

Stellungnahme

bei der Anhörung

im Ausschuss für Justiz und Datenschutz

der Bürgerschaft der Freien und Hansestadt Hamburg

zu den Entwürfen

eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 für den Hamburger Justizvollzug und zur Änderung vollzugsrechtlicher Vorschriften (Drs. 21/11636)

und

eines Gesetzes zur Anpassung des Hamburgischen Datenschutzgesetzes sowie weiterer Vorschriften an die Verordnung (EU) 2016/679 (Drs. 21/11638)

A. Gesetz zum Hamburger Justizvollzug und zur Änderung vollzugsrechtlicher Vorschriften

1. An mehreren Stellen des Gesetzentwurfs wird als qualifizierte Rechtmäßigkeitsvoraussetzung (z.B. für die Verarbeitung von Daten besonderer Kategorien, Art. 1 § 7 Absatz 2; für die indirekte Datenerhebung über Personen, die nicht Gefangene sind, Art. 1 § 9, und für die Beschränkung des Zugangs zu den Ergebnissen von Sicherheitsanfragen, Art. 1 § 15 Abs. 10) der Begriff der „unbedingten Erforderlichkeit“ verwendet. Das ist deshalb problematisch, weil dadurch **der zentrale datenschutzrechtliche Massstab der Erforderlichkeit** relativiert wird („einfache“ vs. „unbedingte“ Erforderlichkeit). Das Unionsrecht (insbesondere auch die Richtlinie (EU) 2016/680) kennt eine solche Differenzierung nicht. Stattdessen sollte ein anderer Begriff für die Situationen gewählt werden, in denen gesteigerte Rechtmäßigkeitsanforderungen gelten sollten. Das Berliner Justizvollzugsdatenschutzgesetz von 2011 verwendet hierfür den Begriff der „Unerlässlichkeit“ (im Unterschied zur Erforderlichkeit).

2. Die in Art. 1 §§ 15 vorgeschlagene Regelung für die **Sicherheitsüberprüfung von Gefangenen und anstaltsfremden Personen** ist unverhältnismäßig und erscheint nicht geeignet, um einer versteckten Radikalisierung von Gefangenen wirksam zu begegnen. Das gilt sowohl für die prinzipiell anlassunabhängige umfassende Sicherheitsanfrage bei allen Gefangenen wie auch für die Anfrage bezüglich anstaltsfremder Personen. Letztere soll zwar nach Art. 1 § 15 Abs. 6 Satz 3 nur

erfolgen, wenn „aufgrund bestimmter Umstände“ davon auszugehen ist, dass eine Sicherheitsüberprüfung ohne Einbeziehung des Verfassungsschutzes nicht ausreicht. Die Voraussetzungen für einen Verzicht auf die Sicherheitsanfrage bei Gefangenen einerseits und bei anstaltsfremden Personen andererseits sind so wenig normenklar gefasst, dass sie keinen Eingriff in das Recht der betroffenen Personen rechtfertigen können. Ich teile insoweit die Einwände des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Offenbar ist die Schwelle für Datenabfragen beim Verfassungsschutz bezüglich anstaltsfremder Personen niedriger als bei Besucherinnen und Besuchern, denn bei letzteren werden immerhin „tatsächliche Anhaltspunkte“ dafür verlangt, dass das Vollzugsziel oder Sicherheit und Ordnung der Anstalt durch den Besuch gefährdet werden können (Art. 1 § 16 Abs. 3).

Vorzugswürdig ist demgegenüber eine restriktive Regelung, wie sie das Berliner Justizvollzugsdatenschutzgesetz getroffen hat. Danach ist (ebenfalls in den §§ 15 und 16) generell die Erhebung von Daten über Gefangene bei Dritten (also auch bei Sicherheitsbehörden) nur zulässig, wenn die Kenntnis der Daten im Einzelfall zu vollzuglichen Zwecken unerlässlich ist und die zu erfüllende Aufgabe ihrer Art oder ihrem Zweck nach eine Erhebung bei Dritten erforderlich macht. Daten über Personen, die nicht Gefangene sind (also sowohl anstaltsfremdes Personal als auch Besucherinnen und Besucher), können bei Dritten (auch Behörden außerhalb des Justizvollzugs) erhoben werden, wenn es zu vollzuglichen Zwecken unerlässlich ist und die Art der Erhebung schutzwürdige Interessen der Betroffenen nicht beeinträchtigt.

Zumindest sollte aber dem Vorschlag des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gefolgt werden, Sicherheitsanfragen zu Gefangenen und anstaltsfremden Personen vom Vorliegen tatsächlicher Anhaltspunkte für eine Gefährdung des Vollzugsziels oder der Sicherheit und Ordnung der Anstalt abhängig zu machen.

3. Der Entwurf stätet den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit auch nicht mit den nach der Richtlinie (EU) 2016/680 gebotenen **Befugnissen** aus. Schon der bisherige Rechtszustand nach dem Hamburgischen Datenschutzgesetz (wie nach dem Datenschutzrecht in Bund und den übrigen Bundesländern) stand im Widerspruch zu den Vorgaben der Datenschutzrichtlinie 95/46/EWG, die – wie die Richtlinie (EU) 2016/680 – wirksame Einwirkungsbefugnisse der Aufsichtsbehörden vorschrieb. Dem genügte das bloße Recht zur förmlichen Beanstandung nicht. Der Entwurf des Senats würde diesen europarechtswidrigen Zustand für den Bereich des Justizvollzugs fortschreiben (Art. 1 § 43 Abs. 1). Die Beanstandung ist keine hinreichend wirksame Einwirkungsbefugnis. Lehnt die verantwortliche Stelle die Umsetzung der in der Beanstandung geforderten Maßnahmen ab, so hat der Datenschutzbeauftragte keine weitergehenden Möglichkeiten, den Datenschutzverstoß abzustellen.

In Art. 1 § 43 sollte deshalb zusätzlich ein Recht der Datenschutzbehörde aufgenommen werden, bestimmte Anordnungen gegenüber verantwortlichen Stellen treffen zu können, wie es der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und die Hessische Landesregierung vorgeschlagen haben.

B. Anpassung an die Datenschutz-Grundverordnung

Der europäische Gesetzgeber hat mit der Datenschutz-Grundverordnung (EU) 2016/679 einen einheitlichen Rechtsrahmen für den Datenschutz in der Europäischen Union geschaffen, der das Datenschutzrecht in Bund und Ländern ab dem 25. Mai 2018 mit unmittelbarer Wirkung bestimmen wird. Die Gesetzgeber in Bund und Ländern haben nur sehr eingeschränkte Optionen, präzisierende Regelungen in diesem Bereich zu treffen. Der Hamburger Senat hat sich daher mit Recht darauf beschränkt, ein schlankes Anpassungsgesetz vorzuschlagen, zumal der Wiederholung von Unionsrecht enge Grenzen gesetzt sind.

Bei der Setzung und Anwendung von innerstaatlichem Recht kommt es daher darauf an, zum einen das Ziel der weitgehenden Harmonisierung des Datenschutzrechts nicht zu vereiteln und zum anderen den Rechtsanwendern, die künftig die Grundverordnung und das innerstaatliche Recht nebeneinander anzuwenden haben, den **Vorrang des Unionsrechts** zu verdeutlichen.

1. Daher empfiehlt es sich, in das Hamburgische Anpassungsgesetz (Art. 1 § 2 des Entwurfs) eine klarstellende Vorschrift aufzunehmen, die den Vorrang des Unionsrechts – gerade auch in Zweifelsfällen - betont. Der Bundesgesetzgeber hat solche Klarstellungen im neuen Bundesdatenschutzgesetz (§ 1 Abs. 5, ebenso § 2 Abs. 5 des Berliner Entwurfs für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – BInDSAnpUG-EU, § 1 Abs. 5 des Entwurfs für ein Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit) und in den bereichsspezifischen Regelungen der Abgabenordnung und des Sozialgesetzbuches vorgenommen (§§ 2a Abs. 3 AO, 35 Abs. 2 SGB Erstes Buch idF des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften v. 17.7.2017).

2. Die **Abberufung und Kündigung des Datenschutzbeauftragten** sollte vom Landesgesetzgeber einschränkend geregelt werden, um seine behördeninterne Unabhängigkeit zu stärken. Anders als die Entwurfsbegründung meint, ist § 626 BGB hier nicht ohne weiteres entsprechend anwendbar. Der Landesgesetzgeber hat nach Auffassung des Berliner Senats durchaus die Kompetenz, eine entsprechende Anwendung des § 626 BGB – wie im Bundesdatenschutzgesetz – vorzusehen. Ohne eine solche Regelung ist der Datenschutzbeauftragte nicht hinreichend vor Benachteiligungen geschützt, wenn er seine Aufgabe ernst nimmt. Bayern plant

darüber hinaus eine Vorschrift, nach der dem Datenschutzbeauftragten Gelegenheit zur Stellungnahme vor dem erstmaligen Einsatz eines Verfahrens zu geben ist. Diese Regelung scheint mir nach meinen Erfahrungen sehr sinnvoll zu sein, denn immer wieder werden behördliche Datenschutzbeauftragte zu spät oder überhaupt nicht bei der Einführung oder wesentlichen Änderung von Datenverarbeitungsverfahren beteiligt.

3. Der Unionsgesetzgeber hat den Mitgliedstaaten die Möglichkeit eröffnet, unter engen Voraussetzungen Ausnahmen vom Gebot der **Zweckbindung** bei der Verarbeitung personenbezogener Daten vorzusehen. Zunächst sollte das innerstaatliche Gesetz verdeutlichen, dass eine Zweckänderung nur in dem Umfang zulässig ist, in dem im Einzelfall die Voraussetzungen der Ausnahmetatbestände vorliegen. Dazu sollte in Art. 1 § 6 Abs. 2 das Wort „wenn“ durch „soweit“ ersetzt werden.

Soweit öffentliche Stellen der Freien und Hansestadt Hamburg fiskalisch tätig werden, finden auf sie die Bestimmungen der Grundverordnung und des BDSG für nicht-öffentliche Stellen Anwendung (Art. 1 § 2 Abs. 3 des Entwurfs, Art. 6 Abs. 1 lit. f) DSGVO). Der in Art. 1 § 6 Abs. 2 Nr. 5 des Entwurfs vorgesehene Zweckänderungsbefugnis bei der Teilnahme am Privatrechtsverkehr bedarf es daher nicht. Bei der Durchsetzung öffentlich-rechtlicher Forderungen wird in der Regel Zweckidentität mit dem ursprünglichen Erhebungszweck vorliegen, so dass Art. 1 § 6 Abs. 2 Nr. 5 insgesamt zu streichen ist.

Die Zweckänderungsbefugnis in Art. 1 § 6 Abs. 2 Nr. 9 erscheint ebenfalls überflüssig, da Art. 1 § 11 des Entwurfs eine solche sowohl für Zwecke der Eigenforschung oder der Sekundärstatistik als auch für übermittelte Daten bereits enthält.

Art. 1 § 6 Abs. 4 adressiert das Problem der Verarbeitung personenbezogener Daten in analoger Form, insbesondere in Akten. Insoweit lässt der Entwurf die Kenntnisnahme, Weitergabe und Übermittlung nicht erforderlicher Daten, die wegen ihrer Verarbeitungsform praktisch untrennbar mit erforderlichen Daten verbunden sind, unter bestimmten Voraussetzungen zu. Zugleich statuiert der Entwurf ein Verarbeitungsverbot bezüglich der nicht erforderlichen Daten. Das würde in der Praxis bedeuten, dass der Empfänger der Daten diese Daten nicht verarbeiten dürfte, also löschen müsste, was aber eine nur mit unverhältnismäßigem Aufwand mögliche Trennung von den erforderlichen Daten voraussetzt, die der Entwurf bei der ursprünglich verantwortlichen Stelle gerade ausschließt. Das Wort „Verarbeitungsverbot“ in Art. 1 § 6 Abs. 3 Satz 2 sollte deshalb durch „*Verwertungsverbot*“ ersetzt werden.

4. Die Datenschutz-Grundverordnung enthält keine Regelungen über **automatisierte Abrufverfahren**, sondern lediglich – in Art. 26 – über **gemeinsam für die Verarbeitung verantwortliche Stellen**. Dennoch ist es sachgerecht und unionsrechtskonform, innerstaatliche Regelungen für automatisierte Abrufverfahren

vorzusehen bzw. beizubehalten. Allerdings trifft Art. 1 § 7 des Entwurfs eine gemeinsame und zu undifferenzierte Regelung sowohl für automatisierte Abrufverfahren als auch für gemeinsame Dateien. Der Verzicht auf den Vorbehalt einer Rechtsvorschrift (in Berlin galt bis 2016 hierfür sogar ein strikter Gesetzesvorbehalt) erscheint sachgerecht, wenn der Gesetzgeber stattdessen eine Angemessenheitsprüfung und eine Vermeidung von Risiken für die Rechte und Freiheiten der betroffenen Personen durch geeignete Maßnahmen vorschreibt, wie es der Entwurf tut. Werden diese Maßnahmen nicht getroffen oder vermeiden sie die genannten Risiken nicht wirksam, ist die Einrichtung eines automatisierten Abrufverfahrens oder einer gemeinsamen Datei nach dem Entwurf unzulässig. Die Gesetzentwürfe zur Anpassung des Bayerischen und des Berliner Datenschutzrechts wollen Verfahren, die ein hohes Risiko für die Rechte der Betroffenen beinhalten können, gleichwohl von einer Einrichtung durch Gesetz oder aufgrund eines Gesetzes abhängig machen.

Allerdings wird mit der Streichung der Pflicht zur **Anhörung des oder der Hamburgischen Datenschutzbeauftragten** (§ 11 Abs. 2 Satz 2 des geltenden HmbGDStG) auf eine wichtige verfahrensrechtliche Sicherung verzichtet, die bisher eine rechtzeitige Überprüfung der Voraussetzungen für ein zulässiges automatisiertes Abrufverfahren ermöglichte. Dieses Anhörungsrecht sollte beibehalten werden. Zumindest sollte – wie in Berlin derzeit und auch nach dem Gesetzentwurf zur Anpassung des Berliner Datenschutzrechts – eine Pflicht zur Unterrichtung des oder der Hamburgischen Datenschutzbeauftragten vorgesehen werden. Im übrigen teile ich die vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vorgetragene grundsätzliche Kritik an einer fehlenden Regelung der Beteiligung der Datenschutzbehörde am Abstimmungsverfahren über Senatsdrucksachen.

5. Art. 1 § 8 Abs. 3 des Entwurfs überträgt bei Nutzung automatisierter Abrufverfahren der abrufenden Stelle die **Verantwortung für die Rechtmäßigkeit des einzelnen Abrufes**. Um einer unkontrollierten informationellen Selbstbedienung der abrufenden Stellen vorzubeugen, sollte hier entsprechend der in Bayern geplanten Regelung eine Pflicht der offenlegenden Stelle zur stichprobenhaften Feststellung des Abrufs vorgesehen werden. Eine Pflicht der offenlegenden Stelle zur Überprüfung der Rechtmäßigkeit des Abrufs sollte nur bei entsprechendem Anlass bestehen.

6. Hinsichtlich der **Videoüberwachung** bleibt der Entwurf bei der Transparenzvorschrift des Art. 1 § 9 Abs. 3 hinter dem BDSG und z.B. dem Entwurf des neuen Berliner Datenschutzgesetzes zurück, indem er nur allgemein eine Erkennbarmachung der verantwortlichen Stelle vorschreibt. Stattdessen sollte wie im Bundesrecht auch in Hamburg ausdrücklich die Nennung des Namens und der Kontaktdaten der verantwortlichen Stelle verlangt werden.

7. Für den **Bereich des Beschäftigtendatenschutzes** enthält die Datenschutz-Grundverordnung (Art. 88) anders als für die Datenverarbeitung im Zusammenhang

mit der freien Meinungsäußerung und der Informationsfreiheit (Art. 85, dazu s. unten Ziff. 9) keinen expliziten Regelungsauftrag, sondern eröffnet den Mitgliedstaaten lediglich die Möglichkeit, spezifischere Vorschriften zur Gewährleistung des Datenschutzes im Beschäftigungskontext zu erlassen. Von dieser Möglichkeit macht der Entwurf in Art. 1 § 10 für den Bereich der Hamburger Verwaltung Gebrauch. Das ist prinzipiell zu begrüßen, denn der Beschäftigtendatenschutz ist seit jeher eine wesentliche normative Leerstelle, die die Gesetzgeber in Bund und Ländern lange vernachlässigt haben. Der Entwurf begnügt sich damit, den bisherigen Rechtszustand (§ 28 HmbDSG) fortzuschreiben.

Allerdings könnte Art. 1 § 10 Abs. 1 dahingehend verstanden werden, dass Beschäftigtendaten einschließlich sensibler Daten wie Gesundheitsinformationen immer schon dann verarbeitet werden dürfen, wenn eine Rechtsvorschrift, ein Tarifvertrag, eine allgemeine Regelung der obersten Dienstbehörde oder eine Dienstvereinbarung dies vorsieht, unabhängig davon, ob die Voraussetzungen der Grundverordnung insbesondere für die Verarbeitung von besonders schutzwürdigen Daten (Art. 9) vorliegen. Dieses Missverständnis wird insbesondere durch die Formulierung des Art. 1 § 10 Abs. 1 Satz 2 des Entwurfs nahegelegt. Da die Mitgliedstaaten die Grundverordnung aber für den Beschäftigungskontext lediglich spezifizieren dürfen, gilt sie in jedem Fall, also auch in den Fällen des Art. 1 § 10 Abs. 1 Satz 1. Das Missverständnis sollte vermieden werden, indem § 10 Abs. 1 Satz 2 wie folgt gefasst wird:

„Diese Regelungen gelten ergänzend zur Verordnung (EU) 2016/679; soweit derartige Regelungen nicht bestehen, gelten ergänzend die Absätze 2 bis 7.“

Die in Art. 1 § 10 Absatz 7 formulierte Zweckbindung bestimmter für technisch-organisatorische Maßnahmen verarbeiteter Daten ist zu eng gefasst. Sie beschränkt sich wie das bisher geltende HmbDSG (§ 28) auf die Speicherung solcher Daten. Der Zweckbindung muss aber auch für andere Formen der automatisierten oder nicht-automatisierten Verarbeitung gelten, denn Möglichkeiten der Verhaltens- und Leistungskontrolle von Beschäftigten bestehen auch mithilfe solcher Daten, die nicht gespeichert werden. Deshalb sollte bei der Zweckbindungsvorschrift der weite Verarbeitungsbegriff der Datenschutz-Grundverordnung (Art. 4 Nr. 2) zugrunde gelegt und in § 10 Abs. 7 das Wort „gespeichert“ durch „*verarbeitet*“ ersetzt werden.

Außerdem sollte zur Klarstellung nach dem Vorbild des § 26 Abs. 6 BDSG folgender neuer Absatz 9 angefügt werden:

„Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.“

8. Die Rechte betroffener Personen auf Auskunft, Berichtigung, Einschränkung der Verarbeitung und auf Widerspruch sollen bei einer **Datenverarbeitung für wissenschaftliche und historische Forschungszwecke sowie für Zwecke der Statistik** nach Art. 1 § 11 Abs. 5 weitergehend eingeschränkt werden, als die

Grundverordnung dies zulässt. Deren Art. 89 Abs. 2 sieht Ausnahmen zu diesen Rechten nur vor, soweit die Wahrnehmung dieser Rechte die Verwirklichung der genannten Zwecke voraussichtlich unmöglich machen oder ernsthaft beeinträchtigen würde *und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind*. Die zuletzt genannte Voraussetzung, die auch der Bundesgesetzgeber in § 27 Abs. 2 Satz 1 BDSG berücksichtigt hat, fehlt im Entwurf des Senats. Sie ist zu ergänzen. Anders als der Bundesgesetzgeber (§ 27 Abs. 2 Satz 2 BDSG) schlägt der Senat allerdings nicht vor, entgegen den unionsrechtlichen Vorgaben ein Auskunftsrecht bei wissenschaftlichen Forschungsvorhaben schon dann auszuschließen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

9. Art. 1 § 12 des Entwurfs versucht, den Regelungsauftrag des Art. 85 der Datenschutz-Grundverordnung für einen Teilbereich, nämlich den der **Meinungsäußerung für künstlerische Zwecke** umzusetzen. Ob dieser Versuch gelungen ist, muss bezweifelt werden.

Zunächst spricht der Entwurf nur von künstlerischen, nicht aber von literarischen Zwecken, die in der Grundverordnung ebenfalls genannt werden und die nicht Gegenstand von Fachgesetzen sind. Man könnte literarische Zwecke aber zugleich als künstlerische Zwecke und deshalb von der Regelung als miteingefasst betrachten. Richtig ist, dass Art. 85 der Grundverordnung sich auf künstlerische und literarische Tätigkeiten als Unterfälle der Meinungsäußerungs- und Informationsfreiheit bezieht, mithin die künstlerische Kommunikation, also die Veröffentlichung von Kunstwerken meint.

Allerdings schließt Art. 1 § 12 Abs. 1 des Entwurfs die Anwendung großer Teile der Datenschutz-Grundverordnung pauschal aus, obwohl diese in Art. 85 Abs. 1 vom Gesetzgeber die Herstellung praktischer Konkordanz zwischen der Meinungs- und Informationsfreiheit einerseits und dem Recht auf Schutz personenbezogener Daten andererseits verlangt und in Abs. 2 Abweichungen und Ausnahmen von bestimmten Kapiteln zulässt, wenn und soweit dies zur Herstellung dieser Konkordanz erforderlich ist. Der vom Gesetzentwurf vorgesehene regelhafte Vorrang der künstlerischen Freiheit vor dem Recht auf Schutz personenbezogener Daten ist deshalb nicht unionsrechtskonform. So ist z.B. nicht nachvollziehbar, weshalb betroffenen Personen pauschal ein Recht auf Auskunft gegenüber den Kunstschaffenden abgesprochen werden soll, auf welche personenbezogenen Daten sie sich stützen, wenn das Kunstwerk sich auf diese betroffenen Personen bezieht. Entsprechend § 41 Abs. 3 BDSG aF müsste ein solches Auskunftsrecht zumindest dann bestehen, wenn das Kunstwerk fertiggestellt und veröffentlicht worden ist. Auch ist nicht nachvollziehbar, weshalb ein Kunstschaffender, in dessen Datenbeständen ein Leck entsteht, zwar die Aufsichtsbehörden, nicht aber die betroffenen Personen benachrichtigen muss.

Andererseits ist zweifelhaft, ob die in Art. 1 § 12 Abs. 1 des Entwurfs vorgesehene **Anwendung des Zweckbindungsgrundsatzes** nach Art. 5 Abs. 1 lit. b der Grundverordnung sachgerecht ist. Die Grundverordnung sieht vor, dass

personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke verarbeitet werden müssen. Wer soll darüber entscheiden, ob ein Künstler personenbezogene Daten für legitime Zwecke verarbeitet? Auch bleibt unklar, wie die weitere Zweckbindung zu verstehen ist: dürfen die Daten nach Fertigstellung eines Werks ohne Einwilligung der Betroffenen für kein anderes Kunstwerk mehr verarbeitet werden oder sind nur nicht-künstlerische Zwecke ausgeschlossen?

Insgesamt erscheint es sachgerechter, die Rechte der Betroffenen nur in engem Rahmen einzuschränken und stattdessen von der Anwendung des Zweckbindungsgrundsatzes in diesem Bereich abzusehen.

Die in Art. 1 § 12 Abs. 2 des Entwurfs enthaltene Figur der mitzuspeichernden Gegendarstellung entstammt dem Medienrecht (insbesondere § 41 Abs. 2 BDSG aF) und passt für die Datenverarbeitung zu künstlerischen Zwecken nicht. Es ist schon zweifelhaft, ob es überhaupt ein Recht auf Gegendarstellung gegenüber einem Kunstwerk, das kein Presse- oder Medienerzeugnis ist, geben kann. Art. 1 § 12 Abs. 2 des Entwurfs sollte daher gestrichen werden.

Außerdem sollte der Landesgesetzgeber für einen praktisch wichtigen **Bereich**, nämlich den **der behördlichen Öffentlichkeitsarbeit**, normenklare Bestimmungen in das Datenschutzgesetz aufnehmen. Die praktische Erfahrung in der Vergangenheit hat gezeigt, dass eine solche Rechtsgrundlage, die einen Ausgleich zwischen dem Informationsinteresse der Öffentlichkeit und dem Recht auf Datenschutz herstellt, dringend notwendig ist. Das Pressegesetz, das vermutlich separat an die Grundverordnung angepasst wird, konnte einen solchen Ausgleich schon in der Vergangenheit wegen seiner Unbestimmtheit nicht herstellen. Behördeninterne Anweisungen sind gleichfalls kein Ersatz für eine gesetzliche Regelung dieses wichtigen Bereichs. Auch das Hamburgische Transparenzgesetz bietet hier keine befriedigenden Lösungen an.

10. Die **Regelung des Begnadigungsverfahrens** in Art. 1 § 14 Satz 2 des Entwurfs ist insoweit fragwürdig, als die entsprechende Anwendung der Art. 5 bis 7 und des Kapitels IV der Grundverordnung mit Ausnahme des Artikels 33 vorgesehen ist. Zum einen ist nicht nachvollziehbar, weshalb die Rechte der Betroffenen, etwa das Auskunftsrecht pauschal ausgeschlossen wird. So hat ein Gefangener, dessen Begnadigung abgelehnt worden ist, ein prinzipiell legitimes Interesse zu erfahren, auf welche Informationen diese Entscheidung gestützt wird, was nicht ausschließt, dass bestimmte dieser Informationen im Einzelfall geheim zu halten sind. Auch ist nicht klar, in welchem Verhältnis Art. 1 § 14 dieses Gesetzentwurfs zu Art. 1 § 32 des Entwurfs zur Umsetzung der Richtlinie (EU) 2016/680 für den Hamburger Justizvollzug steht, der Betroffenen, also auch Gefangenen ein Auskunftsrecht einräumt. In gleicher Weise ist das Konkurrenzverhältnis zwischen § 14 des Entwurfs zur Anpassung des Hamburgischen Datenschutzgesetzes zu den übrigen Betroffenenrechten in den §§ 31, 33, 34 und 35 des Entwurfs für ein Hamburgisches Justizvollzugsdatenschutzgesetz ungeklärt. Grundsätzlich sollten die

Informationspflichten und Betroffenenrechte auch im Begnadigungsverfahren entsprechend gelten.

11. Die Datenschutz-Grundverordnung sieht eine erhebliche Stärkung der **Betroffenenrechte und Informationspflichten** vor. Darin liegt ein zentrales Anliegen des neuen europäischen Rechtsrahmens für den Datenschutz, der der zunehmenden Intransparenz der Datenverarbeitung und der wachsenden informationellen Fremdbestimmung entgegenwirken soll. Der Unionsgesetzgeber lässt eine Beschränkung dieser Rechte und Pflichten daher nur unter engen Voraussetzungen zu. Diese Voraussetzungen erfüllt der Senatsentwurf an mehreren Stellen nicht, er schränkt vielmehr die Betroffenenrechte teilweise noch weitergehend als der Bundesgesetzgeber ein.

a) Die öffentlichen Stellen Hamburgs dürfen nach Art. 1 § 15 Abs. 1 des Entwurfs generell in den dort aufgezählten Situationen keine Informationen erteilen. Dieses pauschale Informationsverbot geht über das Bundesdatenschutzgesetz hinaus (§§ 32, 33 BDSG nF), das zum einen Ausnahmen nur von einzelnen Informationspflichten vorsieht und zum anderen den verantwortlichen Stellen auch in den genannten Ausnahmefällen noch einen Ermessensspielraum belässt und sie nur von einer Informationspflicht freistellt. Art. 1 § 15 Abs. 1 Satz 1, 1. Halbsatz sollte deshalb wie folgt formuliert werden:

„Eine Pflicht zur Information gemäß Artikel 13 oder 14 der Verordnung (EU) 2016/679 besteht nicht, solange und soweit...“

b) Eine Information soll nach Art. 1 § 15 Abs.1 Nr. 1 ausgeschlossen sein, wenn sie die „öffentliche Ordnung“ gefährden würde. Eine solche Ausnahme sieht Art. 23 DSGVO entgegen der Entwurfsbegründung nicht vor. Auch kann der sehr weite Begriff der öffentlichen Ordnung im Sinne des deutschen Gefahrenabwehrrechts nicht unter den Begriff der öffentlichen Sicherheit im Sinne der DSGVO subsumiert werden. Die Worte „oder Ordnung“ in Art. 1 § 15 Abs. 1 Nr. 1 des Entwurfs sind deshalb zu streichen. Das würde auch den Wertungswiderspruch zu Art. 1 §§ 6 Abs. 2 Nr. 1, 16 Abs. 1 Nr. 1 und 18 Abs. 1 Nr. 1 des Entwurfs beseitigen, wo allein von einer Gefährdung der „öffentlichen Sicherheit“ die Rede ist.

Des weiteren verzichtet Art. 1 § 15 Abs. 1 Nr. 1 des Entwurfs im Gegensatz zu §§ 32 Abs. 1 Nr. 3 und 33 Abs. 1 Nr. 1 BDSG nF völlig auf eine Abwägung mit den Interessen der betroffenen Person. Dies ist ebenso wie der Verzicht auf spezifische Vorschriften, die Art. 23 Abs. 2 DSGVO zur Begrenzung der Ausnahmen vorschreibt, mit dem Unionsrecht nicht zu vereinbaren. Die Vorschrift sollte deshalb wie folgt ergänzt werden:

„und die Interessen des Verantwortlichen an der Nichterteilung der Information gegenüber den Interessen der betroffenen Person überwiegen.“

c) Art. 1 § 15 Abs. 1 Nr. 2 schließt jede Information aus, wenn die Tatsache der Verarbeitung nach einer Rechtsvorschrift geheim zu halten ist. Das geht über Art. 23

Abs. 1 lit. e DSGVO insofern hinaus, als dort nur der Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaates Ausnahmen von den Informationspflichten rechtfertigt. Nicht jede durch Rechtsvorschrift statuierte Geheimhaltungspflicht dient solchen wichtigen Zielen des allgemeinen öffentlichen Interesses, wie sie die DSGVO im Folgenden exemplarisch nennt. Die Worte „nach einer Rechtsvorschrift oder“ sollten deshalb entweder gestrichen oder in dem beschriebenen Sinn konkretisiert werden.

d) Art. 1 § 15 Abs. 1 Nr. 3 des Entwurfs geht ebenfalls insoweit über die DSGVO hinaus, als diese in Art. 23 Abs. 1 lit. d eine Beschränkung der Betroffenenrechte nur zur Verfolgung von Straftaten, nicht aber von Ordnungswidrigkeiten zulässt. Derartige Beschränkungen zur Ahndung von bloßem Verwaltungsunrecht wären zudem unverhältnismäßig. Die Worte „und Ordnungswidrigkeiten“ sind deshalb zu streichen.

e) Art. 1 § 15 Abs. 1 Nr. 4 des Entwurfs ist gleichfalls nicht verordnungskonform, weil die DSGVO in Art. 23 Abs. 1 lit. j Ausnahmen lediglich zur Durchsetzung zivilrechtlicher Ansprüche zulässt. Das Wort „rechtlicher“ ist deshalb durch „*zivilrechtlicher*“ zu ersetzen.

f) Auch Art. 1 § 15 Abs. 1 Nr. 5 des Entwurfs, der § 32 Abs. 1 Nr. 1 BDSG entspricht, steht im Gegensatz zur Grundverordnung. Diese differenziert nicht zwischen analoger und digitaler Datenverarbeitung, sondern schränkt ihren Anwendungsbereich für bestimmte Formen der nicht-automatisierten Datenverarbeitung ein (Art. 2 Abs. 1 DSGVO). Auch die Ausnahmetatbestände des Art. 23 DSGVO rechtfertigen diese Ausnahme nicht. Art. 1 § 15 Abs. 1 Nr. 5 ist deshalb zu streichen.

g) Nach Art. 1 § 15 Abs. 2 des Entwurfs sollen Informationen bezüglich einer Übermittlung ihrer Daten an die Sicherheitsbehörden, Finanzbehörden und Nachrichtendiensten nur im Einvernehmen mit diesen an die betroffenen Personen gegeben werden dürfen. Das geht insofern über die Datenschutz-Grundverordnung hinaus, als keine geeigneten Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Personen getroffen werden, wie sie Art. 14 Abs. 5 lit. c und Art. 23 Abs. 2 DSGVO vorschreiben. Zumindest müssten materielle Anforderungen formuliert werden, die erfüllt sein müssen, wenn die empfangenden Behörden die Herstellung des Einvernehmens verweigern wollen. Die Formulierung des Entwurfs lässt es zu, dass dies aus beliebigen Gründen geschieht. Die Grundverordnung erlaubt jedoch Ausnahmen von der Informationspflicht nur dann, wenn die Information über entsprechende Übermittlungen die nationale oder die öffentliche Sicherheit gefährdet. Im Grunde ist Art. 1 § 15 Abs. 2 des Entwurfs überflüssig, weil sein Regelungsziel bereits durch den Tatbestand des Art. 1 § 15 Abs. 1 Nr. 1 abgedeckt wird. Art. 1 § 15 Abs. 2 sollte daher gestrichen werden.

h) Beschränkungen der Betroffenenrechte setzen nach Art. 23 Abs. 2 der Grundverordnung spezifische kompensierende Vorschriften zur Verringerung der

Risiken für Rechte und Freiheiten der betroffenen Personen voraus. Dem genügt Art. 1 § 15 Abs. 2 des Entwurfs nicht hinreichend. Die Vorschrift sollte stattdessen wie folgt formuliert werden:

„Die Entscheidung, ob eine Information der betroffenen Person nach Maßgabe der Absätze 1 und 2 unterbleibt, trifft die Leitung der in § 2 Absatz 1 genannten öffentlichen Stelle. Die Gründe für ein Absehen von der Information sind zu protokollieren und der oder dem Datenschutzbeauftragten nach Art. 37 bis 39 der Verordnung (EU) 2016/679 mitzuteilen. In Zweifelsfällen ist die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zu konsultieren.“

i) Für die Beschränkung des Auskunftsrechts in Art. 1 § 16 Abs. 1 Nrn. 2 und 3 des Entwurfs gilt das oben unter Buchstaben c) und d) Gesagte. Bezüglich der in Art. 1 § 16 Abs. 3 vorgesehenen mit Art. 1 § 15 Abs. 2 übereinstimmenden Beschränkung ist auf das oben unter Buchstabe f) Gesagte zu verweisen.

j) Die erweiterte Pflicht zur **Benachrichtigung der betroffenen Personen über Datenlecks** nach Art. 34 der Grundverordnung ist ein zusätzliches wichtiges Element zur Modernisierung des Datenschutzrechts in Europa. Der Bundesgesetzgeber hat keine Notwendigkeit gesehen, diese Pflicht einzuschränken. Vor diesem Hintergrund sind die in Art. 1 § 18 des Entwurfs für die öffentlichen Stellen Hamburgs vorgesehenen Beschränkungen zu hinterfragen. So ist generell zweifelhaft, inwiefern die in den einzelnen Tatbeständen des Absatz genannten Gründe es rechtfertigen, die Tatsache, dass durch die Verletzung des Datenschutzes ein hohes Risiko für die betroffene Person wahrscheinlich ist, vor dieser dauerhaft geheim zu halten. Bezüglich der in Art. 1 § 18 Abs. 1 Nr. 2 des Entwurfs adressierten möglichen Auswirkungen einer Benachrichtigung auf die Verfolgung von Straftaten (die Ahndung von Ordnungswidrigkeiten ist ohnehin kein zugelassener Beschränkungszweck, s.o. Buchstabe d) enthält Erwägungsgrund 86 Satz 3 der Grundverordnung den Hinweis, dass solche Benachrichtigungen in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Dieser für die Interpretation der Grundverordnung maßgebliche Hinweis verdeutlicht, dass bereits das unmittelbar geltende Unionsrecht die verantwortliche Stelle dazu verpflichtet, von einer Benachrichtigung nur solange abzusehen, wie die Strafverfolgung dies erfordert. Ein endgültiges Absehen von der Benachrichtigung lässt die Grundverordnung dagegen nicht zu.

Auch für Art. 1 § 18 Abs. 1 Nr. 3 und 4 des Entwurfs ist keine Grundlage im Unionsrecht zu erkennen. Bezüglich des pauschalen Verweises auf Geheimhaltungsvorschriften gilt das oben unter Buchstabe c) Gesagte. Auch ist nicht erkennbar, auf welche Weise die Benachrichtigung betroffener Personen über hohe Risiken, die durch Datenlecks entstanden sind, Rechte und Freiheiten anderer Personen derart beeinträchtigen könnte, dass sie dauerhaft unterbleiben muss. Das in Art. 1 § 18 Abs. 1 Nr. 4 des Entwurfs verfolgte Ziel lässt sich zudem durch eine entsprechende Auslegung des Begriffs „unverzüglich“ in Art. 34 DSGVO erreichen.

Erwägungsgrund 86 der Grundverordnung weist ausdrücklich auf die Situation hin, in der eine Benachrichtigung zunächst zurückzustellen ist, wenn nach Abwägung mit den Auswirkungen der Schutzverletzung für die Betroffenen das Treffen geeigneter Maßnahmen gegen fortlaufende oder vergleichbare Schutzverletzungen vorrangig ist.

Art. 1 § 18 des Entwurfs sollte deshalb insgesamt gestrichen werden.

12. Die in Art. 1 § 19 Abs. 6 vorgesehene Übertragung der **Kontrollzuständigkeit gegenüber den Finanzbehörden des Landes** auf die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist abzulehnen. Schon die Entscheidung des Bundesgesetzgebers, diese Zuständigkeit auch dann bei der Bundesbeauftragten zu konzentrieren, wenn steuerrechtliche Vorschriften des Bundes angewandt werden, ist eine aus der Sicht des Bürgers problematische Durchbrechung des Grundsatzes, das die Datenverarbeitung durch öffentliche Stellen seines Landes auch dann von der jeweiligen Aufsichtsbehörde dieses Landes zu kontrollieren ist, wenn Bundesrecht ausgeführt wird. Damit geht ein erheblicher Verlust an Bürgernähe einher. Dies sollte nicht noch dadurch verschärft werden, dass die Bundesbeauftragte auch noch die Zuständigkeit für die Aufsicht über die Eintreibung von Landessteuern erhält, soweit dies auf bundeseinheitlichen Absprache beruht. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat zutreffend dargelegt, dass durch die Datenschutz-Grundverordnung kein mehrfacher Dokumentationsaufwand entsteht und dass die Datenschutzbeauftragten des Bundes und der Länder sich im Fall eines Programmierverbundes – wie schon bisher – abstimmen. Hamburg ist das einzige Bundesland, das erwägt, von der Ermächtigung in § 32h AO Gebrauch zu machen.

Art. 1 § 19 Absatz 6 ist zu streichen.

13. Auch die in Art. 1 § 23 des Entwurfs vorgesehenen **Pflichten des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit nach Ende der Amtszeit** sind im bundesweiten Vergleich beispiellos. Zwar sieht Art. 54 Abs. 1 lit. f DSGVO vor, dass die Mitgliedstaaten Bedingungen im Hinblick auf die Verbote von Handlungen, berufliche Tätigkeiten und Vergütungen während und nach der Amtszeit regeln, die mit den Pflichten des Mitglieds der Aufsichtsbehörde unvereinbar sind. Diese Vorschrift bezieht sogar Bedienstete der Aufsichtsbehörde mit ein, wenngleich der Entwurf nur Regelungen über Tätigkeiten des Hamburgischen Beauftragten nach Ende seiner Amtszeit enthält. Das Motiv des Unionsgesetzgebers für diese Vorschrift ergibt sich jedenfalls nicht aus Erwägungsgrund 121, der lediglich die Notwendigkeit belegt, durch die Unterlassung bestimmte Nebentätigkeiten während der Amtszeit eine Beeinträchtigung der Unabhängigkeit der Aufsichtsbehörde auszuschließen. Problematisch an der Regelung des Entwurfs ist insbesondere die Unbestimmtheit des Unvereinbarkeitskriteriums, über dessen Auslegung zudem die Präsidentin der Bürgerschaft entscheiden soll. Darin liegt zumindest indirekt eine Beeinträchtigung der Unabhängigkeit des Leiters oder der Leiterin der Aufsichtsbehörde. Auch ist

davon abzuraten, den oder die Nachfolgerin im Amt mit der Beurteilung zu betrauen, welche Handlung oder Tätigkeit des Amtsvorgängers mit dessen Amt unvereinbar ist. Man stelle sich etwa vor, ein ehemaliger Datenschutzbeauftragter vertritt oder berät nach dem Ende seiner Amtszeit Personen, deren Daten unrechtmäßig verarbeitet worden sind. Weil dies zu einem erheblichen Anstieg der Beschwerden bei der Dienststelle des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit führt, verbietet dieser seinem Vorgänger im Amt diese Tätigkeit, wogegen dieser sich gerichtlich wehren müsste. Insgesamt teile ich die Auffassung des Hamburgischen Datenschutzbeauftragten, dass das geltende Beamtenrecht in der Auslegung durch das Bundesverwaltungsgericht ausreicht, um die Fälle befriedigend zu regeln, die der Entwurf des Senats offenbar im Blick hat. Einen so unverhältnismäßigen Eingriff in die Freiheit der Berufsausübung, wie ihn der Entwurf zur Folge hätte, verlangt das Unionsrecht nicht.

Art. 1 § 23 ist zu streichen.

Zudem ist Art. 7 Abs. 2 des Entwurfs sowohl verfassungsrechtlichen als auch unionsrechtlichen Einwänden ausgesetzt. Mit dieser Vorschrift würde rückwirkend in die bestehende statusrechtliche Stellung des gegenwärtigen Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit eingegriffen. Das weicht nicht nur von Art. 7 des Gesetzes zur weiteren Stärkung der Unabhängigkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vom 20. Dezember 2016 ab, wo ausdrücklich noch die Unberührtheit der statusrechtlichen Stellung des Amtsinhabers betont wurde (ebenso § 72 des Entwurfs zur Anpassung des Berliner Datenschutzgesetzes an die Datenschutz-Grundverordnung), es beeinträchtigt auch seine unionsrechtlich garantierte völlige Unabhängigkeit.

Art. 7 Absatz 2 ist entsprechend Artikel 7 Absatz 1 Sätze 2 und 3 des Gesetzes zur weiteren Stärkung der Unabhängigkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vom 20. Dezember 2016 zu modifizieren.

14. Der Entwurf folgt in Art. 1 § 24 Abs. 3 dem Vorbild des Bundesgesetzgebers und schließt eine **Verhängung von Bußgeldern gegen Hamburger Behörden** aus. Die Möglichkeit dazu hat der Uniongesetzgeber zwar in Art. 83 Absatz 7 DSGVO vorgesehen. Ein solcher Schritt würde aber zu einer erheblichen Vollzugsasymmetrie zwischen dem Bereich der Wirtschaft, in dem Bußgelder verhängt werden können, und dem Bereich der Verwaltung führen. Auch wenn Bußgelder nach der Grundverordnung nicht das einzige Mittel sind, um die Rechtsbefolgung sicherzustellen, würde dann ein wichtiges Motiv für die Hamburgische Verwaltung zur Befolgung der Vorgaben des Datenschutzrechts entfallen. Weder den von Datenschutzverstößen betroffenen Personen noch der Öffentlichkeit ist zu vermitteln, weshalb die öffentliche Verwaltung gegenüber den Unternehmen in dieser Weise privilegiert werden sollte.

Art. 1 § 24 Absatz 3 des Entwurfs ist zu streichen.

15. Mit dem Inkrafttreten der Datenschutz-Grundverordnung am 25. Mai 2018 werden sich die **Aufgabenbereiche** der Datenschutzaufsichtsbehörden stark erweitern und damit der **Arbeitsaufwand** deutlich anwachsen. Unter den in Art. 57 DSGVO genannten 22 Aufgaben sind insbesondere als zusätzliche Aufgaben hervorzuheben:

- a) Beteiligung an Datenschutz-Folgeabschätzungen nach Art. 35 (Positiv-, Negativlisten);
- b) Verpflichtende Konsultation bei bestimmten Folgeabschätzungen nach Art. 36;
- c) Genehmigungen von Datenexporten in außereuropäische Staaten;
- d) Beteiligung an der Abstimmung unter den europäischen Datenschutzbehörden, nicht nur, aber insbesondere für die Landesaufsichtsbehörde, die die Bundesbeauftragte im Europäischen Datenschutzausschuss vertritt (bisher der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit). Der Abstimmungs- und Kooperationsaufwand insbesondere auf europäischer Ebene wird durch das neu eingeführte Kohärenzverfahren, durch die Pflicht zur Amtshilfe und die Beteiligung an gemeinsamen Maßnahmen der Aufsichtsbehörden drastisch zunehmen.

Ich halte es für nahezu ausgeschlossen, dass der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit mit seinen gegenwärtigen Ressourcen diese durch die Grundverordnung deutlich angewachsenen Aufgaben ausreichend wird erfüllen können.

Auch der hamburgische Haushaltsgesetzgeber ist unionsrechtlich verpflichtet, die Datenschutzaufsichtsbehörde „mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen..“ auszustatten, „...die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im (Europäischen Datenschutz) Ausschuss effektiv wahrnehmen zu können“(Art. 52 Absatz 4 DSGVO).

Die Grundverordnung regelt die Aufgaben der Aufsichtsbehörden selbst sehr detailliert und differenziert dabei auch zwischen Pflicht- und fakultativen Aufgaben. Der Landesgesetzgeber hat praktisch keine Möglichkeiten, hier zusätzlich steuernd einzugreifen.

16. Die Datenschutzgrundverordnung enthält selbst keine positive Regelung der Frage, unter welchen Umständen die Aufsichtsbehörden für ihre Tätigkeiten **Verwaltungsgebühren** erheben dürfen. Dies zu regeln bleibt den Mitgliedstaaten überlassen. Lediglich Art. 57 Abs. 3 und 4 der Grundverordnung sehen zum einen vor, dass die Aufsichtsbehörde ihre Aufgaben für Betroffene und Datenschutzbeauftragte grundsätzlich unentgeltlich zu erfüllen hat und nur in Ausnahmefällen von Betroffenen eine Missbrauchsgebühr verlangen darf. Art. 1 § 25 Absatz 1 des Entwurfs sieht zwar eine grundsätzliche Gebührenpflicht nicht-

öffentlicher Stellen für Amtshandlungen der Aufsichtsbehörde vor, Absatz 2 Satz 2 schränkt diesen Grundsatz jedoch in einer vom Unionsrecht nicht vorgegebenen Weise ein. Artikel 57 Abs. 3 DSGVO würde es auch zulassen, bei der kontrollierten Stelle eine Verwaltungsgebühr zu erheben, wenn die z.B. von einer betroffenen Person veranlasste Prüfung nicht zur Feststellung von Mängeln führt. Der Verwaltungsaufwand entsteht auch in solchen Fällen. Auch ist die Beschränkung der grundsätzliche Gebührenpflicht auf nicht-öffentliche Stellen nicht vom Unionsrecht vorgegeben. Das Bundesgebührengesetz (§ 7 Nr. 6) sieht zwar für Behörden in bestimmten Situationen (Rechts- und Fachaufsicht) eine sachliche Gebührenfreiheit vor. Es besteht aber für den Landesgesetzgeber durchaus die Möglichkeit, auch die Kontrolle von öffentlichen Stellen durch die Hamburgische Datenschutzaufsichtsbehörde gebührenpflichtig zu gestalten.

Weitere naheliegende Fälle aus dem umfangreichen Aufgabenkatalog des Art. 57 sind beispielweise

- a) die Abgabe einer Stellungnahme zu und die Genehmigung von Entwürfen von Verhaltensregeln nach Art. 40 Absatz 5 DSGVO,
- b) die Akkreditierung einer Stelle zur Überwachung der Einhaltung von Verhaltensregeln nach Artikel 41 und einer Zertifizierungsstelle nach Artikel 43,
- c) die Genehmigung von Datenexporten in Drittstaaten nach Artikel 46 DSGVO und von verbindlichen internen Unternehmensregeln für denselben Zweck nach Artikel 47 DSGVO.

Im Gegensatz zu Bußgeldern, die künftig aufgrund des deutlich erweiterten Bußgeldrahmens zu erheblichen Mehreinnahmen für den Landeshaushalt der Freien und Hansestadt führen dürften, würden Verwaltungsgebühren dem Etat der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit direkt zugute kommen.

17. Schon bisher hat die **Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden** in Deutschland eine wesentliche Rolle bei der Kontrolle der Verarbeitung personenbezogener Daten gespielt. Das galt im öffentlichen wie im nicht-öffentlichen Bereich. Dazu haben die Datenschutzbehörden des Bundes und der Länder im Rahmen der Datenschutzkonferenz bewährte Kooperationsstrukturen sowohl auf Leitungs- wie auf Arbeitsebene aufgebaut. So haben einzelne Datenschutzbehörden aufgrund des bei ihnen vorhandenen Sachverständes den Vorsitz in bestimmten themenorientierten Arbeitsgebieten übernommen, um in diesen Bereichen die Datenschutzkontrolle bundesweit zu koordinieren und auf diese Weise möglichst große Synergieeffekte zu erzielen. Diese Formen der Kooperation werden unter der Geltung der Datenschutz-Grundverordnung noch wichtiger werden, zumal die Ausstattung der Aufsichtsbehörden in den einzelnen Bundesländern auch in Zukunft stark von einander abweichen wird.

Die Zusammenarbeit wird sich insbesondere in allen Tätigkeitsfeldern intensivieren, in denen ein Bezug zur europäischen Ebene besteht, etwa weil Entscheidungen des Europäischen Datenschutzausschusses vorbereitet werden müssen. Auch die gegenseitige Amtshilfe und die Durchführung gemeinsamer Maßnahmen, die erstmals in der Grundverordnung vorgesehen sind, werden neben dem zusätzlichen Aufwand (s.o. Nr. 15) auch eine besser koordinierte Rechtsdurchsetzung zur Folge haben. Auch in den Fällen, in denen mit dem Inkrafttreten der Grundverordnung die Zuständigkeit z.B. für US-amerikanische Unternehmen wie Google oder Facebook einer anderen europäischen Datenschutzbehörde zugewiesen wird, ist davon auszugehen, dass der Standpunkt der deutschen Datenschutzbehörden bei der europäischen Abstimmung maßgeblich vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit formuliert werden wird, der für die deutschen Niederlassungen dieser Unternehmen zuständig ist und deren Datenverarbeitung schon bisher mit der gebotenen Konsequenz kontrolliert hat.

Schließlich hat der Bundesgesetzgeber auch in Fällen, in denen Unternehmen Niederlassungen in verschiedenen Bundesländern haben, ohne Daten grenzüberschreitend zu verarbeiten, eine Zuständigkeitskonzentration bei der Datenschutzbehörde der Hauptniederlassung angeordnet (§ 40 Abs. 2 BDSG), was Reibungsverluste bei der föderalen Datenschutzkontrolle reduzieren dürfte.

C. Zusammenfassung

1. Der Entwurf zur Umsetzung der Richtlinie (EU) 2016/680 im Justizvollzug relativiert den unionsrechtlichen Begriff der Erforderlichkeit in unzulässiger Weise. Die Worte „unbedingt erforderlich“ sollten jeweils durch „unerlässlich“ ersetzt werden.
2. Die vorgeschlagenen Regelungen zu Sicherheitsanfragen über Gefangene und anstaltsfremde Personen sind unverhältnismäßig und nicht geeignet, der versteckten Radikalisierung in Haftanstalten wirksam zu begegnen. Sie sollten ebenso wie die Regelung zur Zuverlässigkeitsüberprüfung von Besucherinnen und Besuchern restriktiver gefasst werden.
3. Dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit müssen nach dem Unionsrecht auch im Justizvollzug wirksame Einwirkungsbefugnisse zustehen, was die Möglichkeit umfasst, bestimmte Anordnungen zu treffen.
4. Der Entwurf zur Anpassung des Hamburgischen Datenschutzgesetzes sollte entsprechend dem Bundesdatenschutzgesetz um die Klarstellung ergänzt werden, dass das Unionsrecht im Zweifel vorrangig anzuwenden ist.
5. Die Kündigung und Abberufung des (behördlichen) Datenschutzbeauftragten sollte einschränkend entsprechend § 626 BGB geregelt werden.

6. Zudem entspricht in zahlreichen Punkten nicht den Vorgaben des Unionsrechts oder trifft redundante Regelungen:

a) Die Zweckänderungsbefugnisse des Art. 1 § 6 Abs. 2 Nrn. 5 und 9 sind überflüssig und deshalb zu streichen.

b) Das Wort „Verarbeitungsverbot“ in Art. 1 § 6 Abs. 3 Satz 2 sollte durch „Verwertungsverbot“ ersetzt werden.

c) Bei der Einrichtung automatisierter Abrufverfahren (Art. 1 § 24) sollte am bisherigen Anhörungsrecht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit auf gesetzlicher Ebene festgehalten werden. Zudem sollte einer unbegrenzten informationellen Selbstbedienung der abrufenden Stellen nach bayerischem Vorbild dadurch vorgebeugt werden, dass die den Abruf zulassende Stelle zu einer stichprobenhaften Feststellung des Abrufs verpflichtet wird.

d) Bezüglich der Videoüberwachung sollte bei der Erkennbarmachung der verantwortlichen Stelle wie im Bundesrecht auch die Nennung ihres Namens und ihrer Kontaktdaten vorgeschrieben werden.

e) Die vorgesehene Regelung des Beschäftigtendatenschutzes ist teilweise missverständlich und sollte zum einen präzisiert und zum anderen um die Klarstellung ergänzt werden, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben.

f) Die Informationspflichten der verantwortlichen Stellen und die Rechte betroffener Personen haben in der Grundverordnung einen hohen Stellenwert erhalten. Der Gesetzentwurf des Senats schränkt diese Pflichten und Rechte teilweise noch weitergehend als das Bundesdatenschutzgesetz ein und widerspricht in mehreren Punkten dem Unionsrecht. Auch für die Beschränkung der Benachrichtigungspflicht Hamburger Behörden über Datenlecks fehlt eine unionsrechtliche Grundlage.

g) Die Regelung der Meinungsäußerung zu künstlerischen Zwecken (Art. 1 § 12) erscheint aus mehreren Gründen verfehlt. Stattdessen sollte die Öffentlichkeitsarbeit von Behörden, soweit sie die Offenbarung personenbezogener Daten betrifft, landesgesetzlich geregelt werden, um einen Ausgleich zwischen dem Informationsinteresse der Öffentlichkeit und dem Recht Betroffener auf informationelle Selbstbestimmung herzustellen, wie es Art. 85 der Grundverordnung vorsieht.

h) Auch die Regelung des Begnadigungsverfahrens in Art. 1 § 14 Abs. 2 schränkt die Betroffenenrechte, insbesondere das Auskunftsrecht zu stark ein. Auch ist das Verhältnis zu den Regelungen im Entwurf eines Gesetzes für den Justizvollzug unklar.

i) Die weitergehende Übertragung der Kontrolle von Finanzbehörden der Freien und Hansestadt, wie sie der Entwurf vorsieht, ist abzulehnen. Bereits die Entscheidung des Bundesgesetzgebers für eine Zentralisierung der Datenschutzkontrolle bei

Bundessteuern hat zu einem Verlust an Bürgernähe geführt, der nicht noch verschärft werden sollte.

j) Die vorgeschlagene Regelung der Pflichten des Hamburgischen Datenschutzbeauftragten nach dem Ende seiner Amtszeit sind im bundesweiten Vergleich beispiellos, überflüssig und führen zu einem unverhältnismäßigen Eingriff in die Freiheit der Berufsausübung, der vom Unionsrecht nicht gerechtfertigt ist. Zugleich liegt in ihr zumindest ein indirekter Eingriff in die völlige Unabhängigkeit der Aufsichtsbehörde. Auch greift die Übergangsbestimmung des Art. 7 des Entwurfs in unzulässiger Weise in die statusrechtliche Stellung des gegenwärtigen Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ein.

7. Auch gegen Behörden sollte – abweichend vom Entwurf (Art. 1 § 24 Abs. 3)- die Verhängung von Bußgeldern ermöglicht werden.

8. Die Aufgabenbereiche der Datenschutzbehörden werden durch die Datenschutz-Grundverordnung stark erweitert, ohne dass der Landesgesetzgeber dies beeinflussen könnte. Es erscheint nahezu ausgeschlossen, dass der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit mit seinen gegenwärtigen Ressourcen die zusätzlichen neben den Aufgaben nach bisherigem Recht ausreichend wird erfüllen können. Der Haushaltsgesetzgeber ist auch in Hamburg unionsrechtlich verpflichtet, die notwendige personelle und finanzielle Ausstattung der Datenschutzbehörde sicherzustellen.

9. Der Landesgesetzgeber hat die Möglichkeit, über den vorgelegten Entwurf des Senats hinaus die Erhebung von Verwaltungsgebühren auch gegenüber Behörden zu ermöglichen.

10. Die Zusammenarbeit der Datenschutzbehörden auf europäischer und deutscher Ebene wird durch die Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz erheblich an Bedeutung zunehmen. Dadurch können Synergieeffekte für einen verbesserten Datenschutz entstehen.