Workshop – Institut für Energie- und Regulierungsrecht Berlin – 30. Januar 2024
(*Rechtsanwälte Dr. Kai Mertens und Oliver Geiss, Squire Patton Boggs*)

SQUIRE PATTON BOGGS

EuGH (Rs. C-807/21) definiert Unternehmenshaftung für Datenschutzverstöße –

Unternehmen der Versorgungswirtschaft müssen sich darauf einstellen

Dr. Kai Mertens
Oliver Geiss
Rechtsanwälte und Partner – Squire Patton Boggs

(*Die Autoren sind als Prozessvertreter der Deutsche Wohnen SE im o.g. Verfahren zuständig für allgemeines deutsches und europäisches Unternehmensrecht, Kartellrecht und Gesellschaftsrecht. Sie tragen ihre persönlichen Auffassungen für die Zwecke einer rechtswissenschaftlichen Diskussion vor. Ihr Vortrag und diese Präsentation sind keine Rechtsberatung)*

.

Workshop – Institut für Energie- und Regulierungsrecht Berlin – 30. Januar 2024
(*Rechtsanwälte Dr. Kai Mertens und Oliver Geiss, Squire Patton Boggs*)

Überblick zum Workshop im Anschluss an

EuGH (Große Kammer) – Urteil 5.12.2023 – Rs. C-807/21 (Deutsche Wohnen)

- Kernaussagen des EuGH zur Bußgeldhaftung juristischer Personen nach der DSGVO
- Reaktionen von Datenschützern in Unternehmen und Behörden
- Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls
- Zur weiteren Entwicklung der DSGVO-Geldbußen, offene Fragen und andere Aspekte

Workshop – Institut für Energie- und Regulierungsrecht Berlin – 30. Januar 2024
(*Rechtsanwälte Dr. Kai Mertens und Oliver Geiss, Squire Patton Boggs*)

Kernaussagen der EuGH- Rspr.[1] - zur Bußgeldhaftung juristischer Personen nach der DSGVO:

(1) Nach Art. 83 DSGVO dürfen Bußgelder gegen juristische Personen nur verhängt werden, wenn diese vorsätzlich oder fahrlässig gehandelt haben und sich dabei über die Rechtswidrigkeit ihres Verhaltens nicht im Unklaren befunden haben konnten. Die Schuld der juristischen Person ist nach europäischem Recht durch Bewertung der nach Punkt (2) maßgeblichen Handlungen oder Unterlassungen festzustellen.

(2) Nach Art. 83 DSGVO ist für die Haftung der juristischen Person, die ein Unternehmen ist, von der Aufsichtsbehörde nachzuweisen, dass für sie Personen im Rahmen ihrer unternehmerischen Tätigkeit und in ihrem Namen gegen Datenschutzrecht verstoßen haben.

(3) Gegen juristische Personen kann nach Art. 83 DSGVO ohne Feststellung der Anschlusstat einer Leitungsperson im Sinne von §§ 30 oder 130 OWiG ein Bußgeld ergehen.

(4) Konzern: Maßgeblich für die Bestimmung eines Verstoßes ist allein die Verantwortlichkeit der juristischen Person – keine Mithaftung der Muttergesellschaft oder anderer Konzernunternehmen. (Nur) für die Bußgeldbemessung ist der (konsolidierte) Umsatz des Unternehmens gemäß Art. 101 AEUV - wirtschaftliche Einheit im Sinne des EU-Kartellrechts maßgeblich (*entgegen dem Wortlaut von Art. 4 Nr. 18 und 19 DSGVO in der deutschsprachigen Fassung*!).

[1] Siehe auch Parallelverfahren: EuGH – C-683/21 (Litauens' COVID 19 App) – Höhe der Bußgelder dort = 15tsd. Euro.

Reaktionen von Datenschützern in Unternehmen und Behörden

Jeder freut sich…

(1) **Unternehmen**, weil vom Tisch sind:

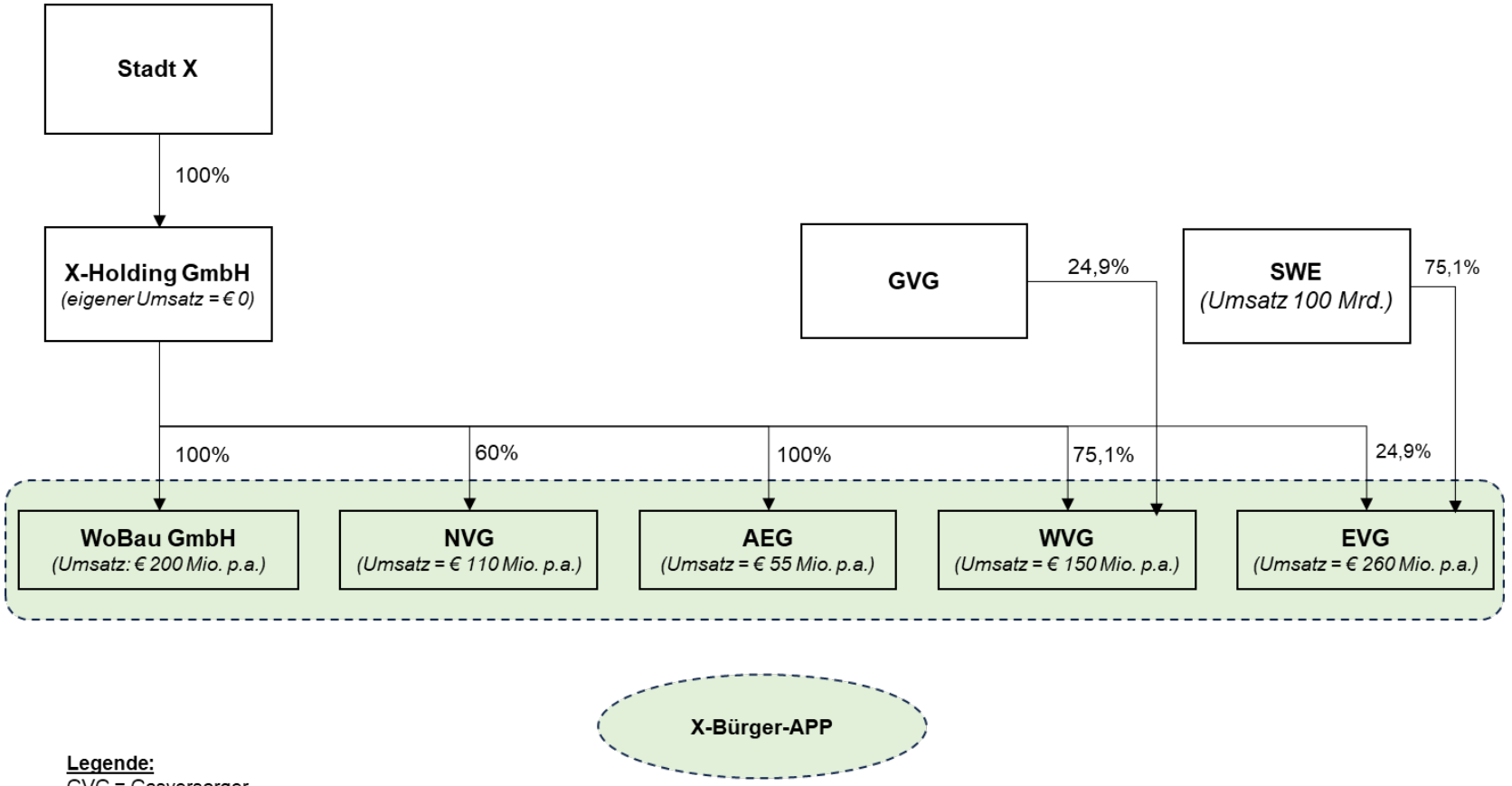
- die sog. „strict liability“ (verschuldensunabhängige, abstrakte Gefährdungshaftung) und auch die Umkehr der Beweislast.
- Unterschiedliche europäische Haftungsstandards nach einzelnen Rechtsordnungen der Mitgliedstaaten.
- Allgemeine Konzernhaftung des Unternehmens (wirtschaftliche Einheit – Art. 101 AEUV nach – so BlnBDI/KG: „Funktionsträgerprinzip“).

(2) **Deutsche Datenschutzbehörden**, weil sie annehmen, dass die Verfolgung von Datenschutzverstößen nun weniger Aufwand erfordert:

- Zurechnung aller Mitarbeiter und sonstiger für die juristische Person handelnder Personen im Unternehmen (im Konzern und außerhalb).
- Klarheit zur Bußgeldobergrenze.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls

(Dieser Modellfall und seine Varianten sind vereinfacht und zur Illustration und Verdeutlichung rechtlicher Themen gebildet und setzt dazu verschiedene Elemente aus relevanten Konzepten der Versorgungswirtschaft zusammen)



Legende:
GVG = Gasversorger
SWE = Stromversorger
NVG = Nahverkehrsgesellschaft
AEG = Abfallentsorgungsgesellschaft
WVG = Wärmeversorgungsgesellschaft
EVG = Energieversorgungsgesellschaft

Workshop – Institut für Energie- und Regulierungsrecht Berlin – 30. Januar 2024
(*Rechtsanwälte Dr. Kai Mertens und Oliver Geiss, Squire Patton Boggs*)

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls

Die Stadt X hält eine 100%-Beteiligung an der **X-Holding** GmbH, diese wiederum ist an kommunalen Versorgungsunternehmen wie folgt beteiligt:

- mit **100%** an dem kommunalen Wohnungsunternehmen **WoBau** (Umsatz **200 Mio.** p.a.).
- mit **60%** an der Nahverkehrsgesellschaft **NVG** (je 20% werden von zwei Nachbargemeinden gehalten, alle wesentlichen Maßnahmen bedürfen 75% der Stimmen) - Umsatz **110 Mio**. p.a.
- mit **100%** der Abfallentsorgungsgesellschaft **AEG**- Umsatz **55 Mio**. p.a.
- mit **75,1%** an der Wärmeversorgungsgesellschaft **WVG** (24,9% werden von einem Gasversorger **GVG** gehalten) – Umsatz **150 Mio**. p.a.

Die Stromversorgung in der Stadt X, aber auch mit einem bundesweiten Angebot, bietet die Energieversorgungsgesellschaft **EVG** (Umsatz **250 Mio.**) an. **75,1%** an der EVG hält der überregionale Stromversorger **SWE** (Umsatz **100 Mrd**.), die weiteren **24,9%** die **X-Holding**.

WoBau, NVG, AEG, WVG und EVG betreiben **als gemeinsam datenschutzrechtlich Verantwortliche** die **X-Bürger-App**, die den Einwohnern der Stadt X den einfachen Zugang zu und die einheitliche Verwaltung ihrer Versorgungsleistungen ermöglicht.

Das für die X-Bürger-App zuständige Projektteam besteht aus jeweils wechselnden Mitarbeitern der IT-Abteilungen aller beteiligten Gesellschaften, die die App im Rahmen ihrer jeweiligen Anstellungsverträge mit den beteiligten Gesellschaften betreuen. Einer dieser Mitarbeiter klickt im Zusammenhang mit der Arbeit an dem Projekt auf den link einer an die Adresse info@bürgerXapp.de gesendete phishing-mail, weil er sie nicht als solche erkannte. Hackern gelingt es daraufhin 100.000 vollständige Bürgerdatensätze (einschließlich Verbrauchsdaten) aus der X-Bürger App in ihre Kontrolle zu bringen.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

EVG meldet den Angriff sofort, gibt aber nicht an, welcher konkrete Teammitarbeiter den Klick auf den link gesetzt hat. Die zuständige Datenschutzbehörde ermittelt, dass Mitarbeiter aller gemeinsam Verantwortlichen Zugang zu dem o.g. E-Mail-Account hatten. Sie geht angesichts der Gestaltung der phishing-mail nicht von einem vorsätzlichen Verstoß aus. Sonstige Datenschutzverstöße kann die Behörde nicht feststellen. Angesichts der Auswirkungen des Hacker-Angriffs möchte sie aber dennoch für jeden Bürgerdatensatz als Ausgangsgröße für die Bemessung des Bußgelds 500 Euro ansetzen.

Gegen welche juristischen Personen kann die Behörde ein Bußgeld in der vorgesehenen Höhe von 50 Mio. Euro erheben - und wen trifft es am Ende wirtschaftlich?

Variante A: Die gemeinsam Verantwortlichen tauchen vertieft ins Gesellschaftsrecht ein, und entdecken, dass sie mit der Vereinbarung zur gemeinsamen Entwicklung und zum Betrieb der X-Bürger-App eine rechtsfähige BGB-Gesellschaft gegründet haben (§ 705 Abs. 2 BGB).

Variante B: Statt eines Projekts in gemeinsamer Verantwortung nach Art. 26 DSGVO gründen die X-Holding (50%), GVG (25%) und EVG (25%) die X-Bürger-App OHG, die eine eigene Geschäftsführung erhält, die App eigenständig entwickelt, die benötigten personenbezogenen Daten eigenständig erhebt und den App-Service durch zwei eigene Mitarbeiter erledigt. Die X-Bürger-App OHG erhielt für die über sie vermittelten Umsätze im letzten relevanten Geschäftsjahr 0,2 Mio. Euro Provisionen von ihren Gesellschaftern und 0,1 Mio. Euro aus der Schaltung von Werbung für Dritte.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

Art. 83 Absatz 5 DSGVO:

1. **Verstoß gegen eine der in Art. 83 Abs. 5 genannten Bestimmungen**, u.a. Verstoß gegen Grundsätze für die Verarbeitung (Art. 5 Absatz 1 f), 6 (Integrität und Vertraulichkeit)).

   EuGH: Juristische Personen können Verantwortliche sein. Bei juristischen Personen, die Unternehmen sind, sind für die Ermittlung eines Verstoßes der juristischen Person alle Handlungen zu berücksichtigen, die von Personen im Rahmen ihrer unternehmerischen Tätigkeit begangen wurden. Eine sog. **Anschlusstat** einer „**identifizierten natürlichen Person**“ im Sinne von § 30 OWiG ist **nicht erforderlich**.

   Folge: Da die Projektmitarbeiter für alle gemeinsam Verantwortlichen - WoBau, NVG, AEG, WVG und EVG- im Rahmen des gemeinsamen X-Bürger-App-Projekts gehandelt haben, indem sie den maßgeblichen E-Mai-Account verwalteten, wird die Datenschutzbehörde ihr Handeln allen gemeinsam Verantwortlichen zurechnen. Fraglich im Einzelfall:
   - Abgrenzung: Welche „Identifikation“ der Handlungen natürlicher Personen ist erforderlich, um den Verstoß der juristischen Person darzulegen (Abgrenzung zurechenbare/nicht zurechenbare Personen)?
   - Was geschieht, wenn die beteiligten Gesellschaften einwenden, der Mitarbeiter habe den link geöffnet, um die X-Bürger-App zu schädigen; daher liege ein Mitarbeiterexzess – kein Handeln im Rahmen der unternehmerischen Tätigkeit - vor, der die Verantwortlichkeit der Gesellschaften ausschließe?

   Keine eigene Haftung der Stadt X, der X-Holding oder der SWE als Verantwortliche: EuGH: Es gibt (entgegen der Auffassung der Berliner Behörde) keine Grundlage für eine Zurechnung der Verantwortlichkeit über den „funktionalen Unternehmensbegriff“; dieser ist nur für die Berechnung der Bußgeldhöhe maßgeblich.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

2. **Schuld der juristischen Person:** EuGH: „**vorsätzlicher oder fahrlässiger**“ Verstoß **ist Haftungsvoraussetzung** (nicht nur „*zu berücksichtigen*“ (siehe Art. 82 Abs. 2) – keine „*strict liability*“ (!)- Die Datenschutzbehörde muss ermitteln und nachweisen, dass Fahrlässigkeit oder Vorsatz vorliegt.

   Nach EU-Recht sind Vorsatz und Fahrlässigkeit aus allen zu berücksichtigenden Handlungen der natürlichen Personen zu ermitteln. WoBau, NVG, AEG, WVG und EVG können sich auch auf subjektiver Ebene nicht auf §§ 30, 130 OWiG – Begrenzung der Verantwortlichkeit auf sogenannte „Leitungspersonen“ berufen.

   Folge: Das Anklicken des links in der phishing-mail muss mindestens als fahrlässige Handlung eingestuft werden können, damit ein Bußgeld durchgesetzt werden kann.

   Die Datenschutzbehörde und, bei Einspruch, das Landgericht werden jedoch ermitteln müssen, da bei vorsätzlicher Öffnung des links durch einen Mitarbeiter ein Exzess vorliegen kann, der nicht nur auf objektiver, sondern auch auf subjektiver Ebene die Zurechnung ausschließt, weil der Mitarbeiter nicht im Rahmen der unternehmerischen Tätigkeit gehandelt hätte.

   Anmerkung: In Fällen, in denen kein Mitarbeiterexzess oder eine Einwirkung unternehmens-/projektexterner Personen in Betracht kommt, und eine von der Leitung des Unternehmens angewiesene Verarbeitung persönlicher Daten erfolgt, gibt es im Ergebnis keine signifikanten Unterschiede zum Konzept der §§ 30, 130 OWiG im Hinblick auf die Zurechenbarkeit des Verstoßes zur juristischen Person. Der Fall Deutsche Wohnen hat sich bislang nur deshalb zu dieser Frage hin entwickelt, weil der Bußgeldbescheid sich auf keine einzige Handlung irgendeiner Person bezieht und die Tathandlung/das ordnungswidrige Unterlassen nicht bestimmt, sondern entgegen § 66 OWiG pauschal als Dauerverstoß der Betroffenen seit dem Inkrafttreten der DSGVO beschreibt. Das deutsche und europäische Kartellrecht wird vom BKartA grundsätzlich effizient nach §§ 81a ff. i.V.m 30 OWiG durchgesetzt.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

3. **Einzel- oder gesamtschuldnerische Bußgeldhaftung mehrerer Verantwortlicher wegen eines einheitlichen Verstoßes**?

Fraglich: Darf die Aufsichtsbehörde das von ihr berechnete Bußgeld gegen jeden beliebigen der gemeinsam Verantwortlichen erheben und ihnen den Ausgleich im Innenverhältnis überlassen – oder muss die Behörde das Bußgeld von jedem gemeinsam Verantwortlichen nach dem „Grad seiner Verantwortung“ (Art. 83 Abs. 2 lit. d) DSGVO)[2] im Innenverhältnis erheben?

Frage in der DSGVO nur für das Zivilrecht geregelt (Art. 26 Abs. 3, 82 Abs. 4 DSGVO).

EU-Kartellrecht: Keine Notwendigkeit und keine Befugnis der Kommission, das Innenverhältnis der Betroffenen zur regeln; regelmäßig gesamtschuldnerische Geldbußen; Kommission hat aber im Prinzip freies Wahlrecht.

§ 30 OWiG sieht auch bei Mittäterschaft keine gesamtschuldnerischen Bußgelder vor (Grundsatz individueller Strafzumessung).

Unsere Erwartung: Es kann im DW-Fall oder einem anderen Fall zu einer erneuten Vorlagefrage an den EuGH kommen. Die Datenschutzbehörde wird bis dahin entweder versuchen, die Frage selbst auf den Tisch zu bringen, und ein gesamtschuldnerisches Bußgeld verhängen oder von mehreren gemeinsam Verantwortlichen gegen diejenige juristische Person ein Bußgeld verhängen, die die höchste Bemessungsgrenze mitbringt (hier im Modellfall ganz eindeutig die EVG).

[2] Vgl. EuGH – C-683/21; Rdn. 42., aber in den edpd-Leitlinien nur Fälle der Compliance/Vorbeugung von Verstößen durch das Unternehmen.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

4. **Erhebung einer Geldbuße im Einklang mit Art. 83 Absatz 2**: „*gebührende Berücksichtigung der Kriterien a) bis k)*“, die zudem „*wirksam, verhältnismäßig und abschreckend“* (Absatz 1) sein muss:

   a. Die in diesem Modellfall von der Behörde kalkulierten 500 Euro je Datensatz betragen weniger als 1/10 des Betrages, der nach Auffassung der Berliner Datenschutzbehörde auf eine nicht mehr lesbare und nicht an die Öffentlichkeit gelangte, 20 Jahre alte Personalausweiskopie entfällt. Hier also auch bei nur fahrlässigem Verstoß unterstellt: 500 Euro je Datensatz wegen des Ausmaßes des Verstoßes grundsätzlich angemessen. *Fraglich, natürlich ob Ansatz der Berliner Datenschutzbehörde nach Art. 83 Abs. 1 und 2 vertretbar (ggf. nächste EuGH-Vorlagefrage?).*

   Nach den *edpb-guidelines (adopted)* sollen die Datenschutzbehörden von ihrer ersten Kalkulationsbasis aus, je „Unternehmen“ (i.S.v. Art. 101 AEUV) bei der Berechnung Abzüge anwenden, wenn der Umsatz niedriger als 500 Mio. Euro ist. (*Prüfung nach Bußgeldrahmen, siehe Ziffer 5.*) Danach (Empfehlung) ergäbe sich:

   - Für EVG (Unternehmen = SWE-Konzern) – über 500 Mio. UE = kein Abzug.

   - Bei Zusammenrechnung der Verantwortlichen AEG, WVG und WoBau über X-Holding zum Unternehmen (NVG konsolidiert) insgesamt 515 Mio. UE = kein Abzug;

   - Gegenüber NVG isoliert als Verantwortliche empfohlen: 15% - 50% = zwischen 7,5 und 25 Mio.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

5. **Bußgeldrahmen:** 20 Mio. „*oder im Fall eines Unternehmens von bis zu 4%*“ des weltweiten Umsatzes (nach dem Wortlaut von Absatz 5 „*bei Verstößen*“; Annahme hier: es gibt mehrere gemeinsam Verantwortliche, aber nur einen Verstoß).

   Unternehmen = Unternehmen i.S.v. Art. 101 AEUV = wirtschaftliche Einheit (Akzo Nobel-Rechtsprechung des EuGH: „*einheitliche Organisation persönlicher, materieller und immaterieller Mittel, die dauerhaft einen bestimmten wirtschaftlichen Zweck verfolgt*“, wobei der EuGH im Wesentlichen darauf abstellt, dass eine Muttergesellschaft die Geschäfte einer Tochtergesellschaft so leiten kann, dass diese keinen eigenständigen Marktauftritt für sich bestimmen kann.

   a. **SWE und EVG** = ein Unternehmen – 4% von 100 Mrd., Bußgeldrahmen also 4 Mrd.

   b. **WoBau, AEG und WVG** über X-Holding als Muttergesellschaft eines Unternehmens – 4% von 515 Mio. (NVG bei X-Holding konsolidiert), also – gemeinsam 20,6 Mio.

   c. **NVG,** wenn nicht in die X-Holding-Unternehmenseinheit einzubeziehen – 4% von 110 Mio., also 4,4 Mio.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

6. **Verhängung des Bußgelds, Szenario hier angenommen:** Die Behörde entscheidet sich der Einfachheit halber, die EVG in Anspruch zu nehmen und verhängt gegen die EVG ein Bußgeld in Höhe von 50 Mio. Euro.[3] Die EVG erhebt Beschwerde. Das zuständige Landgericht entscheidet:

   Die Datenschutzbehörde kann den Nachweis der Fahrlässigkeit anhand der Gestaltung der phishing-mail führen, schon weil das Gericht ihrem Standpunkt folgt, dass links nie direkt geöffnet werden dürfen. Auch in diesem Zusammenhang muss nach Ansicht des Gerichts unter Anwendung des EuGH-Urteils nicht ermittelt werden, wer konkret gehandelt hat, da alle in Betracht kommenden Mitarbeiter einschließlich des Mitarbeiters, der auf den link geklickt hat, für alle gemeinsam Verantwortlichen gehandelt haben. Jeder gemeinsam Verantwortliche: WoBau, NVG, AEG, WVG und EVG habe damit als juristische Person fahrlässig (als „Mittäter“) gehandelt.

   Es bestehe keine Veranlassung zu einer Herabsetzung der Geldbuße gegenüber der EVG, nur weil WoBau, NVG, AEG und WVG von der Behörde nicht in Anspruch genommen wurden.

[3] Oder sie „testet“ ob sie analog zum Kartellrecht gegen die Verantwortlichen als Gesamtschuldner die 50 Mio.-Geldbuße verhängt.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

7. **Aufteilung der Geldbuße unter den gemeinsam Verantwortlichen im Innenverhältnis**:

Die Vereinbarung der gemeinsam Verantwortlichen nach Art. 26 DSGVO enthält keine Regelungen für gemeinsam zu verantwortende Bußgelder. Der Gesamtschuldnerausgleich richtet nach § 426 BGB. In Betracht kommende Aufteilungsmaßstäbe:

- „Grad der Verantwortung" – die beteiligten Unternehmen selbst müssen versuchen zu ermitteln, welcher Mitarbeiter tatsächlich den Fall ausgelöst hat,
- Verteilung der über die X-Bürger-App erzielten Umsätze,
- potenzielle Bußgeldhöhen bei Einzelbetrachtung (also insbesondere: muss hier der der SWE-Konzern, der den hohen Bußgeldrahmen „setzt" dafür verhältnismäßig höher haften; auch dann, wenn „sein Mitarbeiter" nicht verantwortlich ist?).

Danach wird es der EVG gelingen, teilweise bei den weiteren gemeinsam Verantwortlichen einen Ausgleich zu erreichen, mit dem geringsten Haftungsanteil bei der AEG.

Fraglich: Regress der EVG im Konzernverhältnis bei SWE – nur wegen des Konzernumsatzes kommt es dazu, dass gegen die Bußgeldbemessungswerte für die EVG entsprechend hoch sind (anders als im EU-Kartellrecht: Art. 101 AEUV: „Unternehmen" ist dort Tatbestandsmerkmal und nicht nur auf der Rechtsfolgenseite relevant.

Hinweis: Grundsätzlich gilt: Bußgelder sind in Deutschland nicht versicherbar; Haftungs-/Ausgleichsansprüche sind versicherbar.

Erläuterung des Art. 83 DSGVO-Bußgeldhaftungskonzepts nach der EuGH-Rechtsprechung anhand eines Modellfalls (cont.)

Variante A:

Da die X-Bürger-App für die Teilnahme am Rechtsverkehr bestimmt ist, haben die Beteiligten nach § 705 Abs. 2 BGB eine rechtsfähige Gesellschaft gegründet. Art. 26 Absatz 1 Satz 1 DSGVO beruht aber auf der tatsächlichen Feststellung, ob mehrere Personen die Zwecke und die Mittel zur Verarbeitung festlegen.

Variante B:

Die Gründung einer Gesellschaft mit eigener Geschäftsführung, die nicht „beauftragt“ wird (vgl. dazu EuGH (Große Kammer), Urteil v. 5.12.2023 – C-683/21) bei der die Gesellschafter sodann nicht mehr die Zwecke und die Mittel zur Verarbeitung festlegen – sondern nur noch das Eigenkapital aufbringen, Provisionen zahlen und Gewinne entnehmen, führt dazu, dass nur die X-Bürger-App OHG die einzeln Verantwortliche im Sinne der DSGVO ist. Da die X-Bürger-App OHG kein Mitglied eines Unternehmens im Sinne von Art. 101 AEUV ist, ist der Bußgeldbemessung allein ihr eigener Umsatz zugrunde zu legen: Nach den Empfehlungen des edpb 0,2-0,4% von 300tsd Euro und ein Bußgeldrahmen von 20 Mio.

Workshop – Institut für Energie- und Regulierungsrecht Berlin – 30. Januar 2024
(*Rechtsanwälte Dr. Kai Mertens und Oliver Geiss, Squire Patton Boggs*)

Zur weiteren Entwicklung der DSGVO-Geldbußen, offene Fragen und andere Aspekte

- Bei Unternehmen der Versorgungswirtschaft konnte es schon bisher innerhalb, aber auch außerhalb des „eigenen" Konzerns aufgrund hoher Bußgeldbemessungsgrenzen zu **strukturell hohen Bußgeldrisiken** kommen; dieses Risiko erhöht sich durch den weiten personellen Verantwortungskreis für DSGVO-Verstöße, insbesondere auch bei gemeinsamer Verantwortung.

- Da der EuGH einer allgemeinen Konzernhaftung eine Absage erteilt hat, kann eine Limitierung des Bußgeldrisikos in geeigneten Fällen erreicht werden, indem der **Kreis der Verantwortlichen** auf das notwendige Maß begrenzt wird (entgegen einer häufig anzutreffenden weiten Gesamtverantwortlichkeit nach Art. 26 DSGVO). Wichtig dabei: Gemeinsame Verantwortung (Bestimmung der Zwecke und der Mittel) ist Tatfrage.

- Nach § 41 BDSG sollen die §§ 30, 130 OWiG angewendet werden. Die EuGH-Rechtsprechung lässt von § 30 Abs. 1 OWiG wenig übrig. § 66 OWiG, der bislang Entscheidungsgrundlage im Deutsche Wohnen Fall war, bleibt anwendbar. Wie die deutschen Strafgerichte hier im Einzelnen vor dem Hintergrund des Schuldprinzips und des Bestimmtheitsgrundsatzes reagieren (europarechtskonforme Anwendung), bleibt abzuwarten, insbesondere welche Maßstäbe die Gerichte auf der Ebene der Definition der „Unternehmenstat", der Ermittlung des einzelnen oder der gemeinsam Verantwortlichen, des Tatbestands eines Verstoßes und seiner vorsätzlichen oder fahrlässigen Begehung anlegen werden. Diese Ermittlung muss an sich denselben strengen Anforderungen genügen, die der EuGH an Kartellverstöße anlegt.

- Die Grundsätze, nach denen Geldbußen bei gemeinsamer Verantwortung unter den Beteiligten aufzuteilen sind, sollten soweit möglich sowohl innerhalb und vor allem auch bei gemeinsamer Verantwortung außerhalb des eigenen Konzerns spezifisch auch mit Blick auf die Bußgeldrahmen geregelt werden (bei internationaler Zusammenarbeit kann sich zudem die Frage stellen, nach welchem Recht der Gesamtschuldnerausgleich vorzunehmen wäre).

- Es ist möglich, dass das LG Berlin und hiernach das Kammergericht zur Angemessenheit der Höhe von DSGVO-Geldbußen entscheiden müssen; auch hierzu sind Vorlagefragen an den EuGH denkbar.

Weitere Themen

- Offen: Entwicklung zur Frage des Verbotsirrtums (EuGH: *„…sich über die Rechtswidrigkeit nicht im Unklaren sein konnte*“) angesichts der enorm vielen unbestimmten Rechtsbegriffe der DSGVO.

- Organhaftung (§§ 93 AktG, 43 GmbHG) für Verbandsbuße

  Sehr str.; zuletzt Kartellrecht: OLG Düsseldorf – 27.7.23 – 6 U 1/22 (Kart): teleologische Reduktion – aber was ist mit einem Organmitglied, das nach OLG Dresden selbst Verantwortlicher ist?

- Bußgeldregress des Unternehmens (Verbandsbuße) gegen Organmitglieder/Mitarbeiter

  (1) Managerhaftung: nicht alle Argumente OLG Düsseldorf gelten für Art. 83 DSGVO-Bußgelder; KartellR/DSGVO – Öffentliche und zivile Sanktionen anderer Größenordnung und Struktur – Ahndung (Rechtsgut) /Gewinnabschöpfung.

  (2) Gesamtschuldnerausgleich (§ 426 BGB) mehrerer gemeinsam Verantwortlicher (vgl. BGH-Calciumcarbid II; Manager = persönlich ebenfalls Verantwortlicher(?), so jdf. OLG Dresden – 4 U 1158/21)).

- (Nachträgliche) Übernahme durch Unternehmen /Regress (§ 670 BGB bei fehlender Pflichtverletzung) des Organmitglieds oder sonstiger verantwortlicher Personen

  Aufgrund EuGH-Rechtsprechung wahrscheinlich weniger persönliche Bußgelder; zugleich „keine Anschlusstat“ – Eigene Ermittlungen des Unternehmens erforderlich.

- D&O, Cyber-/IT- und sonstige Haftpflichtversicherungen
  - Zivilrechtlicher Regress des Unternehmens D&O-versicherbar

    (läuft ins Leere, wenn kein haftungsrechtlicher Regressanspruch (§§ 93 AktG/43 GmbHG besteht, aber hier: Gesamtschuldnerausgleich (§ 426 BGB) der datenschutzrechtlich Verantwortlichen?)
  - Vorsatzausschluss – wenn „nur“ Unternehmensvorsatz festgestellt wird?

    (interessant LG Frankfurt – 20.1.23 – 2.08 O 313/20)
  - Unmittelbare Versicherbarkeit von Geldbußen weiterhin ausgeschlossen?

(Art. 83 DSGVO-Geldbußen haben Strafcharakter).