung der Bußgeldobergrenze gedachte Funktionsträgerprinzip als Bußgeldkriterium heran. Dies führt zu einer Verzerrung der im Gesetz vorgesehen Maßstäbe für die Bußgeldbemessung im engeren Sinne. Darüber hinaus ergeben sich jedoch auch Widersprüche innerhalb der DSGVO, da der Adressat des Bußgeldes und der Bezugspunkt für die Obergrenze des Bußgeldes auseinanderfallen können. Ein Beispiel dafür kann ein Datenschutzverstoß einer Tochtergesellschaft sein, bei der eine 100%ige Beteiligung der Muttergesellschaft besteht. Denkbar wäre etwa die Durchführung einer Marketingkampagne oder eines Gewinnspiels durch den Geschäftsführer der Tochtergesellschaft ohne eine Weisung der Muttergesellschaft. Wer nun für eine etwaige Datenschutzverletzung verantwortlich ist, hängt von der Zurechnung nach den oben dargestellten Maßstäben ab. Unproblematisch ist insoweit die Zurechnung der Handlungen des Geschäftsführers als natürliche Person gegenüber der Tochtergesellschaft. Eine Zurechnung der Datenverarbeitung gegenüber der Muttergesellschaft ist jedoch nicht möglich. Die Entscheidung über die Zwecke und Mittel der Verarbeitung erfolgt im hier dargestellten Beispielsfall nämlich gerade nicht durch die Muttergesellschaft, sondern durch die Tochtergesellschaft. Hierbei ist zu berücksichtigen, dass Beteiligungsverhältnisse an Gesellschaften im Gegensatz zu Weisungsbefugnissen kein Kriterium zur Bestimmung der Verantwortlichkeit nach Art. 4 Nr. 7 DSGVO sind. Verantwortlich für die Datenverarbeitung und damit Bußgeldadressat ist im dargestellten Beispielsfall demnach die Tochtergesellschaft. Anderes gilt jedoch für die Bußgeldbemessung. Hier ist das Funktionsträgerprinzip anwendbar, sodass für die Bußgeldobergrenze der Jahresumsatz der Muttergesellschaft heranzuziehen ist. Im Ergebnis könnte der Tochtergesellschaft folglich ein Bußgeld mit der für die Muttergesellschaft geltenden Obergrenze auferlegt werden.

IV. Widersprüchlichkeit der DSGVO

Fraglich ist, wie der bestehende Widerspruch zwischen der Bestimmung des Bußgeldadressaten und der Bußgeldobergrenze zu lösen ist. In Betracht kommt zunächst eine Ausdehnung des Funktionsträgerprinzips auf die Bestimmung der Verantwortlichkeit im Konzernkontext. Hierdurch würde eine Verantwortlichkeit des Konzerns für alle dem funktionalen Unternehmensbegriff unterfallenden Entitäten begründet und die Haftung für Datenschutzverletzungen ausgedehnt. In diese Richtung lässt sich auch die Entschließung der DSK zur Haftung von Unternehmen für Datenschutzverstöße ihrer Beschäftigten[38] interpretieren, da die DSK zur Bestimmung der Verantwortlichkeit für Datenschutzverstöße explizit auf den funktionalen Unternehmensbegriff sowie ErwGr. 150 DSGVO verweist. Eine solche Ausdehnung der Verantwortlichkeit ist jedoch unvereinbar mit dem Wortlaut der DSGVO. So bezieht sich ErwGr. 150 DSGVO ausdrücklich nur auf die Bestimmung der Bußgeldobergrenze, während Art. 4 Nr. 7 DSGVO eindeutig die Entscheidung über Zwecke und Mittel als ausschlaggebendes Kriterium für die Verantwortlichkeit benennt. Statt einer Ausdehnung der Verantwortlichkeit durch eine Überinterpretation des ErwGr. 150 DSGVO

30 EuGH, 20. 1. 2011 – C-90/09 P, BeckRS 2011, 80061, Rn. 35.

31 *Weiß*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, Art. 101 AEUV, Rn. 33 f.

32 *Zimmer*, in: Immenga/Mestmäcker (Hrsg.), Wettbewerbsrecht, 6. Aufl. 2019, Art. 101 Abs. 1 AEUV, Rn. 14 f.

33 *Emmerich*, in: Immenga/Mestmäcker (Hrsg.), EU-Wettbewerbsrecht, 5. Aufl. 2012, Art. 101 Abs. 1 AEUV, Rn. 48; *Hellmann*, in: Wiedemann (Hrsg.), Handbuch des Kartellrechts, 4. Aufl. 2020, § 46 Geldbußen und Zwangsgelder, Rn. 8 ff.

34 *Emmerich*, in: Immenga/Mestmäcker (Fn. 33), Art. 101 Abs. 1 AEUV, Rn. 48; *Hellmann*, in: Wiedemann (Fn. 33), § 46 Geldbußen und Zwangsgelder, Rn. 8 ff.

35 *Emmerich*, in: Immenga/Mestmäcker (Fn. 33), Art. 101 Abs. 1 AEUV, Rn. 48; *Hellmann*, in: Wiedemann (Fn. 33), § 46 Geldbußen und Zwangsgelder, Rn. 8 ff.; *Weiß*, in: Callies/Ruffert (Fn. 31), Art. 101 AEUV, Rn. 25.

36 Vgl. dazu: Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der VO (EU) 2016/679 der Art.-29-Datenschutzgruppe vom 3. 10. 2017, WP 253, übernommen vom Europäischen Datenschutzausschuss am 25. 5. 2018, abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

37 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14. 10. 2019, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf.

38 DSK (Fn. 22).

ist für den Fall einer Widersprüchlichkeit von Bußgeldadressat und Bußgeldobergrenze jedoch eine teleologische Reduktion des funktionalen Unternehmensbegriffs geboten. Zur Ermittlung der Bußgeldobergrenze muss – schon unter dem Gesichtspunkt der Verhältnismäßigkeit – der Jahresumsatz des Verantwortlichen herangezogen werden. Im oben genannten Beispiel wäre daher der Jahresumsatz der Tochtergesellschaft für die Bestimmung der Bußgeldobergrenze heranzuziehen. Begründbar ist diese teleologische Reduktion auch mit systematischen Erwägungen. So ist in Art. 82 DSGVO, der Schadensersatzansprüche Betroffener regelt, eindeutig klargestellt, dass diese nur gegenüber dem Verantwortlichen bzw. dem Auftragsverarbeiter bestehen können. Warum für die Verhängung von Bußgeldern anderes gelten sollte, ist nicht ersichtlich.

V. Fazit

Insgesamt lässt sich festhalten, dass der Adressat eines Bußgeldes nach der DSGVO in der Regel der Verantwortliche ist und für dessen Bestimmung einigermaßen klare Regeln – nämlich die Entscheidung über Zwecke und Mittel der Verarbeitung – existieren. Als schwieriger erweist sich die Zurechnung von Handlungen natürlicher Personen insbesondere in Arbeitsverhältnissen. Zwar kommt hier eine Verantwortlichkeit des einzelnen Mitarbeiters nur bei einem Exzess in Betracht, nicht abschließend geklärt ist jedoch, wann ein solcher vorliegt. Der Grundsatz, dass Unternehmen für Datenschutzverstöße ihrer Mitarbeiter haften, soweit kein Exzess vorliegt, ist auf Konzernstrukturen nicht übertragbar, da innerhalb dieser eine Entscheidung über Zwecke und Mittel von Datenverarbeitungen deutlich differenzierter stattfindet. Die Bestimmung der Bußgeldobergrenze bei Unternehmen erfolgt hingegen durch Anwendung des Funktionsträgerprinzips. Hierdurch können Widersprüche entstehen, die eine teleologische Reduktion des funktionalen Unternehmensbegriffs erforderlich machen. Die Bußgeldobergrenze hat sich dann nach dem Jahresumsatz des Verantwortlichen zu richten. In der Praxis ist daher im Rahmen von Bußgeldverfahren stets die Verantwortlichkeit des von der Aufsichtsbehörde ausgewählten Bußgeldadressaten einer kritischen Prüfung zu unterziehen.

Prof. Dr. Jan Dirk Roggenkamp und Prof. Dr. Frank Braun, Berlin/Hofkirchen*

Der tiefe Blick ins ausgelagerte Gehirn

Zur Verfassungsmäßigkeit der Telekommunikationsüberwachung nach dem nordrhein-westfälischen Polizeigesetz und vergleichbaren landesrechtlichen Vorschriften

Mit § 20 c Abs. 1 PolG NRW wurde – neben anderen grundrechtsbelastenden Maßnahmen, die im sog. Gefahrenvorfeld ansetzen – eine Ermächtigungsgrundlage zur Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung geschaffen. Dadurch ist es nun auch in Nordrhein-Westfalen der Vollzugspolizei gestattet, heimlich „die laufende Telekommunikation" zu überwachen und aufzuzeichnen. Der folgende Beitrag nimmt dies zum Anlass, um unter Berücksichtigung der gängigen Überwachungspraxis sowie der modernen Nutzung von Smartphones als „Zweitgedächtnis" und „verlängerten Denkapparat" die Verfassungsmäßigkeit dieser[1] und vergleichbarer Befugnisse zu hinterfragen.

I. Zugriff auf das „ausgelagerte Gehirn"

1. Auswertung des gesamten über den überwachten Anschluss geleiteten Datenstroms

§ 20 c PolG NRW[2] gestattet eine heimliche Überwachung der Telekommunikation (i. W. TKÜ). Längst bedeutet das nicht mehr lediglich ein heimliches Belauschen von Telefonaten oder das Abfangen und Lesen von SMS. Vielmehr wird regelmäßig eine viel umfassendere TKÜ „moderner Prägung" und/oder ein WLAN-Catching durchgeführt.

a) TKÜ „moderner Prägung"

Nach § 20 c Abs. 7 S. 1 PolG NRW hat jeder, der TK-Dienste erbringt oder daran mitwirkt, der Polizei entsprechende Überwachungsmaßnahmen „zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen". Der Umfang der Unterstützung durch die TK-Diensteanbieter bemisst sich gem. § 20 c Abs. 7 S. 2 PolG NRW nach der TKÜV.[3] Nach §§ 3 Abs. 1, 9 TKÜV wird der Polizei der gesamte über einen TK-Anschluss laufende „Rohdatenstrom" als sog. Überwachungskopie übermittelt.[4]

Dieser Rohdatenstrom beinhaltet zunächst die gesamte Individualkommunikation zwischen zwei (oder mehreren) Personen (Mensch-zu-Mensch-Kommunikation), z. B. Telefonie, Fax, E-Mail, SMS und andere Text- und Sprachnachrichten. Er umfasst aber auch alle sonstigen Daten, die im Rahmen des Gebrauchs des überwachten Anschlusses erzeugt werden.[5] In der Praxis und teils auch in der Kommentarliteratur wird es als unproblematisch angese-

* Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 3. 8. 2020.

1 Gegen die hier gegenständliche Regelung im PolG NRW wurde im August 2019 Verfassungsbeschwerde beim BVerfG erhoben. Der Autor *Roggenkamp* ist Verfahrensbevollmächtigter in diesem Verfahren. Zudem begleiten beide Autoren eine der Verfassungsbeschwerden gegen die Neuregelungen der repressiven Quellen-TKÜ und Online-Durchsuchung in der StPO.

2 Eingeführt mit Gesetz v. 13. 12. 2018 (GVBl. NRW S. 684). Dazu im Wesentlichen LT-Drs. 17/2351 und LT-Drs. 17/3865.

3 Telekommunikations-Überwachungsverordnung in der Fassung der Bekanntmachung vom 11. 7. 2017, BGBl. I S. 2316, die zuletzt durch Art. 16 des Gesetzes v. 17. 8. 2017, BGBl. I S. 3202, geändert worden ist.

4 *Meinicke*, in: Taeger, Law as a Service – Recht im Internet- und Cloud-Zeitalter, 2013, S. 968 f.; *Albrecht/Braun*, HRRS 2013, 500 ff.

5 *Albrecht/Braun*, HRRS 2013, 500 ff. m. w. N.; *Hiéramente*, HRRS 2016, 448, 450 f.