ARTIKEL-29-DATENSCHUTZGRUPPE

17/DE

WP 253

Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679

angenommen am 3. Oktober 2017

Diese Gruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingerichtet. Sie ist ein unabhängiges europäisches Beratungsgremium für den Schutz personenbezogener Daten und der Privatsphäre. Ihre Aufgaben werden in Artikel 30 der Richtlinie 95/46/EG und Artikel 15 der Richtlinie 2002/58/EG beschrieben.

Das Sekretariat wird von der Direktion C (Grundrechte und Unionsbürgerschaft) der Europäischen Kommission, Generaldirektion für Justiz, B-1049 Brüssel, Belgien, Büro MO-59 03/075, gestellt.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

DIE ARBEITSGRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER

VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf die Artikel 29 und 30 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE LEITLINIEN ANGENOMMEN:

Inhaltsverzeichnis:

I. Einleitung 4
II. Grundsätze 5
III. Bewertungskriterien in Artikel 83 Absatz 2 9
IV. Schlussfolgerung 18

I. Einleitung

Die EU hat eine umfassende Reform der europäischen Datenschutzbestimmungen abgeschlossen. Die Reform stützt sich auf mehrere Säulen (Schlüsselkomponenten): kohärente Regeln, vereinfachte Verfahren, koordinierte Maßnahmen, Einbindung der Nutzer, wirksamere Informationsbereitstellung und stärkere Durchsetzungsbefugnisse.

Die Zuständigkeiten der Datenverantwortlichen und der Datenverarbeiter wurden erweitert, um sicherzustellen, dass die personenbezogenen Daten von Personen wirksam geschützt werden. Die Aufsichtsbehörden besitzen Befugnisse, mit denen sie dafür sorgen können, dass die Grundsätze der Datenschutzgrundverordnung (im Folgenden „die Verordnung“) und die Rechte der betroffenen Personen entsprechend dem Wortlaut und dem Geist der Verordnung gewahrt werden.

Die einheitliche Durchsetzung der Datenschutzbestimmungen ist für eine harmonisierte Regelung des Datenschutzes von wesentlicher Bedeutung. Geldbußen sind ein zentraler Aspekt der durch die Verordnung eingeführten neuen Durchsetzungsbestimmungen und bilden zusammen mit den anderen Maßnahmen nach Artikel 58 eine starke Komponente der den Aufsichtsbehörden zur Verfügung stehenden Instrumente.

Das vorliegende Dokument ist zur Verwendung durch die Aufsichtsbehörden bestimmt, damit diese für eine bessere Anwendung und Durchsetzung der Verordnung sorgen können. Es gibt ihre einheitliche Auslegung der Bestimmungen von Artikel 83 der Verordnung und von dessen Wechselbeziehung mit den Artikeln 58 und 70 und den diesbezüglichen Erwägungsgründen wider.

Insbesondere ist der Europäische Datenschutzausschuss (im Folgenden „der Ausschuss“) nach Artikel 70 Absatz 1 Buchstabe e befugt, Leitlinien, Empfehlungen und bewährte Verfahren bereitzustellen, um die einheitliche Anwendung der Verordnung zu fördern, und Artikel 70 Absatz 1 Buchstabe k regelt die Ausarbeitung von Leitlinien zur Festsetzung von Geldbußen.

Die vorliegenden Leitlinien sind nicht erschöpfend und enthalten keine Erläuterungen zu den Unterschieden, die zwischen den verwaltungs-, zivil- oder strafrechtlichen Systemen in Bezug auf die Verhängung verwaltungsrechtlicher Sanktionen allgemein bestehen.

Um ein einheitliches Vorgehen bei der Verhängung der Geldbußen sicherzustellen, bei dem alle Grundsätze der vorliegenden Leitlinien gebührend berücksichtigt werden, hat sich der Ausschuss auf eine einheitliche Auslegung der Bewertungskriterien nach Artikel 83 Absatz 2 der Verordnung verständigt, und daher haben der Ausschuss und die einzelnen Aufsichtsbehörden vereinbart, diese Leitlinien als gemeinsames Konzept zu verwenden.

II. Grundsätze

Wurde bei der Bewertung des Sachverhalts ein Verstoß gegen die Verordnung festgestellt, muss die zuständige Aufsichtsbehörde die Abhilfemaßnahme(n) ermitteln, die zur Behebung des Verstoßes am besten geeignet ist bzw. sind. Die Bestimmungen von Artikel 58 Absatz 2 Buchstaben b bis j[1] legen fest, mit welchen Maßnahmen die Aufsichtsbehörden gegen Verstöße eines Verantwortlichen oder eines Auftragsverarbeiters vorgehen können. Bei der Wahrnehmung dieser Befugnisse müssen die Aufsichtsbehörden die folgenden Grundsätze beachten:

---

1. Ein Verstoß gegen die Verordnung sollte zur Verhängung „gleichwertiger Sanktionen" führen.

Das Konzept der „Gleichwertigkeit" ist grundlegend dafür, den Umfang der Pflichten der Aufsichtsbehörden zu bestimmen, damit diese ihre Abhilfebefugnisse gemäß Artikel 58 Absatz 2 allgemein sowie Geldbußen im Besonderen einheitlich anwenden.[2]

Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, ***sollte das Schutzniveau in allen Mitgliedstaaten gleichwertig sein*** (Erwägung 10). Erwägung 11 befasst sich mit dem Umstand, dass ein unionsweit gleichwertiges Schutzniveau für personenbezogene Daten unter anderem „*gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung*" erfordert. Des Weiteren werden in Erwägung 13 der Verordnung gleichwertige Sanktionen in allen Mitgliedstaaten und eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden verschiedener Mitgliedstaaten als Möglichkeiten dafür betrachtet, dass „*Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden*".

Verglichen mit der Richtlinie 95/46/EG schafft die Verordnung eine solidere Grundlage für ein höheres Maß an Einheitlichkeit, da sie in den Mitgliedstaaten direkt anwendbar ist. Während die Aufsichtsbehörden im Hinblick auf nationale Verwaltungen, Verantwortliche oder Auftragsverarbeiter „*völlig unabhängig*" handeln (Artikel 52), sind sie zur Zusammenarbeit verpflichtet, „*um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten*" (Artikel 57 Absatz 1 Buchstabe g).

In der Verordnung wird bezüglich der Verhängung von Sanktionen mehr Kohärenz gefordert als in der Richtlinie 95/46/EG. In grenzüberschreitenden Fällen soll Kohärenz in erster Linie durch das Verfahren der Zusammenarbeit und Kohärenz sowie teilweise durch das im Rahmen der neuen Verordnung festgelegte Kohärenzverfahren erreicht werden.

In nationalen Fällen im Geltungsbereich der Verordnung wenden die Aufsichtsbehörden diese Leitlinien im Geist der Zusammenarbeit gemäß Artikel 57 Absatz 1 Buchstabe g und Artikel 63 an, um für eine kohärente Anwendung und Durchsetzung der Verordnung zu sorgen. Obwohl die

[1] Gemäß Artikel 58 Absatz 2 Buchstabe a können Warnungen ausgegeben werden, wenn „beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen". In dem durch diese Bestimmung abgedeckten Fall ist also der Verstoß gegen die Verordnung noch nicht eingetreten.

[2] Selbst in denjenigen EU-Mitgliedstaaten, nach deren Rechtsordnungen die in dieser Verordnung vorgesehenen Geldbußen nicht zulässig sind, müssen die Vorschriften mit der gleichen Wirkung wie die von den Aufsichtsbehörden verhängten Geldbußen angewandt werden (Erwägungsgrund 151). Die Gerichte sind an die Verordnung, nicht aber an diese Leitlinien des Ausschusses gebunden.

Aufsichtsbehörden ihre Wahl der in Artikel 58 Absatz 2 genannten Abhilfemaßnahmen unabhängig treffen können, sollten sie es vermeiden, in vergleichbaren Fällen unterschiedliche Abhilfemaßnahmen anzuwenden.

Das gleiche Prinzip gilt, wenn solche Abhilfemaßnahmen in Form von Geldbußen verhängt werden.

2. Wie alle von den Aufsichtsbehörden gewählten Abhilfemaßnahmen sollten Geldbußen „wirksam, verhältnismäßig und abschreckend" sein.

Wie alle Abhilfemaßnahmen allgemein sollten Geldbußen der Art, der Schwere und den Folgen des Verstoßes angemessen sein, und die Aufsichtsbehörden müssen alle Aspekte des Sachverhalts in kohärenter und objektiv gerechtfertigter Weise bewerten. Was im Einzelfall als wirksam, verhältnismäßig und abschreckend betrachtet wird, hängt auch vom Ziel der Abhilfemaßnahme ab, das heißt davon, ob mit ihr die Verletzung der Bestimmungen behoben oder rechtswidriges Verhalten bestraft werden soll (oder beides).

Die Aufsichtsbehörden sollten sowohl in nationalen Fällen (Artikel 55) als auch in Fällen der grenzüberschreitenden Verarbeitung personenbezogener Daten (gemäß der Begriffsbestimmung in Artikel 4 Nummer 23) eine Abhilfemaßnahme ermitteln, die „*wirksam, verhältnismäßig und abschreckend*" (Artikel 83 Absatz 1) ist.

In den vorliegenden Leitlinien wird berücksichtigt, dass die nationalen Rechtsvorschriften gegebenenfalls zusätzliche Anforderungen an das von den Aufsichtsbehörden anzuwendende Durchsetzungsverfahren vorsehen. Diese können beispielsweise Anforderungen in Bezug auf Adressmeldungen, Formulare und Fristen für Stellungnahmen, Einsprüche, Ausführungen und Zahlungen einschließen.[3]

In der Praxis sollten Anforderungen dieser Art gleichwohl die Wirksamkeit, die Verhältnismäßigkeit und die abschreckende Wirkung von Abhilfemaßnahmen nicht beeinträchtigen.

Eine genauere Bestimmung dieser drei Merkmale (Wirksamkeit, Verhältnismäßigkeit und abschreckende Wirkung) wird sich aus der bei den Aufsichtsbehörden entstehenden Praxis im Bereich Datenschutz und aus den Erfahrungen in anderen Regulierungsbereichen sowie aus der Auslegung dieser Grundsätze im Zuge der Rechtsprechung ergeben.

Damit die von den Aufsichtsbehörden verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sind, sollte für sie die vom EuGH für die Anwendung der Artikel 101 und 102 AEUV festgelegte Definition des Begriffs „Unternehmen" maßgeblich sein, wonach als Unternehmen eine Wirtschaftseinheit **verstanden wird**, zu der gegebenenfalls die Muttergesellschaft und alle abhängigen Tochtergesellschaften gehören. Gemäß dem EU-Recht und der geltenden Rechtsprechung der EU[4] ist ein Unternehmen als Wirtschaftseinheit zu verstehen, die unabhängig von den beteiligten juristischen Personen an wirtschaftlichen Tätigkeiten beteiligt ist (Erwägungsgrund 150).

[3] Als Beispiel sei Irland angeführt, wo die Verfassungsordnung und der Gesetzesentwurf zum Datenschutz vorsehen, dass zunächst zum Sachverhalt der Nichteinhaltung an sich eine förmliche Entscheidung zu treffen und den betroffenen Parteien mitzuteilen ist, bevor die Höhe der Sanktion(en) festgesetzt wird. Im Zuge der Festsetzung der Höhe der Sanktion(en) kann die Entscheidung zum Sachverhalt der Nichteinhaltung an sich nicht erneut erörtert werden.

[4] In der Rechtsprechung des EuGH wird der Begriff wie folgt definiert: „[...] umfasst der Begriff des Unternehmens jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung" (Rechtssache Höfner und Elsner, Rdnr. 21, ECLI:EU:C:1991:161). „unter dem Begriff des Unternehmens [ist] im Rahmen des Wettbewerbsrechts eine im Hinblick auf den jeweiligen

3. Die zuständige Aufsichtsbehörde nimmt „in jedem Einzelfall" eine Bewertung vor.

Geldbußen können wegen ganz unterschiedlicher Verstöße verhängt werden. Artikel 83 der Verordnung legt ein einheitliches Vorgehen bei Verletzungen der in den Absätzen 4 bis 6 ausdrücklich aufgeführten Pflichten fest. Die Rechtsvorschriften der Mitgliedstaaten können die Anwendbarkeit von Artikel 83 auf Behörden und öffentliche Stellen ausweiten, die in dem betreffenden Mitgliedstaat niedergelassen sind. Darüber hinaus können die Rechtsvorschriften der Mitgliedstaaten die Verhängung einer Geldbuße für Verstöße zulassen oder sogar vorschreiben, die nicht in Artikel 83 Absätze 4 bis 6 genannte Bestimmungen betreffen.

Die Verordnung schreibt vor, dass in jedem Einzelfall eine Bewertung erfolgen muss.[5] Artikel 83 Absatz 2 bildet den Ausgangspunkt für eine solche Einzelfallbewertung. Dort heißt es: „*Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt: [...]*". Demnach und vor dem Hintergrund der Erwägung 148[6] liegt es in der Verantwortung der Aufsichtsbehörde, die am besten geeignete(n) Maßnahme(n) zu bestimmen. In den in Artikel 83 Absätze 4 bis 6 aufgeführten Fällen **müssen** bei dieser Auswahl alle Abhilfemaßnahmen berücksichtigt werden, was die Verhängung einer angemessenen Geldbuße entweder zusätzlich zu einer Abhilfemaßnahme gemäß Artikel 58 Absatz 2 oder alleinstehend einschließt.

Geldbußen sind ein wichtiges Instrument, von dem die Aufsichtsbehörden unter angemessenen Umständen Gebrauch machen sollten. Die Aufsichtsbehörden sind dazu angehalten, bei der Anwendung von Abhilfemaßnahmen einem überlegten und ausgewogenen Ansatz zu folgen, durch

---

Vertragsgegenstand bestehende wirtschaftliche Einheit zu verstehen [...], selbst wenn diese wirtschaftliche Einheit rechtlich aus mehreren natürlichen oder juristischen Personen gebildet wird" (Rechtssache Confederación Española de Empresarios de Estaciones de Servicio, Rdnr. 40, ECLI:EU:C:2006:784).

[5] Über die Anwendung der Kriterien in Artikel 83 hinaus sind weitere Bestimmungen vorgesehen, die die Grundlage für diesen Ansatz stärken, darunter Folgende:

- Erwägungsgrund 141: „*Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist*".
- Erwägungsgrund 129: „*Die Befugnisse der Aufsichtsbehörden sollten in Übereinstimmung mit den geeigneten Verfahrensgarantien nach dem Unionsrecht und dem Recht der Mitgliedstaaten unparteiisch, gerecht und innerhalb einer angemessenen Frist ausgeübt werden. Insbesondere sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung dieser Verordnung geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind [...]".*
- Artikel 57 Absatz 1 Buchstabe f: „*[...] sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen [...]*".

[6] „*Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen gegen diese Verordnung zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen verhängt werden. Im Falle eines geringfügigeren Verstoßes oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden. Folgendem sollte jedoch gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, dem vorsätzlichen Charakter des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, der Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen*".

den eine wirksame und abschreckende, aber auch verhältnismäßige Reaktion auf den Verstoß erreicht wird. Es geht darum, Geldbußen weder als letztes Mittel zu betrachten noch vor ihrer Verhängung zurückzuschrecken, sie aber auch nicht derart zu nutzen, dass ihre Wirksamkeit als Instrument eingeschränkt wird.

Wenn der Ausschuss gemäß Artikel 65 der Verordnung zuständig ist, erlässt er einen verbindlichen Beschluss zu Streitigkeiten zwischen Behörden insbesondere zu der Frage, ob ein Verstoß vorliegt. Wenn der maßgebliche und begründete Einspruch die Frage aufwirft, ob die Abhilfemaßnahme mit Verordnung in Einklang steht, wird in dem Beschluss des Ausschusses auch erörtert, inwieweit bei der Geldbuße, die in dem Beschlussentwurf der zuständigen Aufsichtsbehörde vorgeschlagen wird, die Grundsätze der Wirksamkeit, Verhältnismäßigkeit und abschreckenden Wirkung gewahrt werden. Anleitungen des Ausschusses zur Anwendung von Artikel 65 der Verordnung folgen gesondert zur näheren Erläuterung der Art des vom Ausschuss zu treffenden Beschlusses.

---

4. Ein harmonisiertes Vorgehen hinsichtlich Geldbußen im Bereich Datenschutz erfordert die aktive Beteiligung der Aufsichtsbehörden und einen Informationsaustausch zwischen ihnen.

In diesen Leitlinien wird berücksichtigt, dass die Befugnis zur Verhängung von Geldbußen für einige nationale Aufsichtsbehörden im Bereich des Datenschutzes neu ist und zahlreiche Fragen zu Ressourcen, Organisation und Verfahrensweisen aufwirft. Insbesondere können die Beschlüsse, mit denen die Aufsichtsbehörden die ihnen übertragenen Befugnisse zur Verhängung von Geldbußen wahrnehmen, vor nationalen Gerichten angefochten werden.

Mithilfe der in dieser Verordnung vorgesehenen Mechanismen der Zusammenarbeit sollen die Aufsichtsbehörden untereinander sowie gegebenenfalls mit der Kommission zusammenarbeiten, um auf diese Weise den formalen und informalen Informationsaustausch, etwa in Form regelmäßiger Workshops, zu unterstützen. Im Mittelpunkt dieser Zusammenarbeit sollten ihre Erfahrungen und Vorgehensweisen bei der Wahrnehmung ihrer Befugnisse zur Verhängung von Geldbußen stehen, wodurch letztlich eine größere Kohärenz erreicht werden soll.

Dieser proaktive Informationsaustausch könnte zusammen mit der sich entwickelnden Rechtsprechung über die Wahrnehmung dieser Befugnisse dazu führen, dass die Grundsätze oder die genauen Einzelheiten dieser Leitlinien überarbeitet werden.

III. Bewertungskriterien in Artikel 83 Absatz 2

Artikel 83 Absatz 2 enthält eine Auflistung von Kriterien, die die Aufsichtsbehörden anwenden sollen, wenn sie bestimmen, ob und in welcher Höhe eine Geldbuße verhängt werden sollte. Dabei wird keine wiederholte Bewertung der gleichen Kriterien empfohlen, sondern eine Bewertung, bei der gemäß Artikel 83 alle Umstände jedes Einzelfalls berücksichtigt werden.[7]

Die in der ersten Phase der Bewertung gezogenen Schlussfolgerungen können auch in der zweiten Phase zur Festsetzung des Betrags für die Geldbuße verwendet werden, sodass das gleiche Kriterium nicht zwei Mal bewertet werden muss.

In diesem Abschnitt erhalten die Aufsichtsbehörden Anleitung dazu, wie die individuellen Aspekte eines Sachverhalts vor dem Hintergrund der Kriterien in Artikel 83 Absatz 2 zu bewerten sind.

a) Art, Schwere und Dauer des Verstoßes [...];

Fast alle in der Verordnung festgelegten Pflichten der Verantwortlichen und Auftragsverarbeiter werden in den Bestimmungen von Artikel 83 Absätze 4 bis 6 nach ihrer **Art** in Kategorien eingeteilt. Mit der Festlegung von zwei unterschiedlichen Höchstbeträgen für Geldbußen (10 bzw. 20 Mio. EUR) weist die Verordnung bereits darauf hin, dass bei einigen Bestimmungen der Verordnung ein Verstoß schwerer wiegen kann als bei anderen. Aufgrund der Bewertung des Sachverhalts mithilfe der in Artikel 83 Absatz 2 festgelegten allgemeinen Kriterien kann die zuständige Aufsichtsbehörde jedoch entscheiden, dass es in einem bestimmten Fall in stärkerem bzw. geringerem Maße geboten ist, mit einer Abhilfemaßnahme in Form einer Geldbuße zu reagieren. Wurde eine Geldbuße als die geeignete Abhilfemaßnahme oder eine der geeigneten Abhilfemaßnahmen gewählt, erfolgt eine Einordnung gemäß Artikel 83 Absätze 4 bis 6 der Verordnung, um zu bestimmen, welche Geldbuße entsprechend der Art des fraglichen Verstoßes maximal verhängt werden kann.

In Erwägung 148 wird der Begriff des „geringfügigeren Verstoßes“ eingeführt. Ein solcher Verstoß kann eine oder mehrere der in Artikel 83 Absätze 4 bzw. 5 aufgeführten Bestimmungen der Verordnung betreffen. Aufgrund der Bewertung der Kriterien in Artikel 83 Absatz 2 kann die Aufsichtsbehörde jedoch zu der Auffassung gelangen, dass der Verstoß unter den konkreten Umständen des Falls beispielsweise keine erhebliche Gefahr für die Datenschutzrechte der betroffenen Personen darstellt und die fragliche Pflicht in ihrem Kern nicht beeinträchtigt. In solchen Fällen kann die Geldbuße durch eine Verwarnung ersetzt werden (jedoch nicht zwingend).

Die Aufsichtsbehörden werden durch die Erwägung 148 nicht verpflichtet, bei geringfügigeren Verstößen die Geldbuße immer durch eine Verwarnung zu ersetzen („*kann anstelle einer Geldbuße eine Verwarnung erteilt werden*“). Vielmehr bietet er eine Möglichkeit, die nach einer konkreten Bewertung aller Umstände des Einzelfalls genutzt werden kann.

Die Ersetzung einer Geldbuße durch eine Verwarnung ermöglicht die Erwägung 148 auch dann, wenn der Datenverantwortliche eine natürliche Person ist und die voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung bewirken würde. Den Ausgangspunkt bildet die Bewertung der Aufsichtsbehörde, ob angesichts der Umstände des vorliegenden Falls die Verhängung einer Geldbuße erforderlich ist. Wenn sie für die Verhängung einer Geldbuße entscheidet, muss die Aufsichtsbehörde auch prüfen, ob die zu verhängende Geldbuße für eine natürliche Person eine unverhältnismäßige Belastung darstellen würde.

[7] Die Festsetzung der zu verhängenden Sanktion kann gesondert erfolgen, nachdem die Fragestellung untersucht wurde, ob aufgrund der nationalen Verfahrensvorschriften, die sich aus den verfassungsrechtlichen Anforderungen in einigen Ländern ergeben, ein Verstoß vorliegt. Dies kann den Inhalt und die Ausführlichkeit eines von der federführenden Aufsichtsbehörde in einem solchen Land vorgelegten Beschlussentwurfs einschränken.

In der Verordnung wird für spezifische Verstöße kein bestimmter Betrag festgelegt, sondern lediglich eine Obergrenze (Höchstbetrag). Dies kann als Hinweis darauf gelten, dass ein Verstoß gegen die in Artikel 83 Absatz 4 genannten Pflichten weniger schwerwiegend ist als ein Verstoß gegen die Pflichten gemäß Artikel 83 Absatz 5. Was jedoch eine wirksame, verhältnismäßige und abschreckende Reaktion auf einen Verstoß gegen Artikel 83 Absatz 5 ist, hängt von den Umständen des Einzelfalls ab.

Es ist anzumerken, dass Verstöße gegen die Verordnung, die gemäß Artikel 83 Absatz 4 ihrer Art nach eigentlich in die Kategorie „*von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes*“ fallen würden, unter bestimmten Umständen auch in eine höhere Kategorie (20 Mio. EUR) eingestuft werden können. Dies wäre wahrscheinlich dann der Fall, wenn die fraglichen Verstöße zuvor bereits Gegenstand einer Anweisung[8] der Aufsichtsbehörde waren, die vom Verantwortlichen oder Auftragsverarbeiter nicht befolgt wurde[9] (Artikel 83 Absatz 6). Die Bestimmungen der nationalen Rechtsvorschriften können in der Praxis einen Einfluss auf diese Bewertung haben.[10] Neben der Art des Verstoßes ist auch die Beurteilung „*des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens*“ ein Indikator für die **Schwere** des Verstoßes. Liegen in einem bestimmten Einzelfall mehrere verschiedene Verstöße gleichzeitig vor, kann die Aufsichtsbehörde bei der Verhängung einer wirksamen, verhältnismäßigen und abschreckenden Geldbuße den Höchstbetrag für den schwerwiegendsten Verstoß zugrunde legen. Wenn also ein Verstoß gegen Artikel 8 und Artikel 12 festgestellt wurde, kann die Aufsichtsbehörde gegebenenfalls die Abhilfemaßnahmen gemäß Artikel 83 Absatz 5 auswählen, die für die Kategorie des schwerwiegendsten Verstoßes (d. h. gegen

[8] In Artikel 58 Absatz 2 sind die folgenden Anweisungen vorgesehen:

- den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,
- den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,
- den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen,
- eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
- die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,
- die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,
- die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

[9] Bei der Anwendung von Artikel 83 Absatz 6 sind zwingend die nationalen verfahrensrechtlichen Vorschriften zu berücksichtigen. Durch die nationalen Rechtsvorschriften wird festgelegt, wie eine Anweisung ausgestellt und gemeldet wird, ab wann sie gilt und ob es eine Anpassungsfrist (Zeitraum, in dem auf die Erfüllung der Anweisung hingearbeitet wird) gibt. Insbesondere sollte die Wirkung eines Rechtsbehelfs auf die Durchsetzbarkeit einer Anweisung berücksichtigt werden.

[10] Gesetzliche Verjährungsvorschriften können bewirken, dass eine vorhergehende Anweisung der Aufsichtsbehörde aufgrund des Zeitraums, der seit ihrer Ausstellung vergangen ist, womöglich nicht mehr berücksichtigt wird. In einigen Rechtsräumen legen die Vorschriften fest, dass nach Ablauf der Verjährungsfrist für eine Anweisung keine Geldbuße wegen der Nichteinhaltung dieser Anweisung gemäß Artikel 83 Absatz 6 mehr verhängt werden darf. Es ist Sache der einzelnen Aufsichtsbehörden in jedem Rechtsraum, festzustellen, inwieweit sie durch solche Auswirkungen betroffen sind.

Artikel 12) anwendbar sind. Eine ausführlichere Erläuterung geht an dieser Stelle über den Geltungsbereich dieser konkreten Leitlinie hinaus (da ausführliche Berechnungen den Schwerpunkt einer möglichen nachfolgenden Stufe dieser Leitlinien bilden würden).

Die im Folgenden genannten Faktoren sollten in Kombination bewertet werden, d. h. beispielsweise die Anzahl der betroffenen Personen zusammen mit den möglichen Auswirkungen auf sie.

Die **Anzahl** der betroffenen Personen sollte ermittelt werden, um festzustellen, ob der Verstoß ein Einzelereignis ist oder auf ein systembedingtes Problem bzw. Fehlen geeigneter Verfahrensweisen hinweist. Das heißt nicht, dass Einzelereignisse nicht geahndet werden sollten, da auch sie eine große Anzahl an Personen betreffen können. Je nach den Umständen des Einzelfalls kann dies beispielsweise von der Gesamtzahl der in der fraglichen Datenbank registrierten Personen, der Zahl der Nutzer eines Dienstes, der Zahl der Kunden oder den Bevölkerungszahlen des Landes abhängen.

Auch der **Zweck** der Verarbeitung muss bewertet werden. In ihrer Stellungnahme zur „Zweckbindung“[11] analysierte die Artikel-29-Datenschutzgruppe die zwei Hauptbausteine dieses Grundsatzes im Datenschutzrecht: Zweckbindung und Vereinbarkeit der Nutzung. Bei der Bewertung des Zwecks der Verarbeitung im Rahmen von Artikel 83 Absatz 2 sollten die Aufsichtsbehörden prüfen, in welchem Umfang die beiden wichtigsten Aspekte dieses Grundsatzes bei der Verarbeitung gewahrt werden.[12] In bestimmten Situationen hält es die Aufsichtsbehörde womöglich für erforderlich, in die Analyse von Artikel 83 Absatz 2 eine tiefergehende Untersuchung des Zwecks der Verarbeitung einzubeziehen.

Wenn die betroffenen Personen einen **Schaden** erlitten haben, muss das Ausmaß des Schadens berücksichtigt werden. Die Verarbeitung von personenbezogenen Daten kann mit Risiken für die Rechte und Freiheiten der Personen einhergehen, wie die Erwägung 75 verdeutlicht:

> „*Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten*

[11] WP 203, „Opinion 03/2013 on purpose limitation“ (Stellungnahme 03/2013 zur Zweckbindung), abrufbar auf: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Siehe auch WP 217, „Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC“ (Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des Datenverantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG), S. 24, zu folgender Fragestellung: „Wann ist ein Interesse berechtigt, wann unberechtigt?“

schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.“

Wurde aufgrund des Verstoßes gegen die Verordnung ein Schaden erlitten oder wird voraussichtlich erlitten, sollte die Aufsichtsbehörde dies bei der Wahl ihrer Abhilfemaßnahme berücksichtigen, auch wenn sie selbst nicht dafür zuständig ist, den entsprechenden Schadenersatz für den erlittenen Schaden zu gewähren.

Die Verhängung einer Geldbuße hängt nicht davon ab, ob die Aufsichtsbehörde einen kausalen Zusammenhang zwischen dem Verstoß und dem materiellen Schaden feststellen kann (siehe z. B. Artikel 83 Absatz 6).

Die **Dauer** des Verstoßes kann Hinweise auf Folgendes geben:

a) vorsätzliches Verhalten des Datenverantwortlichen oder

b) Versäumnisse beim Ergreifen vorbeugender Maßnahmen oder

c) Unvermögen, die notwendigen technischen und organisatorischen Maßnahmen zu treffen.

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

Im Allgemeinen schließt der Begriff des „Vorsatzes“ bei den Merkmalen einer Straftat Wissen und Wollen ein, während „nicht vorsätzlich“ bedeutet, dass der Verstoß unbeabsichtigt erfolgte, auch wenn der Verantwortliche bzw. Auftragsverarbeiter seine gesetzlich vorgeschriebene Sorgfaltspflicht verletzt hat.

Es wird allgemein anerkannt, dass vorsätzliche Verstöße, die eine offenkundige Missachtung der gesetzlichen Bestimmungen darstellen, schwerwiegender sind als nicht vorsätzliche Verstöße und daher eher die Verhängung einer Geldbuße rechtfertigen können. Die maßgeblichen Schlussfolgerungen zur Vorsätzlichkeit oder Fahrlässigkeit werden gezogen, indem aus dem Sachverhalt die objektiven Grundzüge des Verhaltens ermittelt werden. Darüber hinaus werden die Rechtsprechung und die Praxis, die sich aufgrund der Anwendung der Verordnung im Bereich des Datenschutzes etablieren, die Umstände näher bestimmen, die den Rahmen für eine klare Einschätzung dazu bilden, ob ein Verstoß vorsätzlich erfolgte.

Umstände, die auf vorsätzliche Verstöße hindeuten, liegen beispielsweise vor, wenn eine unrechtmäßige Verarbeitung von der obersten Führungsebene des Verantwortlichen genehmigt wurde oder wenn – entgegen den Empfehlungen des Datenschutzbeauftragten oder unter Missachtung vorhandener Richtlinien – Daten über die Mitarbeiter eines Wettbewerbers in der Absicht erfasst und verarbeitet wurden, diesen Wettbewerber auf dem Markt in Verruf zu bringen.

Weitere mögliche Beispiele:

- Änderung personenbezogener Daten in der Absicht, einen irreführenden (positiven) Eindruck über die Erreichung von Zielvorgaben zu vermitteln – ein entsprechender Fall wurde im Zusammenhang mit den Zielvorgaben für Krankenhauswartezeiten aufgedeckt;
- Handel mit personenbezogenen Daten für Marketingzwecke, d. h. Verkauf als Daten, für die eine Zustimmung zur Verarbeitung vorliegt, ohne jedoch den Standpunkt der betroffenen Personen zur Verwendung ihrer Daten eingeholt zu haben oder zu beachten.

Andere Umstände, wie Versäumnisse beim Lesen und Einhalten vorhandener Richtlinien, menschliches Versagen, Versäumnisse bei der Prüfung veröffentlichter Informationen auf personenbezogene Daten, Versäumnisse bei der zeitnahen Durchführung technischer

Aktualisierungen, Versäumnisse bei der Umsetzung von Richtlinien (im Gegensatz zum schlichten Versäumnis ihrer Anwendung) können auf Fahrlässigkeit hindeuten.

Die Unternehmen sollten die Verantwortung dafür tragen, Strukturen und Ressourcen einzusetzen, die der Art und Komplexität ihrer Geschäftstätigkeit angemessen sind. Aus diesem Grund können die Verantwortlichen und Auftragsverarbeiter Verstöße gegen das Datenschutzrecht nicht mit fehlenden Ressourcen begründen. Bei den Arbeitsabläufen und der Dokumentation in Verbindung mit Verarbeitungstätigkeiten ist ein risikobasierter Ansatz gemäß der Verordnung zu befolgen.

Es gibt Grauzonen, die die Entscheidungsfindung über die Auferlegung einer Abhilfemaßnahme beeinflussen, sodass die Behörde gegebenenfalls weiterführende Untersuchungen durchführen muss, um die Aspekte des Sachverhalts festzustellen und allen spezifischen Umständen eines Einzelfalls gebührend Rechnung zu tragen.

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

Die Datenverantwortlichen und Datenverarbeiter sind verpflichtet, technische und organisatorische Maßnahmen zu treffen, mit denen ein dem Risiko angemessenes Sicherheitsniveau gewährleistet wird, Datenschutz-Folgenabschätzungen durchzuführen und die Risiken zu mindern, die sich aus der Verarbeitung personenbezogener Daten für die Rechte und Freiheiten der betroffenen Personen ergeben. Wenn jedoch ein Verstoß erfolgt und die betroffene Person einen Schaden erlitten hat, sollte die verantwortliche Partei alles Erdenkliche tun, um die Folgen des Verstoßes für die betroffene(n) Person(en) gering zu halten. Ein solches verantwortungsvolles Handeln (oder sein Fehlen) wird von der Aufsichtsbehörde bei der Wahl der Abhilfemaßnahme(n) und der Festsetzung der in einem speziellen Fall zu verhängenden Sanktion berücksichtigt.

Auch wenn erschwerende und mildernde Umstände besonders dafür geeignet sind, den Betrag für die Geldbuße genau an die jeweiligen Umstände des Einzelfalls anzupassen, sollte auch ihre Rolle bei der Wahl der geeigneten Abhilfemaßnahme nicht unterschätzt werden. In Fällen, in denen die Bewertung anderer Kriterien bei der Aufsichtsbehörde Zweifel daran aufkommen lässt, ob eine Geldbuße alleinstehend oder kombiniert mit anderen Maßnahmen gemäß Artikel 58 eine verhältnismäßige Abhilfemaßnahme ist, können solche erschwerenden oder mildernden Umstände den Ausschlag für die Entscheidung geben, welche Maßnahmen im fraglichen Fall wirksamer, verhältnismäßiger und abschreckender sind.

Mithilfe dieser Bestimmung kann bewertet werden, inwieweit der Verantwortliche nach dem Eintreten eines Verstoßes verantwortlich gehandelt hat. Sie kann sich auf Fälle beziehen, in denen die Verantwortlichen bzw. Auftragsverarbeiter offenkundig nicht fahrlässig oder leichtfertig gehandelt, sondern alles Erdenkliche getan haben, um ihre Handlungen zu korrigieren, nachdem sie Kenntnis von dem Verstoß erlangt hatten.

Die regulatorischen Erfahrungen mit den Kontrollstellen nach Maßgabe der Richtlinie 95/46/EG haben gezeigt, dass es angemessen sein kann, ein gewisses Maß an Flexibilität gegenüber den Datenverantwortlichen bzw. Datenverarbeitern zu zeigen, die ihren Verstoß eingestanden und die Verantwortung dafür übernommen haben, die Auswirkungen ihres Handelns zu korrigieren oder zu beschränken. Mögliche Beispiele (die jedoch nicht zwangsläufig ein flexibleres Vorgehen nach sich ziehen):

- Kontaktaufnahme mit anderen Verantwortlichen bzw. Auftragsverarbeitern, die gegebenenfalls an einer Erweiterung der Verarbeitung beteiligt waren, z. B. wenn ein Teil der Daten irrtümlich an Dritte weitergegeben wurde.

- rechtzeitiges Tätigwerden des Datenverantwortlichen bzw. Datenverarbeiters mit dem Ziel, den Verstoß zu beheben oder zu verhindern, dass er eine Stufe bzw. Phase erreicht, in der er weit schwerere Auswirkungen hätte als die bereits eingetretenen.

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

Mit der Verordnung wurde für den Datenverantwortlichen gegenüber der Datenschutzrichtlinie 95/46/EG ein weitaus höherer Grad der Verantwortung eingeführt.

Wenn der Grad der Verantwortung des Verantwortlichen oder Auftragsverarbeiters bewertet wird, um eine geeignete Abhilfemaßnahme zu bestimmen, könnten folgende Fragen gestellt werden:

- Hat der Verantwortliche technische Maßnahmen ergriffen, die den Grundsätzen des Datenschutzes durch Technik oder der datenschutzfreundlichen Voreinstellungen (Artikel 25) entsprechen?
- Hat der Verantwortliche organisatorische Maßnahmen ergriffen, mit denen die Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Voreinstellungen (Artikel 25) auf allen Organisationsebenen umgesetzt werden?
- Hat der Verantwortliche bzw. Auftragsverarbeiter ein angemessenes Schutzniveau umgesetzt (Artikel 32)?
- Sind die maßgeblichen Arbeitsabläufe bzw. Richtlinien für den Datenschutz auf der geeigneten Managementebene der Organisation bekannt und werden dort angewendet (Artikel 24)?

In den Artikeln 25 und 32 der Verordnung ist festgelegt, dass die Verantwortlichen Maßnahmen „*[U]nter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen*“ treffen. Mit diesen Bestimmungen wird keine Ergebnisverpflichtung, sondern eine Bemühungsverpflichtung eingeführt, das heißt der Verantwortliche muss die erforderlichen Bewertungen vornehmen und zu angemessenen Schlussfolgerungen gelangen. Anschließend ist von der Aufsichtsbehörde die Frage zu beantworten, inwieweit der Verantwortliche so gehandelt hat, wie es von ihm aufgrund der Art, der Zwecke und des Umfangs der Verarbeitung angesichts seiner Verpflichtungen gemäß der Richtlinie zu erwarten gewesen wäre.

Bei dieser Bewertung sollten, sofern vorhanden und anwendbar, bewährte Verfahren oder Methoden gebührend berücksichtigt werden. Industriestandards sowie Verhaltensregeln in dem betreffenden Bereich oder Beruf sind ebenfalls wichtige Bezugspunkte. Verhaltensregeln können Hinweise darauf liefern, was im jeweiligen Bereich gängige Praxis ist und welche Kenntnisse über die verschiedenen Möglichkeiten zur Behandlung typischer Sicherheitsprobleme bei der Datenverarbeitung vorhanden sind.

Während bewährte Verfahren grundsätzlich das anzustrebende Ideal sein sollten, müssen auch die spezifischen Umstände jedes Einzelfalls berücksichtigt werden, wenn der Grad der Verantwortung ermittelt wird.

e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

Mit diesem Kriterium soll bewertet werden, in welchem Umfang die für den Verstoß verantwortliche Einrichtung bereits in der Vergangenheit Verstöße begangen hat. Die Aufsichtsbehörden sollten berücksichtigen, dass der Rahmen dieser Bewertung relativ weit ausgelegt sein kann, da jede Art von Verstoß gegen die Verordnung, auch wenn er anders gelagert ist als der aktuell von der Aufsichtsbehörde untersuchte Verstoß, für die Bewertung maßgeblich sein könnte, da er womöglich Hinweise auf einen allgemein unzureichenden Kenntnisstand oder eine allgemeine Missachtung der Datenschutzregelungen liefert.

Die Aufsichtsbehörde sollte folgende Fragestellungen untersuchen:

- Hat der Verantwortliche bzw. Auftragsverarbeiter den gleichen Verstoß bereits zu einem früheren Zeitpunkt begangen?
- Hat der Verantwortliche bzw. Auftragsverarbeiter einen Verstoß gegen die Verordnung bereits in gleicher Weise begangen? (beispielsweise infolge unzureichender Kenntnis der vorhandenen Arbeitsabläufe in der Organisation oder infolge einer unangemessenen Risikobewertung, in Form von Versäumnissen bei der zeitnahen Beantwortung von Anträgen betroffener Personen, ungerechtfertigten Verzögerungen bei der Beantwortung von Anträgen usw.).

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

Artikel 83 Absatz 2 sieht vor, dass der Umfang der Zusammenarbeit bei der Entscheidung darüber, ob und in welcher Höhe eine Geldbuße verhängt wird, „gebührend berücksichtigt“ werden kann. Die Verordnung gibt keine genaue Antwort auf die Frage, wie den Bemühungen des Verantwortlichen oder des Auftragsverarbeiters, einen von der Aufsichtsbehörde bereits festgestellten Verstoß zu beheben, Rechnung zu tragen ist. Darüber hinaus ist klar, dass bei der Festsetzung der Höhe der Geldbuße in der Regel die Kriterien zur Anwendung kommen würden.

Wenn das Tätigwerden des Verantwortlichen jedoch dazu geführt hat, dass die nachteiligen Folgen für die Rechte der betroffenen Personen keine Beeinträchtigung oder eine geringere Beeinträchtigung als andernfalls möglich verursacht haben, könnte dies bei der Wahl der Abhilfemaßnahme, die in diesem Einzelfall verhältnismäßig ist, berücksichtigt werden.

Folgende Fragestellung soll als Beispiel dafür dienen, wann die Zusammenarbeit mit der Aufsichtsbehörde einen maßgeblichen Aspekt darstellen könnte:

- Hat die Einrichtung in diesem speziellen Fall auf besondere Weise auf die Anfragen der Aufsichtsbehörden während der Untersuchungsphase reagiert, wodurch die Auswirkungen auf die Rechte der betroffenen Personen erheblich vermindert wurden?

Ausgehend davon wäre es jedoch nicht angemessen, einen gesetzlich bereits vorgeschriebenen Aspekt der Zusammenarbeit besonders zu berücksichtigen. Beispielsweise ist die Einrichtung in jedem Fall verpflichtet, der Aufsichtsbehörde im Rahmen von Prüfungen bzw. Inspektionen Zugang zu ihren Räumlichkeiten zu gewähren.

g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

Im Folgenden werden einige Beispiele für wesentliche Fragen genannt, deren Beantwortung die Aufsichtsbehörde, sofern im Einzelfall angemessen, in diesem Zusammenhang als notwendig erachten könnte:

- Betrifft der Verstoß die Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 und 10 der Verordnung?

- Sind die Daten direkt oder indirekt identifizierbar?
- Werden Daten verarbeitet, durch deren Verbreitung der betroffenen Person ein unmittelbarer Schaden bzw. eine unmittelbare Notsituation entstehen würde (die nicht in die Kategorie von Artikel 9 oder 10 fallen)?
- Sind die Daten unmittelbar ohne technische Schutzmechanismen zugänglich oder sind sie verschlüsselt?[13]

h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

Eine Aufsichtsbehörde kann von einem Verstoß durch eine Untersuchung, Beschwerden, Presseberichte, anonyme Hinweise oder die Meldung des Datenverantwortlichen Kenntnis erlangen. Der Verantwortliche ist gemäß der Verordnung verpflichtet, der Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten zu melden. Wenn der Verantwortliche lediglich dieser Pflicht nachkommt, kann dies nicht als erschwerender bzw. mildernder Umstand gewertet werden. In Fällen, in denen der Datenverantwortliche bzw. Datenverarbeiter fahrlässig gehandelt hat, indem er keine Meldung gemacht oder zumindest nicht alle Einzelheiten des Verstoßes gemeldet hat, weil der Umfang des Verstoßes nicht angemessen bewertet wurde, kann die Aufsichtsbehörde ebenfalls entscheiden, dass eine schwerere Sanktion verhängt werden soll, d. h. eine Einstufung als „geringfügigerer Verstoß“ ist unwahrscheinlich.

i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

Ein Verantwortlicher oder Auftragsverarbeiter kann bereits im Fokus der Aufsichtsbehörde stehen, wenn diese nach einem früheren Verstoß die Einhaltung der Bestimmungen durch diesen Verantwortlichen bzw. Auftragsverarbeiter überwacht. In diesem Fall hat es wahrscheinlich intensive Kontakte mit dem Datenschutzbeauftragten, sofern vorhanden, gegeben. Daher wird die Aufsichtsbehörde die vorherigen Kontakte berücksichtigen.

Anders als bei den Kriterien unter Buchstabe e sollen die Aufsichtsbehörden mit diesen Bewertungskriterien lediglich daran erinnert werden, auf die Maßnahmen Bezug zu nehmen, die sie selbst zuvor gegenüber dem gleichen Verantwortlichen oder Auftragsverarbeiter „*in Bezug auf denselben Gegenstand*“ angeordnet haben.

j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 [...]

Die Aufsichtsbehörden müssen „*die Anwendung dieser Verordnung überwachen und durchsetzen*“ (Artikel 57 Absatz 1 Buchstabe a). Die Einhaltung von genehmigten Verhaltensregeln kann vom Verantwortlichen oder Auftragsverarbeiter gemäß Artikel 24 Absatz 3, Artikel 28 Absatz 5 oder Artikel 32 Absatz 3 als Nachweis für die Einhaltung genutzt werden.

Bei einem Verstoß gegen eine Bestimmung der Verordnung kann die Einhaltung von genehmigten Verhaltensregeln einen Hinweis darauf geben, wie dringend es ist, mit einer wirksamen, verhältnismäßigen und abschreckenden Geldbuße oder anderen Abhilfemaßnahme der Aufsichtsbehörde einzugreifen. Gemäß Artikel 40 Absatz 4 sehen die genehmigten Verhaltensregeln

[13] Wenn der Verstoß nur indirekt identifizierbare oder sogar pseudonyme/verschlüsselte Daten betrifft, sollte dies nicht immer als zusätzlicher mildernder Umstand angesehen werden. Auch bei solchen Verstößen könnte die Gesamtbewertung der anderen Kriterien mäßige oder starke Anhaltspunkte dafür liefern, dass eine Geldbuße verhängt werden sollte.

Verfahren vor, „*die es der [...] [Überwachungs-]Stelle ermöglichen, die obligatorische Überwachung der Einhaltung ihrer Bestimmungen [...] vorzunehmen*“.

In Fällen, in denen der Verantwortliche oder Auftragsverarbeiter genehmigte Verhaltensregeln eingehalten hat, genügt dies der Aufsichtsbehörde womöglich als Hinweis darauf, dass die für die Durchsetzung der Regeln zuständige Regelgemeinschaft selbst geeignete Maßnahmen gegenüber ihren Mitgliedern ergreift. Ein Beispiel hierfür sind Mechanismen, mit denen die Verhaltensregeln überwacht und durchgesetzt werden. Daher könnte die Aufsichtsbehörde zu der Auffassung gelangen, dass die entsprechenden Maßnahmen in diesem konkreten Fall wirksam, verhältnismäßig und abschreckend genug sind und es nicht erforderlich ist, dass die Aufsichtsbehörde selbst noch weitere Maßnahmen ergreift. Bestimmte Formen der Sanktionierung von pflichtwidrigem Verhalten können im Rahmen der Überwachung gemäß Artikel 41 Absatz 2 Buchstabe c und Artikel 42 Absatz 4 erfolgen, einschließlich eines vorläufigen oder endgültigen Ausschlusses des Verantwortlichen oder Auftragsverarbeiters aus der Regelgemeinschaft. Die Befugnisse der Überwachungsstelle berühren jedoch nicht die „*Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde*“, d. h. die Aufsichtsbehörde ist nicht verpflichtet, die Sanktionen zu berücksichtigen, die zu einem früheren Zeitpunkt im Rahmen der Selbstkontrollregelung verhängt wurden.

Die Nichteinhaltung von Selbstregulierungsmaßnahmen könnte auch auf fahrlässiges oder vorsätzliches Verhalten des Verantwortlichen bzw. Auftragsverarbeiters in Verbindung mit dem Verstoß hindeuten.

k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

Die Bestimmung selbst enthält Beispiele dafür, welche anderen Aspekte bei der Entscheidung darüber berücksichtigt werden können, ob eine Geldbuße bei einem Verstoß gegen die Bestimmungen von Artikel 83 Absätze 4 bis 6 ein geeignetes Mittel ist.

Informationen über Gewinne, die infolge eines Verstoßes erzielt wurden, können für die Aufsichtsbehörden besonders wichtig sein, da wirtschaftliche Gewinne aus Verstößen nicht durch Maßnahmen ohne geldlichen Aspekt ausgeglichen werden können. Dementsprechend könnte der Umstand, dass der Verantwortlichen durch den Verstoß gegen die Verordnung einen Gewinn erzielt hat, ein deutlicher Hinweis darauf sein, dass eine Geldbuße verhängt werden sollte.

IV. Schlussfolgerung

Überlegungen zu Fragen, wie sie im vorstehenden Abschnitt behandelt wurden, werden den Aufsichtsbehörden dabei helfen, anhand der maßgeblichen Sachverhalte diejenigen Kriterien zu bestimmen, die sich am besten für eine Entscheidung darüber eignen, ob eine angemessene Geldbuße zusätzlich zu oder anstelle von anderen Maßnahmen nach Artikel 58 verhängt werden soll. Vor dem Hintergrund, den eine solche Bewertung liefert, kann die Aufsichtsbehörde die jeweils wirksamste, verhältnismäßigste und abschreckendste Abhilfemaßnahme als Reaktion auf den Verstoß bestimmen.

Artikel 58 gibt eine gewisse Anleitung dazu, welche Maßnahmen die Aufsichtsbehörde wählen könnte, da die Abhilfemaßnahmen als solche ja unterschiedlicher Art und vorrangig für unterschiedliche Zwecke geeignet sind. Bestimmte Maßnahmen nach Artikel 58 können unter Umständen sogar miteinander kombiniert werden, sodass mit mehr als einer Abhilfemaßnahme regulatorisch eingegriffen werden kann.

Es ist gleichwohl nicht immer erforderlich, die gewählte Maßnahme durch eine andere Abhilfemaßnahme zu ergänzen. Beispielsweise können die Wirksamkeit und die abschreckende Wirkung des Eingreifens der Aufsichtsbehörde unter angemessener Berücksichtigung dessen, was im spezifischen Fall verhältnismäßig ist, auch mit der Geldbuße allein erreicht werden.

Im Wesentlichen geht es darum, dass die Behörden mit allen ihnen zur Verfügung stehenden Maßnahmen dafür sorgen, dass die Bestimmungen fortan wieder eingehalten werden. Die Aufsichtsbehörden sollen zudem verpflichtet werden, die beste Möglichkeit für regulatorische Maßnahmen zu wählen. Dazu könnten beispielsweise auch geeignete strafrechtliche Sanktionen zählen (sofern diese auf einzelstaatlicher Ebene möglich wären).

Die kohärente Anwendung von Geldbußen in der Europäischen Union ist ein noch in der Entwicklung befindlicher Prozess. Die Aufsichtsbehörden sollten bei der Anwendung derartiger Maßnahmen zusammenarbeiten, damit die Kohärenz kontinuierlich verbessert wird. Dies kann durch den regelmäßigen Austausch im Rahmen fallbezogener Workshops oder anderer Veranstaltungen erreicht werden, die einen Vergleich von Fällen auf subnationaler, nationaler und grenzübergreifender Ebene ermöglichen. Zur Unterstützung dieser fortlaufenden Anstrengungen wird empfohlen, eine ständige, an den für diesen Bereich zuständigen Teil des Europäischen Datenschutzausschusses angegliederte Untergruppe einzusetzen.