Bußgelder wegen Datenschutzverstößen – aus Sicht von Aufsichtsbehörden und Unternehmen

Bußgeldkonzept
Sanktionen
Haftung
Datenschutzbehörden
Rechenschaftspflicht

ZD-Interview mit Barbara Thiel und Tim Wybitul

Lesedauer: 22 Minuten

ZD: *Die europäischen Datenschutzbehörden nehmen bei den Bußgeldern nach Art. 83 DS-GVO erkennbar Fahrt auf. Erst kürzlich hat das britische Information Commissioner's Office (ICO) zwei Bußgelder in jeweils dreistelliger Millionenhöhe angekündigt. Die Berliner Datenschutzbehörde hat dann nachgezogen und ein Bußgeld i.H.v. € 14,5 Mio. verhängt. Liebe Frau Thiel, was versteht Ihre Behörde unter wirksamen, verhältnismäßigen und abschreckenden Bußgeldern nach Art. 83 DS-GVO?*

Thiel: Ganz grundsätzlich orientieren wir uns hier zunächst am Working Paper (WP) 253 der *Art. 29-Datenschutzgruppe*, das vom *Europäischen Datenschutzausschuss* übernommen wurde. Es handelt sich dabei um einen internen Leitfaden für die Aufsichtsbehörden, der zu einer Harmonisierung der Bußgeldpraxis beitragen soll. Darin heißt es u.a., dass wir alle Aspekte eines Sachverhalts in kohärenter und objektiv gerechtfertigter Weise bewerten müssen.

Wirksam und abschreckend ist eine Sanktion aus unserer Sicht, wenn sie einerseits generalpräventiv geeignet ist, die Allgemeinheit von Verstößen abzuhalten sowie das Vertrauen der Allgemeinheit in die Geltung des Rechts zu stärken, und andererseits spezialpräventiv dazu führt, den Täter von weiteren Verstößen abzuhalten. Verhältnismäßigkeit wiederum bedeutet für mich, dass die Schwere des Verstoßes in einem angemessenen Verhältnis zur Sanktion stehen muss.

Was im Einzelfall als wirksam, verhältnismäßig und abschreckend betrachtet wird, hängt letztlich auch vom Ziel der Abhilfemaßnahme ab, also: Soll damit die Verletzung behoben oder rechtswidriges Verhalten bestraft werden – oder beides?

ZD: *Lieber Herr Wybitul, wie sehen Sie dies?*

Wybitul: Zu dem von der *Berliner Datenschutzbeauftragten* verhängten Bußgeld kann ich hier leider nichts sagen, da ich Teil des Verteidigerteams des betroffenen Unternehmens bin. Insofern sehe ich Bußgelder natürlich aus einem etwas anderen Blickwinkel als die Datenschutzbehörden. Das kürzlich verhängte Bußgeld zeigt jedenfalls, dass Sanktionen nach Art. 83 DS-GVO für Unternehmen ein immer konkreter werdendes Risiko darstellen. Derartige Bußgeldrisiken muss man vor allem nach ihrer Eintrittswahrscheinlichkeit und der Höhe möglicher Geldbußen bewerten. Dabei darf man auch Folgeprobleme nicht vernachlässigen. Die Erfahrung zeigt z.B. auch, dass Unternehmen Schadensersatzklagen drohen können, nachdem gegen sie ein hohes Bußgeld verhängt wurde. Mittlerweile gibt es bereits Prozessfinanzierer, die sich auf bekanntwerdende Datenschutzverstöße oder Indizien für mögliche Verstöße spezialisiert haben. Sobald es Presseberichte über Datenschutzvorfälle gibt, werben sie um betroffene Personen, um für diese – vor allem immaterielle – Schadensersatzansprüche einzuklagen.

Vor allem aber machen die Datenschutzbehörden zunehmend von ihren enorm gestiegenen Befugnissen Gebrauch, wie die neuere Entwicklung klar zeigt.

ZD: *Ist denn eigentlich jeder Verstoß gegen das Datenschutzrecht mit einem Bußgeld bedroht?*

Wybitul: Die Bußgeldtatbestände in Art. 83 Abs. 4, 5 und 6 DS-GVO nehmen auf so gut wie alle Handlungspflichten Bezug, die Verantwortliche oder Auftragsverarbeiter einhalten müssen. Sogar wegen eines Verstoßes gegen die – ja doch sehr vage gehaltene – Kooperationspflicht kann eine Behörde nach Art. 83 Abs. 4 lit. a DS-GVO ein Bußgeld verhängen. Zudem sind nach Art. 83 Abs. 5 lit. d DS-GVO auch Verstöße gegen die Vorgaben des BDSG oder sonstiger Ausführungsgesetze der Mitgliedstaaten zur DS-GVO bußgeldbewehrt. Damit ist etwa auch die unzureichende Umsetzung der in § 26 BDSG getroffenen Regelungen zum Beschäftigtendatenschutz mit einem Bußgeld bedroht.

ZD: *Frau Thiel, bedeutet dies, dass Datenschutzbehörden künftig bei nennenswerten Verstößen gegen das Datenschutzrecht regelmäßig Bußgelder verhängen werden?*

Thiel: Bei nennenswerten Verstößen wird das sicherlich so sein, da lässt die DS-GVO aus meiner Sicht auch wenig Spielraum. Es ist ja auch ein deutlich formuliertes Ziel der *EU-Kommission* gewesen, mit der DS-GVO die Durchsetzung des Datenschutzrechts zu verbessern. Bußgelder sind dafür ein zentrales Mittel.

ZD: *Gegen welche Adressaten bzw. Täter können Datenschutzbehörden denn überhaupt Bußgelder verhängen?*

Thiel: Ich sehe beim möglichen Täterkreis mit Blick auf Art. 83 Abs. 4 bis 6 DS-GVO eindeutig die Verantwortlichen und Auftragsverarbeiter im Fokus. Datenschutzrechtlich Verantwortliche können nach Art. 4 Nr. 7 DS-GVO neben juristischen auch natürliche Personen sein. Voraussetzung ist, dass derjenige über die Zwecke und Mittel der Verarbeitung entscheidet.

Gegenüber juristischen Personen können Geldbußen auch dann festgesetzt werden, wenn die Ordnungswidrigkeit nicht von einem vertretungsberechtigten Organ oder einer sonstigen für die Leitung verantwortlichen Person begangen wurde. Nach übereinstimmender Auffassung der Aufsichtsbehörden wird die Regelung des § 30 OWiG durch den Anwendungsvorrang der DS-GVO verdrängt. Die Haftung für Mitarbeiterverschulden ergibt sich aus der Anwendung des sog. funktionalen Unternehmensbegriffs des europäischen Primärrechts (Art. 101, 102 AEUV), auf den Erwägungsgrund 150 DS-GVO klarstellend Bezug nimmt. Nach der

Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten ihrer Beschäftigten, ohne dass eine Kenntnis oder gar Anweisung der Geschäftsführung oder auch nur eine Verletzung der Aufsichtspflicht für die Zurechnung erforderlich ist. Auch die Regelung des § 130 OWiG wird durch das europäische Sekundärrecht verdrängt.

Ausnahme ist der sog. Mitarbeiter-Exzess, also eine Handlung, die nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zuzurechnen ist. Hier werden Beschäftigte einer verantwortlichen Stelle richtigerweise zu eigenen Verantwortlichen, womit auch gegen sie ein Bußgeld festgesetzt werden kann.

Überhaupt nicht in Frage kommen Bußgelder gegen Datenschutzbeauftragte, da ihnen in der DS-GVO keine eigene Verantwortlichkeit zugewiesen wird.

Wybitul: Diese Beschränkung des Adressatenkreises von Bußgeldern auf Verantwortliche und Auftragsverarbeiter durch die Datenschutzbehörden ist sinnvoll; leider ist dieser Ansatz im deutschen Ordnungswidrigkeitenrecht nicht zwingend. Im OWiG gibt es verschiedene Vorschriften, die es Behörden ermöglichen könnten, nicht nur gegen das Unternehmen, sondern auch gegen Manager und Mitarbeiter Bußgelder zu verhängen. Mögliche Anknüpfungspunkte wären etwa §§ 30, 130 und 9 OWiG, die auch ein Vorgehen gegen einzelne Beteiligte denkbar scheinen lassen. Insofern ist die Klarstellung wichtig, dass die Behörden diese Vorschriften nicht anwenden, um gegen einzelne Entscheidungsträger vorzugehen.

Eine andere Fallkonstellation ist der von *Frau Thiel* bereits angesprochene sog. Mitarbeiter-Exzess. Verarbeitet ein Mitarbeiter personenbezogene Daten eigenmächtig, kann sich die Verantwortlichkeit für diese Datenverarbeitung bei eigenmächtigen Handlungen einzelner Beschäftigter von Unternehmen oder Behörden zu diesen Beschäftigten verschieben, der sog. Mitarbeiter-Exzess. Der *LfDI Baden-Württemberg* hat z.B. kürzlich gegen einen Polizeibeamten ein Bußgeld verhängt. Dieser Beamte hatte polizeiliche Datenbanken für private Zwecke genutzt. Der *LfDI* kam daher zu dem Ergebnis, dass dieses Handeln nicht mehr der Polizeibehörde zugerechnet werden kann, und verhängte ein Bußgeld gegen den Beamten. Das halte ich für richtig. Denn in einem solchen Fall legt halt nicht mehr der Dienstherr, sondern der einzelne Beamte die Zwecke der Verarbeitung fest. Dadurch wird er selbst Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO – und damit auch Täter der datenschutzrechtlichen Ordnungswidrigkeit. Diese Grundsätze gelten nicht nur bei Behörden, sondern ebenso bei eigenmächtig handelnden Beschäftigten privater Unternehmen.

ZD: *Die Spanne der bislang unter Geltung der DS-GVO in den einzelnen EU-Mitgliedstaaten verhängten Bußgelder ist groß. Sie reicht von einigen hundert Euro bis zu dreistelligen Millionenbeträgen. In einigen EU-Mitgliedstaaten scheinen die Behörden im Vergleich besonders scharf durchzugreifen. Hängt die Höhe eines drohenden Bußgelds demnach vor allem von der zuständigen Datenschutzbehörde ab?*

Thiel: Nein, natürlich nicht! Es wäre fatal, wenn ein solcher Eindruck entstünde. Art. 83 Abs. 2 DS-GVO nennt ja ganz klar die Kriterien, welche die Bußgeldhöhe beeinflussen: Das sind z.B. die Art und Schwere des Verstoßes, die Frage, ob Vorsatz oder Fahrlässigkeit vorlag, ob der Verantwortliche Wiederholungstäter ist, welche Maßnahmen er zur Eindämmung des Schadens ergriffen hat, usw. Das schon erwähnte WP 253 macht auch hierzu detailliertere Ausführungen, aber trotzdem liegt natürlich noch einiges an Abstimmungsarbeit vor uns, bevor wir von einer europaweit harmonisierten Bußgeldpraxis sprechen können.

Innerhalb der deutschen *Datenschutzkonferenz (DSK)* hat sich der *Arbeitskreis (AK) Sanktionen* des Themas der Bußgeldbemessung angenommen und hierzu ein entsprechendes Konzept entwickelt, das die *DSK* am 16.10.2019 veröffentlicht hat. Das Konzept gestaltet im Wesentlichen die Vorgaben des Art. 83 DS-GVO aus, bietet aktuell die Grundlage für die Bußgeldzumessung in der Sanktionspraxis der deutschen Aufsichtsbehörden und ist auf Fortentwicklung angelegt. Ziel des Konzepts ist es, den Datenschutzaufsichtsbehörden eine einheitliche Methode für eine systematische, transparente und nachvollziehbare Bemessung von Geldbußen zur Verfügung zu stellen. Mit seiner Veröffentlichung verbindet die *DSK* das Ziel, einen Beitrag zur Transparenz im Hinblick auf die Durchsetzung des Datenschutzrechts zu leisten. Verantwortliche und Auftragsverarbeiter sollen in die Lage versetzt werden, die Entscheidungen der Aufsichtsbehörden nachzuvollziehen.

Das Konzept sieht vor, dass Unternehmen zunächst anhand ihres Umsatzes in eine von 20 Größenklassen eingeteilt werden. Daraus ergibt sich ein bestimmter Grundbetrag, der anschließend in sehr differenzierter Weise anhand weiterer Kriterien an den jeweiligen Einzelfall angepasst wird. Denn das Bußgeld muss ja insbesondere, so schreibt es Art. 83 Abs. 1 DS-GVO vor, verhältnismäßig sein, und dies setzt voraus, dass die Art des Verstoßes und das Täterverhalten insgesamt bei der Sanktionierung einbezogen werden müssen. U.a. werden hier z.B. auch eine drohende Zahlungsunfähigkeit oder in der Branche zu erwartende besonders geringe Renditen berücksichtigt. So bleibt es möglich, in jedem Einzelfall den zunächst eingeschlagenen „Bußgeldkorridor" wieder zu verlassen. Bei dieser Vorgehensweise stellt der Umsatz dann lediglich die Grundlage für eine Bußgeldberechnung dar.

ZD: *Herr Wybitul, wie sind hierzu ihre bisherigen Erfahrungen aus der Beratungspraxis?*

Wybitul: Wir haben bereits einige Fälle bearbeitet, in denen Bußgelder auf der Grundlage des von *Frau Thiel* genannten Bußgeldmodells festgelegt wurden. Unser Eindruck ist, dass das Konzept der Behörden zu deutlich höheren Geldbußen führt, als sie bislang in Deutschland verhängt wurden. Aus rechtlicher Sicht halte ich das Bußgeldmodell für problematisch, weil es vor allem umsatzbasiert ist. Ein hoher Umsatz führt daher fast automatisch zu einem hohen Bußgeld – auch bei leichten Verstößen. Zwar müssen die von nach Art. 83 Abs. 1 DS-GVO verhängten Bußgelder „wirksam und abschreckend" sein. Nach dieser Vorschrift müssen sie aber auch „verhältnismäßig" sein.

Verhältnismäßig bedeutet bei Bußgeldern vor allem, dass sie tat- und schuldangemessen sein müssen. Da habe ich bei einem derart vom Umsatz eines Unternehmens geprägten Berechnungsmodell einige Zweifel. Das zeigt sich auch bei einem Vergleich mit dem Kartellrecht, das ja Vorbild der Bußgeldmechanik des Art. 83 DS-GVO war. Dort unterscheiden die Behörden zwischen Bußgeldrahmen und der konkreten Bemessung des Bußgelds im Einzelfall. Die flexible Regelung des Art. 83 DS-GVO zum Bußgeldrahmen soll vor allem verhindern, dass umsatzstarke Marktteilnehmer Bußgelder einfach „einpreisen" könnten, die Behörden auf der Basis starrer Maximalbeträge verhängen. Dies ist in Bezug auf den Bußgeldrahmen nachvollziehbar – so können die Datenschutzbehörden auch bei großen Marktteilnehmern wirksame Bußgelder verhängen. Bei einem global agierenden Konzern hätte etwa eine starre Obergrenze von € 20 Mio. eine weniger abschreckende Wirkung als die in Art. 83 DS-GVO vorgesehene Obergrenze von bis zu 4% des globalen Umsatzes.

Das führt aber nicht dazu, dass die Behörden neben der Bestimmung des Bußgeldrahmens auch bei der Bemessung einzelner Bußgelder zwingend den Umsatz heranziehen dürften. Das zeigt sich auch bei einem Vergleich mit dem Kartellrecht. Dort ziehen die Behörden für den Bußgeldrahmen den gesamten

Umsatz ebenfalls einer wirtschaftlichen Einheit heran. Die einzelnen Bußgelder bemessen die Behörden dort aber auf der Grundlage des sog. „befangenen Umsatzes". Das ist der Umsatz, den man mit Produkten oder Leistungen erzielt hat, deren Absatz der Kartellverstoß begünstigt hat. Wenn ein Unternehmen durch Datenschutzverstöße also tatsächlich Umsätze erzielt oder Ausgaben einspart, kann dies i.R.d. Bußgeldzumessung durchaus maßgeblich sein. Liegen diese Voraussetzungen nicht vor, kann eine umsatzbezogene Bußgeldbemessung unverhältnismäßig sein. Das eröffnet einige Möglichkeiten für die erfolgreiche Verteidigung von Unternehmen gegen zu hohe Bußgelder.

ZD: *Das von der DSK veröffentlichte Modell soll mehr Transparenz schaffen und Verantwortliche sowie Auftragsverarbeiter in die Lage versetzen, die Entscheidungen der Aufsichtsbehörden nachzuvollziehen. Hat das neue Modell zur Folge, dass man künftig drohende Bußgelder im Voraus genau berechnen kann? Besteht nicht das Risiko, dass Unternehmen vorab i.R.e. wirtschaftlichen Gesamtbetrachtung prüfen könnten, ob zu erwartende Gewinne höher als mögliche Bußgelder ausfallen könnten?*

Wybitul: Nein, auf den Euro genau kann man drohende Bußgelder auch mit dem Bußgeldmodell der deutschen Datenschutzbehörden nicht berechnen. Dafür haben die Behörden zu große Spielräume dabei, wie sie die Umstände und die Folgen eines Datenschutzverstoßes einschätzen bzw. bewerten. Das neue Bußgeldmodell gibt eher einen Korridor vor, in dem sich die Bußgelder für konkret festgestellte Datenschutzverstöße künftig bewegen werden. Insofern können Risikomanager künftig mögliche DS-GVO-Bußgelder auf der Grundlage des neuen Modells einigermaßen präzise vorhersagen. Hier kann man ja auch unterschiedliche Szenarien rechnen, etwa einen „best case", einen „worst case" und einen „Normalfall". Gleichwohl halte ich es für sehr unwahrscheinlich, dass Unternehmen mögliche Bußgelder künftig einfach einpreisen könnten. Zum einen würde ein solches Vorgehen schon nach den Kriterien des neuen Bußgeldmodells zu einer drastischen Erhöhung des zu verhängenden Bußgelds führen. Denn hier würden die Behörden voraussichtlich eine besonders schwere Form einer vorsätzlichen Tatbegehung annehmen. Zum anderen führt die umsatzbasierte Berechnung des Bußgelds gerade bei großen Unternehmen oder Konzernen zu sehr hohen Beträgen, die ein Vorstand oder ein Aufsichtsrat allein ihrer Höhe wegen keinesfalls einfach einpreisen kann.

ZD: *Stichwort „Kooperation" – Verantwortliche sind nach Art. 31 DS-GVO ja ohnehin verpflichtet, mit Datenschutzbehörden zusammenzuarbeiten. Darüber hinaus müssen Verantwortliche viele Datenschutzverstöße nach Art. 33 DS-GVO sogar selbst der zuständigen Behörde melden. Gibt es im Datenschutzrecht dann überhaupt so etwas wie eine „Selbstbelastungsfreiheit" für Verantwortliche?*

Wybitul: In dieser Frage sprechen Sie zwei Ebenen an, die man trennen muss. Zum einen gibt es im – dem Bußgeldverfahren in der Regel vorgelagerten – Verwaltungsverfahren die in Art. 31 DS-GVO geregelte Mitwirkungspflicht für Verantwortliche. Diese Kooperationspflicht ergänzt die in Art. 58 Abs. 1 DS-GVO geregelten Untersuchungsbefugnisse der Datenschutzbehörden im Verwaltungsverfahren und betrifft das behördliche Prüfverfahren, welches dem ordnungswidrigkeitenrechtlichen Ermittlungsverfahren vorgelagert ist. Auf dieser Ebene müssen Verantwortliche grundsätzlich mit der Aufsichtsbehörde kooperieren. Auf derselben Ebene steht auch die Meldepflicht des Verantwortlichen nach Art. 33 DS-GVO. Für diesen Fall regelt § 43 Abs. 4 BDSG ausdrücklich, dass Datenschutzbehörden eine Datenpannenmeldung in einem späteren Bußgeldverfahren nur mit Zustimmung des Verantwortlichen verwenden dürfen. Zwar sind manche Datenschutzexperten der Meinung, dass diese Regelung des deutschen Gesetzgebers unionsrechtswidrig ist. Momentan ist sie allerdings geltendes Recht, sodass eine Sanktionierung derzeit nicht zulässig wäre. Auf einer zweiten Ebene steht dann das eigentliche Bußgeldverfahren nach dem OWiG. Es ist insbesondere umstritten, ob juristische Personen Selbstbelastungsfreiheit genießen. Nach einer Ansicht sollten Unternehmen oder andere juristische Personen bzw. deren Vertreter auch zu Aussagen verpflichtet sein, die das Unternehmen belasten könnten. Das halte ich allerdings nach geltendem Recht wegen Art. 6 Abs. 1 EMRK und Art. 47 Abs. 2 GRCh für problematisch. Die dort geregelten Grundsätze eines fairen Verfahrens schließen eine Selbstbelastungspflicht auch juristischer Personen aus. Dementsprechend regelt auch Art. 83 Abs. 2 lit. f DS-GVO, dass die Datenschutzbehörden den Umfang der Kooperation des Verantwortlichen bei der Festlegung des Bußgelds berücksichtigen sollen. Diese Vorgabe ergibt nur dann Sinn, wenn der Verantwortliche im Bußgeldverfahren nicht zur Zusammenarbeit mit der Datenschutzbehörde verpflichtet ist. Die Kooperationspflicht des Art. 31 DS-GVO greift auf dieser Ebene demnach nicht.

Thiel: Auch ich bin der Auffassung, dass Art. 31 DS-GVO lediglich für das Verwaltungsverfahren gilt. Im Bußgeldverfahren gelten dagegen die Regelungen des OWiG. Wir trennen beide Verfahren immer sehr sorgfältig. Im Verwaltungsverfahren ist der Verantwortliche nach Art. 31 DS-GVO verpflichtet, der Aufsichtsbehörde Auskunft zu erteilen. Im Bußgeldverfahren besteht dagegen keine Mitwirkungspflicht des Betroffenen; er hat vielmehr das Recht, zu schweigen, und muss auch keine Tatsachen oder Beweismittel angeben (§§ 163a Abs. 3 Satz 2, 136 Abs. 1 Satz 2 StPO i.V.m. § 46 Abs. 1 OWiG). Auch wenn die OWiG-Vorschrift streng genommen auf natürliche Personen zugeschnitten ist, wenden wir diese Regelung i.Ü. auch auf juristische Personen als Verantwortliche an, da das Bußgeldverfahren an das Strafverfahren angelehnt ist und dort tatsächlich der Grundsatz der Selbstbelastungsfreiheit gilt. Allerdings beschränkt sich das Recht, zu schweigen, natürlich nur auf den konkreten Tatvorwurf in einem bereits eröffneten Bußgeldverfahren. Die Kooperationspflicht nach Art. 31 DS-GVO wird also nicht gänzlich ausgehebelt.

Soweit bei der besonderen Konstellation der Datenpannenmeldung vereinzelt die Auffassung vertreten wird, § 43 Abs. 4 BDSG sei europarechtswidrig, aber gleichwohl geltendes Recht, verweise ich hier auf den Anwendungsvorrang des Europarechts. D.h., ist eine europarechtskonforme Auslegung nicht möglich, überlagert die DS-GVO die jeweilige nationale Bestimmung, die dann von uns Aufsichtsbehörden nicht anzuwenden wäre. Allerdings bin ich der Auffassung, dass die Regelung des § 43 Abs. 4 BDSG auf eine Öffnungsklausel, nämlich Art. 83 Abs. 8 DS-GVO, zurückgreift und daher nicht den europarechtlichen Grundlagen widerspricht. Außerdem kennt das EU-Recht selbst das Verbot der Selbstbezichtigung und den Grundsatz des fairen Strafverfahrens.

ZD: *Noch eine prozessuale Frage – nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO müssen Unternehmen und andere Verantwortliche ja nachweisen können, dass sie die Vorgaben der DS-GVO umsetzen. Im zivilrechtlichen Kontext wird das oft als Beweiszumessungsregel bewertet. Drohen Unternehmen nun ggf. schon dann Bußgelder, wenn sie nicht nachweisen können, dass sie die DS-GVO richtig anwenden?*

Wybitul: Nein, eine solche Auslegung wäre schon von den Grundrechten und Grundfreiheiten der jeweiligen Verantwortlichen und Auftragsverarbeiter her nicht zu rechtfertigen. Die DS-GVO geht zwar datenschutzrechtlichen Regelungen der Mitgliedstaaten vor. Sie setzt aber natürlich nicht die EU-Grundrechte außer Kraft. Dementsprechend verweist Art. 83 Abs. 8 DS-GVO darauf, dass die Ausübung der Bußgeldbefugnisse der

Behörden angemessenen Verfahrensgarantien nach dem Unionsrecht und dem Recht der Mitgliedstaaten unterliegt. Damit finden u.a. die Justizgrundsätze der EU Anwendung. Und die Unschuldsvermutung ergibt sich hier ja aus Art. 48 GRCh.

Übrigens halte ich auch die Annahme für falsch, dass die in Art. 5 Abs. 2 sowie Art. 24 Abs. 1 DS-GVO geregelte Rechenschaftspflicht zu einer zivilrechtlichen Beweislastumkehr führe. Die Vorschriften sehen letztlich lediglich eine Nachweispflicht gegenüber den Datenschutzbehörden vor. Diese datenschutzrechtliche Rechenschaftspflicht führt aber weder zu einer Abkehr von den grundsätzlichen zivilprozessualen Maßstäben für die Verteilung der Beweislast noch zu einem Abweichen von der Unschuldsvermutung im Bußgeldverfahren. Dies zeigt sich zum einen daran, dass weder Art. 5 Abs. 2 noch Art. 24 Abs. 1 DS-GVO konkrete Regeln für die zivilprozessuale oder gar ordnungswidrigkeitenrechtliche Beweislast vorsehen. Zudem zeigt auch Erwägungsgrund 82 DS-GVO deutlich, dass die DS-GVO allein eine Nachweispflicht gegenüber den zuständigen Behörden im Verwaltungsverfahren vorsieht – aber nicht gegenüber betroffenen Personen oder der Bußgeldstelle.

ZD: *Frau Thiel, wie ist die Sicht der Datenschutzbehörden zu dieser Frage?*

Thiel: Eine Beweislastumkehr sehe ich in der Regelung des Art. 5 Abs. 2 DS-GVO ebenfalls nicht. Die Vorschrift stellt die Pflicht des Verantwortlichen fest, Nachweise zur pflichtgemäßen Erfüllung der Datenschutzregelungen vorzuhalten. Bei der Nachweispflicht nach Art. 5 Abs. 2 DS-GVO handelt es sich also um eine echte Handlungspflicht des Verantwortlichen, die nach Art. 83 Abs. 5 lit. a DS-GVO auch von den Bußgeldtatbeständen umfasst ist. Diese Pflicht kann man etwa durch Vorlage eines Verfahrensverzeichnisses oder sonstiger schriftlicher Dokumente erfüllen. Verfügt eine verantwortliche Stelle über gar keine Nachweisdokumente, kann dieser Verstoß gegen die Pflicht aus Art. 5 Abs. 2 DS-GVO auch sanktioniert werden. Solche Bußgelder sind auch schon festgesetzt worden. Litauen und Griechenland haben bereits Bußgelder i.H.v. € 61.500,– bzw. € 150.000,– u.a. deshalb festgesetzt, weil Unternehmen ihren Rechenschaftspflichten nicht oder nicht ausreichend nachgekommen sind.

Im Ordnungswidrigkeitenverfahren selbst gilt natürlich verfahrensrechtlich die Unschuldsvermutung, die Ordnungswidrigkeitenbehörde muss also den Verstoß nachweisen. Die Beweislast liegt bei der Bußgeldbehörde wie im Strafverfahren bei der Staatsanwaltschaft. Das schließt aber den Tatbestand an sich nicht aus. Zivilrechtlich – also im Verhältnis zwischen dem Verantwortlichen und dem Betroffenen – gilt in Verfahren wegen Schadensersatz ohnehin Art. 82 Abs. 3 DS-GVO, wonach der Verantwortliche nachzuweisen hat, dass er für einen Schaden nicht verantwortlich ist.

ZD: *In den Medien und in Fachpublikationen wird regelmäßig berichtet, dass großen datenverarbeitenden Unternehmen sogar Bußgelder in Milliardenhöhe drohen können. Art. 83 DS-GVO legt den maximalen Bußgeldrahmen mit 2% bzw. 4% des weltweiten Vorjahresumsatzes fest. Was ist in diesem Zusammenhang eigentlich mit dem „weltweiten" Umsatz gemeint?*

Thiel: Wir gehen hierbei vom kartellrechtlich-funktionalen Unternehmensbegriff aus. D.h., ein Unternehmen wird als Wirtschaftseinheit verstanden, zu der die Muttergesellschaft und alle abhängigen Tochtergesellschaften gehören. In der für das Bußgeldverfahren maßgeblichen Vorschrift des Art. 83 DS-GVO ist in der englischen Fassung von „undertaking" (für Unternehmen) die Rede. Dieser Begriff wird auch im europäischen Kartellrecht verwendet. Demgemäß haben sich die europäischen Aufsichtsbehörden im WP 253 der Auffassung angeschlossen, dass der kartellrechtliche Unternehmensbegriff maßgeblich ist. In unserem Kurzpapier Nr. 2 zu Aufsichtsbefugnissen und Sanktionen haben wir uns in der *DSK* ebenfalls auf diese Lesart verständigt. Mir ist bewusst, dass der Erwägungsgrund 150 DS-GVO in diesem Zusammenhang nur davon spricht, dass der Begriff in dieser Weise so verstanden werden „sollte", und dass dies in der Auslegung deshalb nicht unumstritten ist. M.E. ist der Begriff „sollte" aber lediglich dem Umstand geschuldet, dass Erwägungsgründe keinen verfügenden Charakter haben, eine Einschränkung der Aussage ist damit nicht verbunden.

Wybitul: Nach den bisherigen Aussagen der *DSK* ist bei der Festlegung von Bußgeldrahmen der jeweilige Konzernumsatz heranzuziehen. Auch die im Vereinigten Königreich angekündigten hohen Bußgelder legen nahe, dass die dortige Datenschutzbehörde *ICO* den Bußgeldrahmen anhand des jeweiligen Konzernumsatzes bestimmt hat.

Die DS-GVO ist in diesem Punkt allerdings weniger eindeutig, als man annehmen könnte. Art. 83 Abs. 4, 5 und 6 DS-GVO nennt aber eindeutig nur den weltweit erzielten Jahresumsatz des Unternehmens als Bezugsgröße. Zwar sieht Erwägungsgrund 150 Satz 3 DS-GVO durch einen recht vage formulierten Verweis auf Art. 101 und Art. 102 AEUV wohl vor, dass Datenschutzbehörden den kartellrechtlichen Unternehmensbegriff zu Grunde legen könnten. Erwägungsgründe sind allerdings anders als die Artikel der DS-GVO keine verbindlichen Rechtsvorschriften. Sie sind vielmehr Auslegungshilfen. Mir erscheint sehr fraglich, wie man eine derart wesentliche Erweiterung des potenziellen Bußgeldrahmens allein auf einen Erwägungsgrund stützen will. Und eine Auslegung gegen den klaren Wortlaut von Art. 83 DS-GVO halte ich für problematisch. Daher ist der Bezug auf den kartellrechtlichen Unternehmensbegriff rechtlich sehr problematisch.

Natürlich lässt sich darüber streiten, ob man eine derart wesentliche Erweiterung des potenziellen Bußgeldrahmens allein auf einen Erwägungsgrund stützen darf. Ich persönlich bin da aber eher skeptisch.

Was außerdem in diesem Zusammenhang oft aus dem Blick gerät und was man keinesfalls außer Acht lassen sollte, ist, dass der Unternehmensumsatz nur ein Bemessungskriterium ist. Daneben legt die DS-GVO in Art. 83 Abs. 2 fest, welche Kriterien bei der Bußgeldbemessung innerhalb des möglichen Rahmens berücksichtigt werden müssen.

ZD: *Bisher haben wir allgemein über Bußgelder als mögliche Folge von Datenschutzverstößen gesprochen. Zum Abschluss unseres Interviews würde ich gerne noch einen etwas weiteren Blick auf den Weg von einem Datenschutzverstoß bis zu einem Bußgeld nehmen. Frau Thiel, wie laufen Ermittlungs- und Bußgeldverfahren von Datenschutzbehörden denn typischerweise ab?*

Thiel: Das gestaltet sich ganz unterschiedlich, weil es verschiedene Anlässe für diese Verfahren gibt. Das kann eine Beschwerde betroffener Personen sein, eine Datenpannenmeldung gem. Art. 33 DS-GVO, eine anlasslose Prüfung, eine Nachkontrolle oder auch eine Übernahme von der Polizei bzw. der Staatsanwaltschaft, wie es etwa beim unsachgemäßen Einsatz von Dash Cams häufig der Fall ist. Ganz grundsätzlich ermitteln wir unabhängig vom Auslöser zunächst einmal den genauen Sachverhalt. Nur so können wir alle relevanten Aspekte bewerten, wie sie in Art. 83 Abs. 2 DS-GVO aufgelistet sind und wie es das WP 253 von uns verlangt. Auf Basis dieser Bewertung können wir dann entscheiden, ob wir in ein Ordnungswidrigkeitenverfahren einsteigen, in dessen Rahmen es zu einem Bußgeld kommen kann, aber nicht muss. Der Verantwortliche hat es i.Ü. selbst in der Hand, ob ein Bußgeldverfahren eingeleitet wird oder nicht. Datenschutzkonformes Verhalten lässt Anlässe wie die genannten gar nicht erst entstehen, und damit ist ein Bußgeldverfahren von vornherein ausgeschlossen.

ZD: *Herr Wybitul, deckt sich diese Beschreibung von Frau Thiel mit ihren Erfahrungen und was bedeutet das für Unternehmen?*

Wybitul: Unsere Erfahrungen aus laufenden DS-GVO-Bußgeldverfahren decken sich mit den Feststellungen von *Frau Thiel*. Aus Unternehmensperspektive ist es daher für eine effektive Vorbereitung auf drohende oder mögliche Bußgeldverfahren vor allem wichtig, mögliche Auslöser für Ermittlungs- oder Bußgeldverfahren in den Blick zu nehmen. Es gibt einige typische Situationen, die häufig den ersten Schritt hin zu einem Bußgeld darstellen, z.B. Beschwerden betroffener Personen bei einer Aufsichtsbehörde. Gerade im Bereich des Beschäftigtendatenschutzes beschweren sich Beschäftigte z.B. häufig eher in der Endphase ihres Beschäftigungsverhältnisses bei Datenschutzbehörden. Wie schon angesprochen dürfen Datenschutzbehörden den Inhalt von Datenpannenmeldungen in einem Bußgeldverfahren zwar nicht verwenden. Allerdings können Datenschutzbehörden eine solche Meldung als Anlass für eigene Ermittlungen (z.B. in Form einer Datenschutzüberprüfung) nehmen. Wie *Frau Thiel* richtig sagt, führen die Datenschutzbehörden inzwischen auch vermehrt Datenschutzprüfungen zu bestimmten Themenbereichen bei zufällig ausgewählten Unternehmen durch. Unternehmen sollten bei der Planung von Verteidigungsstrategien gegen DS-GVO-Bußgelder daher nicht erst bei schon laufenden Verfahren ansetzen. Vielmehr sollten Unternehmen bei ihrer Planung auch typische konfliktbeladene oder risikoreiche Datenverarbeitungsszenarien in den Blick nehmen. Sehr hilfreich sind auch sog. „Verteidigungshandbücher" mit Ablaufplänen, Regelungen zu internen Zuständigkeiten, einem Leitfaden für Durchsuchungen durch die Datenschutzbehörden, Vorlagen für Pressemeldungen und anderen vorab vorbereiteten Notfallmaßnahmen. Wenn die Behörde vor der Tür steht oder ein Whistleblower auf massive Missstände beim Datenschutz hinweist, kann es enorm hilfreich sein, wenn klar ist, wer wen anruft und wer welche Aufgabe erledigt. Wenn man diese Fragen erst klärt, wenn das Problem aufgetreten ist, verliert man Zeit und macht Fehler.

Neben der Sensibilisierung auf mögliche Auslöser für Bußgeldverfahren sollten Unternehmen sowohl die Wahrscheinlichkeit der Verhängung eines Bußgelds als auch dessen potenzielle Höhe evaluieren. Dies gilt insbesondere im Hinblick auf das am 16.10.2019 veröffentlichte Bußgeldmodell der *DSK*. Das Modell behebt also in gewissem Umfang die bisher bestehende Unsicherheit in Bezug auf die Höhe etwaiger künftig verhängter Bußgelder. Aus dieser Abschätzbarkeit der Bußgeldhöhe können sich für Unternehmen neue bzw. konkretisierte Verpflichtungen ergeben, sofern das Risiko einer datenschutzbehördlichen Verfolgung eines Datenschutzverstoßes und einer einhergehenden Bußgeldverhängung hinreichend hoch ist. Insbesondere ist hier an die mögliche Verpflichtung zur Bildung von Rückstellungen zu denken. Zwar bestand diese Verpflichtung bereits bisher, durch die Berechenbarkeit der potenziellen Bußgeldhöhe werden die zu bilanzierenden Beträge jedoch um einiges konkreter. Bei börsennotierten Unternehmen kommen ggf. sogar wertpapierhandelsrechtliche Ad-hoc-Publizitätspflichten in Betracht.

Die wesentlichste Veränderung für Unternehmen ist m.E., dass wir uns künftig auf mehr und höhere Datenschutzbußgelder einstellen können. Und wir werden mehr Gerichtsverfahren wegen Bußgeldern nach Art 83 DS-GVO sehen.

ZD: Vielen Dank für das Gespräch.

Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen, und Tim Wybitul, Mitherausgeber der ZD sowie Partner und Datenschutzbeauftragter bei Latham & Watkins in Frankfurt/M., im Gespräch mit Anke Zimmer-Helfrich, Chefredakteurin der ZD.