Erläuterungen
zum Hamburgischen Datenschutzgesetz

(vom 5. Juli 1990 mit den Änderungen vom 18. März 1997 und 30. Januar 2001)

I.

Vorbemerkung

Für die nachstehenden Erläuterungen sind folgende Materialien weithin wörtlich verwendet worden:

– die „Ergänzte Begründung“ zum Hamburgischen Datenschutzgesetz vom 5. Juli 1990 gemäß der Broschüre „Das neue Datenschutzrecht“ in der Reihe „Hamburger Datenschutzhefte“ (seit längerem vergriffen)

– die Begründung des Senats zur Änderung des Hamburgischen Datenschutzgesetzes gemäß der Senatsmitteilung vom 21. November 1995 (Bürgerschafts-Drs. 15/4411)

– der Bericht des bürgerschaftlichen Rechtsausschusses vom 25. Februar 1997 (Bürgerschafts-Drs. 15/7012) über die Beratungen zur Novellierung des Hamburgischen Datenschutzgesetzes

– die Begründung des Senats zur Änderung des Hamburgischen Datenschutzgesetzes gemäß der Senatsmitteilung vom 14. März 2000 (Bürgerschafts-Drs. 16/3995)

– der Bericht des bürgerschaftlichen Rechtsausschusses vom 14. Dezember 2000 (Bürgerschafts-Drs. 16/5345) über die Beratungen zur weiteren Novellierung des Hamburgischen Datenschutzgesetzes.

Die Materialien sind aktualisiert und redaktionell überarbeitet worden, soweit dies infolge ihrer Zusammenfassung erforderlich erschien; insbesondere wurden auch die Verweisungen der oben erwähnten „Ergänzten Begründung“ auf das insoweit überholte erste Hamburgische Datenschutzgesetz von 1981 beseitigt. Außerdem sind die Materialien durch eigene Ausführungen ergänzt worden, wo dies zum besseren Verständnis angebracht war. Schließlich wurden gelegentlich Zusätze zur Klarstellung bei Datenschutzregelungen eingefügt, deren Auslegung oder Anwendung in der Praxis wiederholt zu Zweifeln und Missverständnissen geführt hat.

Die Erläuterungen sind – wie seinerzeit die „Ergänzte Begründung“ – mit der für das hamburgische Datenschutzrecht federführenden Justizbehörde abgestimmt worden. Wegen weitergehender oder abweichender Auffassungen des Hamburgischen Datenschutzbeauftragten, die bei den Gesetzesnovellierungen nicht aufgegriffen wurden, kann auf die angegebenen Berichte des Rechtsausschusses und zur näheren Darstellung auf die Tätigkeitsberichte des Hamburgischen Datenschutzbeauftragten aus den letzten Jahren verwiesen werden.

II.

Allgemeines

1. **Ausgangslage und Ziele**

   Das Bundesverfassungsgericht hat in seinem Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 (BVerfGE 65, 1 ff.) grundlegende verfassungsrechtliche Aussagen zum Datenschutz getroffen. Danach wird insbesondere unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Weitergabe und Verwendung seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikels 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes (GG) umfasst. Dieses Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (Recht auf informationelle Selbstbestimmung).

   Damit ist der Datenschutz als Konkretisierung eines wesentlichen Aspekts des Persönlichkeitsrechts anerkannt; er hat Verfassungsrang erhalten. Mit diesem Grundrecht auf informationelle Selbstbestimmung ist eine Gesellschaftsordnung und eine diese stützende Rechtsordnung unvereinbar, in der der Bürger nicht mehr wissen

kann, wer was wann und bei welcher Gelegenheit über ihn weiß (BVerfGE a.a.O., S. 43).

Das Hamburgische Datenschutzgesetz vom 5. Juli 1990 (HmbGVBl. S. 133, 165, 226) ist nach wie vor ein modernes und fortschrittliches Gesetz. Das schließt jedoch Änderungsbedarf nicht aus. Gerade die noch relativ junge Materie Datenschutzrecht ist ein dynamisches Rechtsgebiet.

Mit der Novelle vom 18. März 1997 (HmbGVBl. S. 76) wurden neben notwendigen Anpassungen an das Bundesdatenschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2955), zuletzt geändert am 14. September 1994 (BGBl. I S. 2325, 2384, 2385), auch Unstimmigkeiten weitgehend redaktioneller Art im geltenden Gesetz beseitigt, die sich bei der Anwendung des Gesetzes gezeigt haben. Der Vergleich mit den seit Ende 1990 neu erlassenen Landesdatenschutzgesetzen hat Anregungen erbracht, aus denen weitere Änderungsvorschläge resultierten. Einige kleinere Änderungen waren Reaktionen nach Entscheidungen des Bundesverfassungsgerichts. Schließlich haben mehrere bürgerschaftliche Ersuchen den Senat zu einzelnen Vorschlägen für Gesetzesänderungen veranlasst.

Schwerpunkte dieser Novelle waren:

- Präzisierung des Anwendungsbereichs des Gesetzes (§2 Absätze 1 bis 3),
- Ergänzung der Grundsatzregelung über die Zulässigkeit der Datenverarbeitung um den Grundsatz der Datenvermeidung (§5 Absatz 4),
- Verfahrensvereinfachungen bei den Dateibeschreibungen (§9 Absätze 1 und 4) und Verzicht auf das Dateiregister (§24),
- Normierung der Pflicht zur Risikoanalyse vor Einführung oder der wesentlichen Änderung eines automatisierten Verfahrens (§8 Absatz 4),
- Schaffung einer Vorschrift für die Datenverarbeitung in oder aus gemeinsamen und verbundenen automatisierten Dateien (§11a),
- Stärkung der Rechtsstellung der bzw. des Hamburgischen Datenschutz beauftragten durch Abschaffung der Rechtsaufsicht des Senats (§22 Absatz 1) und durch Einräumung des Rechts, sich jederzeit an die Bürgerschaft wenden zu können (§23 Absatz 3),
- Präzisierung der Regelung über die Stellvertretung der bzw. des Hamburgischen Datenschutzbeauftragten (§22 Absatz 3),
- Erweiterung der Prüfungsbefugnisse der bzw. des Hamburgischen Datenschutzbeauftragten bei den Gerichten und beim Rechnungshof (§23 Absatz 1),
- Änderung der Vorschrift über die Datenverarbeitung bei Beschäftigungsverhältnissen, Vereinheitlichung der Regelungen über die Verarbeitung von Personalaktendaten (§28),
- Einführung einer Vorschrift über das Fernmessen und Fernwirken (§29).

Die weitere Novelle vom 30. Januar 2001 (HmbGVBl. S. 9) ist durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG Nr. L 281/31 – im Folgenden: EG-Datenschutzrichtlinie) veranlasst. Gleichzeitig nutzt sie die Gelegenheit der notwendigen Richtlinienumsetzung, um das hamburgische Datenschutzrecht weiter zu modernisieren und zukunftssicher auszugestalten. Sich bietende Möglichkeiten zur Verwaltungsvereinfachung wurden genutzt und damit dem Bedürfnis nach einem nicht nur effektiven, sondern auch effizienten Datenschutzrecht im Rahmen der bestehenden Regelungsspielräume Rechnung getragen.

Zentrales Anliegen der EG-Datenschutzrichtlinie ist die Vereinheitlichung von Datenschutzstandards zur Gewährleistung eines freien Datenverkehrs im europäischen Wirtschaftsraum. Die Richtlinie ist deshalb in erster Linie für den Datenschutz im nicht-öffentlichen Bereich von Belang, der nicht in die landesgesetzliche Zuständigkeit fällt. Da sie insgesamt nicht zwischen öffentlichem und nicht-öffentlichem Bereich differenziert, erfordert sie gleichwohl auch eine Reihe von Änderungen des allgemeinen Datenschutzrechts für den öffentlichen Bereich. In Wesentlichen sind dabei die folgenden Änderungen des Hamburgischen Datenschutzgesetzes zu nennen:

- die Einschränkung der Verarbeitung besonders sensibler Daten (§5 Absatz 1 Satz 2);
- die Schaffung des Rechts, aus persönlichen Gründen Einwendungen auch gegen eine rechtmäßige Datenverarbeitung zu erheben (§5 Absatz 3);
- die Einführung einer Bestimmung über automatisierte Einzelentscheidungen (§5a);

– die Einführung von Bestimmungen über die Vorabkontrolle von Datenverarbeitungsverfahren, von denen eine besondere Gefährdung für die Rechte Betroffener ausgeht (§8 Absatz 4);
– die Ersetzung der Dateibeschreibungen durch Verfahrensbeschreibungen, die für jedermann einsehbar sind (§9);
– die Schaffung der Möglichkeit zur Bestellung behördlicher Datenschutzbeauftragter (§10a);
– die Erweiterung der Pflichten zur Unterrichtung Betroffener im Rahmen von Datenerhebungen (§12a);
– die Neuregelung der Übermittlungen ins Ausland unter Gleichstellung EU-weiter mit inländischen Übermittlungen (§17);
– die Erweiterung des Inhalts von Auskunfts- und Nachberichtspflichten (§§18 und 19);
– die Erweiterung des Schadenersatzanspruchs wegen unzulässiger oder unrichtiger Datenverarbeitung (§20).

Über die Richtlinienumsetzung hinaus wird das Hamburgische Datenschutzgesetz durch folgende Bestimmungen weiterentwickelt und den aktuellen und künftigen Bedürfnissen eines modernen Datenverarbeitungsumfeldes angepasst:

– Aufnahme einer Bestimmung über die Verarbeitung personenbezogener Daten anlässlich von Beratungs- und Gutachtenaufträgen (§3);
– Erweiterung der Schriftform auf digital gespeicherte Dokumente (§4a);
– Schaffung einer Regelung, die den besonderen datenschutzrechtlichen Risiken des Chipkarteneinsatzes begegnet (§5b);
– Neufassung des Katalogs der Datensicherungsmaßnahmen unter technologieoffener Überarbeitung der verwendeten Begrifflichkeiten (§8);
– Abschaffung des Geräteverzeichnisses (§9);
– Regelung der Datenerhebung über Personenkreise, insbesondere im Rahmen einer Videoüberwachung (§12).

2. **Grundlinien des Gesetzes**

Entsprechend der Bedeutung des Grundrechts auf informationelle Selbstbestimmung kann ein Datenschutzgesetz sich nicht auf den Schutz des Einzelnen vor Missbrauch der auf seine Person bezogenen Daten beschränken. Das Gesetz erkennt das Recht des Bürgers an, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, und regelt im einzelnen, unter welchen Voraussetzungen dieses Recht eingeschränkt werden darf.

Das Gesetz erfasst nicht nur die Datenverarbeitung in und aus Dateien, sondern auch die aktenmäßige Datenverarbeitung.

Dem Schutz des Rechts auf informationelle Selbstbestimmung entspricht die Einbeziehung einer jeden Phase der Datenverarbeitung in den Regelungsbereich des Gesetzes. Damit werden insbesondere auch die Erhebung und die weitere Verwendung von Daten unter den Schutz des Gesetzes gestellt. Dabei ist die Datenverarbeitung auch an dem Ziel auszurichten, dass so wenig personenbezogene Daten wie möglich erhoben und weiter verarbeitet werden. Der Bürger muss wissen können, wer was und bei welcher Gelegenheit über ihn weiß. Auch gibt es unter den Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr.

Es werden daher Regelungen getroffen, die klar vorschreiben, zu welchem Zweck personenbezogene Daten erhoben und weiterverarbeitet werden dürfen. Die Betroffenen müssen wissen und darauf vertrauen können, dass die ihre Person betreffenden Daten im Grundsatz nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden. Das Gesetz selbst umschreibt die eng umrissenen Ausnahmetatbestände vom Gebot der Zweckbindung. Das Gebot der Zweckbindung gilt für alle Phasen der Datenverarbeitung.

Automatisierte Abrufverfahren rufen besondere Gefährdungsmöglichkeiten für das Recht auf informationelle Selbstbestimmung hervor. Das Gesetz enthält insoweit besondere Regelungen; unter anderem lässt es die Einrichtung solcher Verfahren unter verschiedenen öffentlichen Stellen nur auf Grund einer Rechtsverordnung zu. Hinzu kommt eine entsprechende Regelung für die Datenverarbeitung bei gemeinsamen oder verbundenen automatisierten Dateien.

Das Gesetz enthält umfassende Regelungen über das Auskunftsrecht; nur ein weitgehendes Auskunftsrecht sichert die Ausübung des Rechts auf informationelle Selbstbestimmung. Die Betroffenen haben einen Rechtsanspruch
auf unentgeltliche Auskunft über die zu ihrer Person gespeicherten Daten, über die Zweckbestimmungen und die Rechtsgrundlage der Speicherung sowie über die Herkunft der Daten, die Empfängerinnen oder Empfänger oder

den Kreis der Empfängerinnen oder Empfänger und die Teilnahme an einem automatisierten Abrufverfahren sowie in den Fällen des §5a den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten. Außerdem wird klargestellt, dass die Verwaltung nach pflichtgemäßem Ermessen die Auskunft auch im Wege der Akteneinsicht oder durch einen Ausdruck der gespeicherten Daten erteilen kann. Die erforderlichen Einschränkungen dieses Auskunftsrechts werden klar umschrieben. Die Betroffenen haben weiterhin einen Anspruch auf Berichtigung, Sperrung und Löschung von Daten, unter besonderen Voraussetzungen auch einen Anspruch auf Schadensersatz.

In Übereinstimmung mit den Forderungen des Bundesverfassungsgerichts sind bereits im Gesetz von 1990 die Anforderungen an eine interne und externe Kontrolle verstärkt worden. Der internen Kontrolle dient die Verpflichtung der Daten verarbeitenden Stellen, eine laufend auf dem neuesten Stand zu haltende Verfahrensbeschreibung zu erarbeiten; auf ihrer Grundlage werden interne und externe Kontrollen erleichtert.

Der externen Kontrolle dient die Institution unabhängiger Datenschutzbeauftragter, deren Mitwirkung nach dem Bundesverfassungsgericht von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung ist. Die Rechtsstellung der bzw. des Hamburgischen Datenschutzbeauftragten wurde durch die Novelle vom 18. März 1997 dadurch gestärkt, dass die Rechtsaufsicht des Senats abgeschafft wurde und ihr bzw. ihm das Recht eingeräumt wurde, sich jederzeit an die Bürgerschaft zu wenden. Ihre bzw. seine Prüfungsbefugnisse wurden bei den Gerichten und beim Rechnungshof erweitert. Gesetzliche Geheimhaltungsvorschriften können einem Auskunfts- oder Akteneinsichtsverlangen der bzw. des Datenschutzbeauftragten nicht entgegengehalten werden (§23 Absatz 5 Satz 3). Lediglich für die Einsicht in sicherheitsrelevante Akten sieht das Gesetz engbegrenzte Ausnahmen vor (§23 Absatz 6 Satz 2).

Das Gesetz enthält weiterhin besondere Datenschutzregelungen für spezifische Bereiche. Von großer Bedeutung für die Praxis ist dabei die „Forschungsklausel“ (§27). Zu erwähnen sind aber auch die – ergänzenden – Regelungen zum Datenschutz der Beschäftigten (§28) und zur Datenverarbeitung für Planungszwecke (§30).

3. **Kosten und sonstige Auswirkungen**

Die Sicherung des Rechts auf informationelle Selbstbestimmung durch einen zeitgemäßen Standard des Datenschutzes ist ein bedeutsamer Aspekt der rechtmäßigen Aufgabenerfüllung durch die öffentliche Verwaltung und deren Akzeptanz bei den Bürgern. Insofern besteht keine Alternative zu einem gewissen zusätzlichen Verwaltungsaufwand zur Beachtung des Datenschutzes.

Ein der Höhe nach nicht bestimmbarer Mehraufwand ist mit der (fakultativen) Bestellung behördlicher Datenschutzbeauftragter gemäß der Novelle vom 30. Januar 2001 verbunden. Allerdings sind die von den behördlichen Datenschutzbeauftragten wahrzunehmenden Aufgaben größtenteils bereits bisher in den Daten verarbeitenden Stellen zu erfüllen. Bei der Bestellung behördlicher Datenschutzbeauftragter wird es deshalb im Wesentlichen um eine Zusammenfassung der in verschiedenen Bereichen der Daten verarbeitenden Stelle bereits wahrzunehmenden Aufgaben gehen, deren Aufwand zu einem großen Teil durch entsprechende organisatorische Maßnahmen zu kompensieren sein wird.

Die mit der Novelle vom 18. März 1997 normierte Pflicht zur Durchführung einer Risikoanalyse vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens (§8 Absatz 4) kann weiterhin zu gewissem Mehraufwand führen. Diese Kosten dürften sich aber dadurch amortisieren, dass hierdurch teure Korrekturen im installierten System unterbleiben oder jedenfalls reduziert werden können. Dies gilt auch für die Untersuchungen, die zu einer Vorabkontrolle gemäß dem mit der Novelle vom 30. Januar 2001 angefügten §8 Absatz 4 Satz 3 führen. Der Hamburgische Datenschutzbeauftragte geht davon aus, dass die für die Untersuchung zuständige Stelle mit deren Ergebnis jeweils auch die Begründung als Voraussetzung für eine Vorabkontrolle zuleitet.

Die Daten verarbeitenden Stellen, die behördliche Datenschutzbeauftragte bestellen, haben die Aufgabe der unabhängigen Vorabkontrolle solcher automatisierter Datenverarbeitungen, von denen nach dem Ergebnis der Risikoanalyse eine besondere Gefährdung für die Rechte Betroffener ausgeht. Da solche Datenverarbeitungen je nach Aufgabenstellung der verarbeitenden Stelle unterschiedliche Bedeutung haben, insgesamt aber nicht allzu häufig sein werden, lässt sich der daraus resultierende Aufwand nicht sicher qualifizieren.

Sofern Daten verarbeitende Stellen keine behördlichen Datenschutzbeauftragten bestellen, fällt die Aufgabe der Vorabkontrolle der bzw. dem Hamburgischen Datenschutzbeauftragten zu. Der Hamburgische Datenschutzbeauftragte wird bis Ende 2002 dem Rechtsausschuss/Unterausschuss Datenschutz gemäß §23 Absatz 3 Satz 3 HmbDSG über die Auswirkungen berichten, die sich aus seiner vorgesehenen Beteiligung an

der Vorabkontrolle nach dem neuen §8 Absatz 4 Satz 3 HmbDSG ergeben.

Mit der Novelle vom 30. Januar 2001 werden die bisherigen Unterrichtungs- und Auskunftspflichten gemäß der EG-Datenschutzrichtlinie erweitert. Damit ist ein nicht quantifizierbarer zusätzlicher Aufwand für die Daten verarbeitenden Stellen verbunden. Allerdings ist aufgrund der Ausschöpfung der nach der EG-Datenschutzrichtlinie zulässigen Ausnahmen und Beschränkungen kein wesentlicher Mehraufwand zu erwarten. Dasselbe gilt für die verfahrensmäßige Verwirklichung des Rechts, aus persönlichen Gründen Einwendungen gegen eine Datenverarbeitung zu erheben und Einsicht in die Verfahrensbeschreibungen zu nehmen sowie für die Erweiterung des Schadenersatzanspruchs wegen unzulässiger oder unrichtiger Datenverarbeitung. Diese Instrumente dürften in der Praxis (weiterhin) eine nur untergeordnete Rolle spielen.

III.

Zu den einzelnen Vorschriften

Zu §1 (Aufgabe des Datenschutzes)

Der Wortlaut von §1 macht deutlich, dass es nicht allein die Aufgabe des Gesetzes ist, den Missbrauch bei der Verarbeitung personenbezogener Daten zu verhindern, sondern dass es um grundsätzliche Regelungen für den Gebrauch personenbezogener Daten im öffentlichen Bereich geht. Es soll der Schutz des Einzelnen vor möglichen Gefährdungen oder Beeinträchtigungen gewährleistet werden, die sich aus der bloßen Informationsverarbeitung durch die öffentliche Verwaltung ergeben können. In seinem Urteil zum Volkszählungsgesetz (BVerfGE 65,1) hat das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung als Befugnis des Einzelnen definiert, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Da diese Beschreibung für die Betroffenen verständlicher ist als der Begriff der informationellen Selbstbestimmung, wurde sie bei der Darlegung der Aufgabe des Gesetzes an den Anfang gestellt.

Das Bundesverfassungsgericht hat aber in diesem Urteil auch ausgeführt, dass der Einzelne grundsätzlich „Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen muss“. Das Gericht hat weiter festgestellt, dass diese Beschränkungen „einer gesetzlichen Grundlage bedürfen, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht“. Da auch die Schaffung dieser rechtlichen Grundlagen zu der Aufgabe des Gesetzes gehört, wurde sie ebenfalls in §1 aufgenommen, um die Zweiseitigkeit im Verhältnis der Interessen des Einzelnen und der Allgemeinheit deutlich zu machen.

Das Gesetz umfasst auch die aktenmäßige Datenverarbeitung. Das ist erforderlich, da das Grundrecht auf informationelle Selbstbestimmung für jede Form der Datenverarbeitung, also auch für die Datenverarbeitung in Akten gilt. Soweit Besonderheiten der aktenmäßigen Datenverarbeitung eine Abweichung von den allgemeinen Grundsätzen erfordern, werden die – wenigen – Sonderregelungen im Zusammenhang mit den jeweiligen Grundregelungen formuliert.

Das Hamburgische Datenschutzgesetz trifft als „Querschnittsgesetz“ die grundlegenden Regelungen zum Schutze des Einzelnen bei der Datenverarbeitung durch öffentliche Stellen, doch gehen besondere Datenschutzregelungen vor (Subsidiarität). Die Notwendigkeit zu entsprechenden bereichsspezifischen Regelungen besteht im größerem Umfang.

Zu §2 (Anwendungsbereich)

In Absatz 1 wird der Anwendungsbereich des Gesetzes beschrieben. In Nummer 1 wird die Bürgerschaft ausdrücklich genannt. Das Gesetz gilt für die Bürgerschaft bei allen ihren Tätigkeiten. Ihre besondere Stellung ist durch die Formulierung eines entsprechenden Tatbestandes im Katalog der Zweckdurchbrechungen (§13 Absatz 2 Satz 1 Nummer 8) und durch eine Beschränkung der Datenschutzkontrolle auf die Verwaltungstätigkeit der Bürgerschaft (§23 Absatz 1 Satz 2) berücksichtigt worden. Der Umgang mit personenbezogenen Daten bei der Wahrnehmung parlamentarischer Aufgaben ist bereichsspezifisch in der Datenschutzordnung der Hamburgischen Bürgerschaft vom 19. Oktober 1999 (HmbGVBl. S. 243) geregelt.

Die Formulierung in Nummer 2 „und deren öffentlich-rechtlich organisierte Einrichtungen“ ist vorsorglich im Hinblick auf etwaige neue Entwicklungen im Bereich der Zusammenarbeit der genannten juristischen Personen des

öffentlichen Rechts gewählt worden. Satz 1 Nummer 3 stellt schließlich klar, dass Beliehene, denen die Wahrnehmung hoheitlicher Aufgaben der öffentlichen Verwaltung übertragen ist, insoweit öffentliche Stellen im Sinne des Gesetzes sind. Aus der Gesetzgebungsbefugnis Hamburgs ergibt sich, dass damit nur hamburgische Verwaltungsaufgaben gemeint sein können.

Früher kam es verschiedentlich zu Einordnungsproblemen bezüglich solcher juristischer Personen, Gesellschaften und anderer Personenvereinigungen des privaten Rechts, an denen die Freie und Hansestadt Hamburg oder eine ihrer Aufsicht unterstehende juristische Person des öffentlichen Rechts beteiligt ist. Diese Probleme beruhten darauf, dass im Gegensatz zum Bundesdatenschutzgesetz und zu den meisten Landesdatenschutzgesetzen in §2 Absatz 1 „deren Vereinigungen“ nicht ausdrücklich genannt sind; auch bei Einbeziehung des §4 Absatz 7 wurden nicht immer eindeutige Ergebnisse erzielt.

Satz 2 entscheidet diese Frage in der Weise, dass immer dann, wenn eine solche „Vereinigung“ privatrechtlich organisiert ist (z.B. Aktiengesellschaft, GmbH, eingetragener Verein), nur die auf nicht-öffentliche Stellen anzuwendenden Vorschriften des Bundesdatenschutzgesetzes gelten. Diese Lösung erspart im Einzelfall schwierige Abgrenzungsfragen. So besteht in der Literatur keinesfalls Einvernehmen über die Auslegung des Begriffs „Vereinigungen“ und damit über die wichtige Weichenstellung öffentliche/nicht-öffentliche Stelle. Zum Teil werden Vereine usw., an denen auch nicht-öffentliche Mitglieder beteiligt sind, als nicht-öffentliche Stellen bezeichnet, soweit nicht die Voraussetzungen des §2 Absatz 3 BDSG vorliegen. Andere beziehen die Bezeichnung „deren Vereinigungen“ nur auf die bundes- bzw. landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts; demnach wären Unternehmen, an denen das Land selbst beteiligt ist, keine Vereinigungen in diesem Sinn. Schwierig ist im Einzelfall auch die Bestimmung des Begriffs „Wahrnehmung von Aufgaben der öffentlichen Verwaltung“.

Um in der Gesetzesanwendung nicht erst im Einzelfall die unter Umständen schwierige Frage klären zu müssen, für welche Unternehmen mit hamburgischer Beteiligung das Hamburgische Datenschutzgesetz gilt, bestimmt Absatz 1 Satz 2, dass für alle Vereinigungen, die privatrechtlich organisiert sind, nur die Vorschriften des Bundesdatenschutzgesetzes für nicht-öffentliche Stellen anzuwenden sind. Im Ergebnis gilt demnach für alle privatrechtlich organisierten Unternehmen mit hamburgischer Beteiligung das gleiche Datenschutzrecht sowohl hinsichtlich der materiellen Regelungen als auch hinsichtlich der Datenschutzkontrolle; auf die im Einzelfall schwierige Grenzziehung zwischen öffentlicher und nicht-öffentlicher Stelle kommt es insoweit daher nicht an.

Die Aussage des Absatzes 1 Satz 2 stellt eine landesgesetzliche Regelung des Datenschutzes im Sinne von §1 Absatz 2 Nummer 2 und §12 Absatz 2 BDSG dar mit der Folge, dass für diejenigen privatrechtlich organisierten Vereinigungen, die §2 Absatz 2 BDSG als öffentliche Stellen des Landes bezeichnet, nicht die Vorschriften des Bundesdatenschutzgesetzes für öffentliche Stellen zur Anwendung kommen.

Sind an einer derartigen Vereinigung auch noch öffentliche Stellen eines anderen Landes oder mehrerer anderer Länder beteiligt, wird es bei der Frage, welchem der beteiligten Länder die Vereinigung rechtlich zuzuordnen ist, auf staatsvertragliche Regelungen oder – wenn solche nicht bestehen – auf den Sitz der Vereinigung ankommen. Dies ist auch anzunehmen, wenn mehrere Länder ohne den Bund an einer Vereinigung beteiligt sind.

Beteiligt sich eine Vereinigung des privaten Rechts im Sinne des Absatzes 1 Satz 2 an einer weiteren Vereinigung des privaten Rechts, ist ebenfalls von der Geltung des Absatzes 1 Satz 2 auszugehen.

Die Einschränkung am Ende des Absatzes 1 Satz 2 ist erforderlich, da §2 Absatz 3 Satz 2 BDSG bestimmte privatrechtlich organisierte Vereinigungen, an denen öffentliche Stellen des Bundes und der Länder beteiligt sind, als öffentliche Stellen des Bundes bezeichnet.

Wie bisher soll für öffentliche Stellen, die am Wettbewerb teilnehmen, gemäß Absatz 2 materiell im Wesentlichen das Bundesdatenschutzgesetz gelten. Die neu formulierte Vorschrift vermeidet indes die missverständliche Bezeichnung „öffentlich-rechtliche Unternehmen“; im Sinne einer eindeutigen Regelung wird hier – und in den nachfolgenden einschlägigen Vorschriften – ausdrücklich angegeben, dass es (nur) um die in Absatz 1 Satz 1 genannten Stellen geht.

Um auch die Vorschriften des Bundesdatenschutzgesetzes über betriebliche Datenschutzbeauftragte unzweifelhaft anwendbar zu machen, wird Bezug genommen auf die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes. Außerdem beschränkt die geänderte Vorschrift die Gleichstellung mit nicht-öffentlichen Stellen durch Verwendung des Wortes „soweit“ auf die Bereiche, in denen die Stellen im Wettbewerb stehen. Da sich die Datenschutzkontrolle aber auch bei diesen Stellen insgesamt nach dem Hamburgischen Datenschutzgesetz

richtet, wird §38 BDSG von der Verweisung ausgenommen.

Gemäß Absatz 3 gelten für öffentlich-rechtliche Kreditinstitute weiterhin nicht – auch nicht teilweise – die Vorschriften dieses Gesetzes, sondern allein diejenigen Vorschriften des Bundesdatenschutzgesetzes, die auf privatrechtliche Kreditinstitute anzuwenden sind. Die Rechtfertigung dieser Sonderregelung besteht bei der Hamburgischen Wohnungsbaukreditanstalt (WK) aber in den Bereichen nicht, in denen sie Verwaltungsaufgaben wahrnimmt, die ihr vom Senat aufgrund von §3 Absatz 4 des Gesetzes über die Hamburgische Wohnungsbaukreditanstalt übertragen worden sind und bei denen die WK dem Bürger wie eine Behörde gegen übertritt. Insoweit gilt für die WK das Hamburgische Datenschutzgesetz gemäß der Grundregelung des Absatzes 1 Satz 1.

Absatz 4 nimmt die Ausübung des Gnadenrechts wegen der Besonderheiten dieses Verfahrens nach wie vor aus dem Anwendungsbereich des Gesetzes aus.

Absatz 5 nimmt einen Anwendungsfall von Absatz 7 vorweg. Die Vorschrift nennt beispielhaft Bereiche, deren Eigenart von vornherein keine Prüfung zulässt, ob datenschutzrechtliche Lücken durch die Grundsatzregelungen des allgemeinen Gesetzes ausgefüllt werden können. Fachgesetze, deren Regelungen für den Umgang mit personenbezogenen Daten nicht mehr den heutigen Anforderungen genügen, müssen vom Gesetzgeber unter Berücksichtigung aller Besonderheiten des jeweiligen Bereichs geändert werden und können nicht durch das allgemeine Gesetz ergänzt werden, da es für die Lösung spezieller Konflikte nicht geeignet ist.

Gemäß Satz 1 finden die angegebenen Datenschutzvorschriften auf die dort genannten Stellen dann keine Anwendung, wenn es sich um eine nicht-automatisierte Datenverarbeitung außerhalb von Dateien handelt. Die üblichen Vorgangsakten, die im Hinblick auf die darin enthaltenen personenbezogenen Daten nicht strukturiert sind, fallen nicht unter den Dateibegriff.

Satz 2 stellt klar, dass die für die Gerichte geltende Bereichsausnahme nicht für Gerichtsvollzieherinnen und Gerichtsvollzieher gilt. Hiermit wird auch eine Harmonisierung mit §23 Absatz 1 Satz 2 erreicht. Der allgemeine Vorrang bereichsspezifischer Datenschutz- und Datenverarbeitungsregelungen gemäß §2 Absatz 7 gilt selbstverständlich auch für Gerichtsvollzieherinnen und Gerichtsvollzieher.

Absatz 6 berücksichtigt, dass für personenbezogene Daten, die in allgemein zugänglichen Quellen enthalten sind (wie z.B. in Zeitungen, Adress- und Telefonbüchern), oder für solche personenbezogenen Daten, die die Betroffenen selbst der Öffentlichkeit zugänglich gemacht haben, kein Schutzbedürfnis besteht. Dies gilt allerdings nur, solange die Daten in den allgemein zugänglichen Quellen enthalten sind. Sobald sie in nicht allgemein zugängliche Dateien oder Akten übernommen werden, finden die Vorschriften dieses Gesetzes Anwendung. Anders verhält es sich, wenn die Betroffenen ihr Selbstbestimmungsrecht dahingehend ausgeübt haben, dass sie ihre Daten zur Veröffentlichung bestimmt haben. Das Gesetz findet daher auch dann keine Anwendung, wenn diese Daten aus allgemein zugänglichen Quellen entnommen werden, um zum Beispiel ein Autorenverzeichnis zu erstellen.

Dies gilt allerdings nicht für unrichtige und unzulässige Veröffentlichungen durch Dritte, da die Daten in diesen Fällen nicht von den Betroffenen zur Veröffentlichung bestimmt worden sind. Wenn die Betroffenen jedoch die Veröffentlichung und damit die Zugänglichkeit für jedermann zugelassen haben, z.B. in Interviews, können sie sich nicht gegen eine aus ihrer Sicht zweckwidrige Verwendung der veröffentlichten Daten wenden, da die Veröffentlichung keine bestimmte Zweckbindung enthält.

Absatz 7 macht deutlich, dass es sich bei dem allgemeinen Hamburgischen Datenschutzgesetz um ein Auffanggesetz handelt, das gegenüber spezialgesetzlichen Regelungen subsidiär ist. Rechtsvorschriften sind auch Tarifvertragsnormen, die für allgemein verbindlich erklärt werden.

Dies gilt nicht nur für Bereiche, die in die Gesetzgebungskompetenz des Bundes fallen (z.B. Teil X des Sozialgesetzbuchs für den gesamten Bereich des Sozialrechts), sondern auch für die einzelnen Fachgesetze des Landes (z.B. Hamburgisches Meldegesetz). Nur soweit diese zum Umgang mit personenbezogenen Daten keine Regelungen enthalten, gilt das allgemeine Datenschutzgesetz. Enthalten sie lediglich unvollständige Regelungen, dann ist zu prüfen, ob deren Sinn und Zweck eine Ergänzung durch die Anwendung der allgemeinen Vorschriften zulässt. Dies entspricht der Auslegung bereits bestehender Subsidiaritätsregelungen in den Verwaltungsverfahrensgesetzen.

Durch die Verwendung des Eingangswortes „Soweit“ wird klargestellt, dass besondere Rechtsvorschriften, die sich auf die Verarbeitung personenbezogener Daten beziehen, nur in ihrem jeweiligen Regelungsumfang den Vorschriften des Hamburgischen Datenschutzgesetzes vorgehen.

Um zu vermeiden, dass der in Absatz 7 ausgesprochene Vorrang bereichsspezifischer Vorschriften zu eng ausgelegt wird, wird der Begriff der Rechtsvorschriften über den Datenschutz gesetzlich umfassend definiert. Der Klammerzusatz „(Rechtsvorschriften über den Datenschutz)“ macht es entbehrlich, entsprechende Umformulierungen an anderen Stellen des Gesetzes vorzunehmen, an denen dieser Begriff enthalten ist.

Zu §3 (Datenverarbeitung im Auftrag)

Der Anwendungsbereich der Vorschrift gemäß Absatz 1 Satz 1 ist entsprechend ihrem Zweck auf die technische Hilfeleistung beschränkt.

Bei der Verarbeitung personenbezogener Daten im Auftrage öffentlicher Stellen tragen diese letztlich die alleinige Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften; die auftraggebende Stelle ist Daten verarbeitende Stelle und zugleich Adressat der Rechte der Betroffenen. Ihr obliegen nach Satz 2 besondere Verpflichtungen bei der Auswahl der auftragnehmenden Stelle. Bei der Auftragsvergabe sind nach Satz 3 erforderlichenfalls zusätzliche Festlegungen zu treffen.

Satz 4 verlangt die Verpflichtung der auftragnehmenden Stellen auf strikte Zweckbindung und Rückgabe bzw. Löschung personenbezogener Daten nach Erledigung des Auftrags. Von besonderer Bedeutung ist die Regelung in den Fällen des Absatzes 4 Nummer 1. Da sie indes auch den Grundsätzen der herkömmlichen Datenverarbeitung im Auftrag entspricht, ist sie in Absatz 1 aufgenommen worden.

Absatz 2 Satz 3 entspricht §11 Absatz 3 Satz 2 BDSG; auch verschiedene Landesdatenschutzgesetze enthalten vergleichbare Bestimmungen. Die Vorschrift beruht auf der Überlegung, dass in der Praxis die auftragnehmende Stelle häufig bessere datenschutzrechtliche Kenntnisse hat als die auftraggebende Stelle. Sie statuiert allerdings keine Pflicht, jeden Auftrag sorgfältig auf seine Rechtmäßigkeit hin zu überprüfen.

Absatz 3 Satz 1 soll Missverständnissen vorbeugen. Das Hamburgische Datenschutzgesetz enthält in den §§7 bis 9 mehrmals Bestimmungen, die ausdrücklich für öffentliche Stellen „und ihre auftragnehmenden Stellen“ Regelungen enthalten. Diese Regelungen gelten aber nur für solche auftragnehmenden Stellen, die unter §2 Absatz 1 Satz 1 fallen und die zudem nicht durch §2 Absätze 2 und 3 von der Geltung der §§7 bis 9 freigestellt sind. Damit der Inhalt der genannten Regelungen auch für solche auftragnehmenden Stellen verbindlich wird, auf die diese Bestimmungen nicht schon kraft Gesetzes anwendbar sind, soll er durch vertragliche Regelung verbindlich gemacht werden.

Absatz 4 Nummer 1 regelt die Datenverarbeitung im Rahmen beratender, begutachtender und vergleichbarer unterstützender Tätigkeiten (z.B. Übernahme von Verfahrensvertretungen) für eine in §2 Absatz 1 Satz 1 genannte Stelle. Diese Tätigkeiten bewegen sich einerseits allenfalls im Randbereich der Auftragsdatenverarbeitung, da Beratern, Gutachtern und vergleichbar Tätigen wegen ihrer besonderen Sachkenntnis und der ihnen zur Erfüllung ihrer Aufgaben notwendigerweise einzuräumenden Entscheidungsspielräume die Verarbeitung personenbezogener Daten nach Art und Umfang nicht im Einzelnen vorgegeben werden kann. Andererseits fällt es häufig schwer, in diesen Fällen eine gesetzliche Übermittlungsbefugnis herzuleiten. Nummer 1 schließt diese Lücke.

Nummer 2 vermeidet die schwierige rechtliche Einordnung von Wartung und Fernwartung. Überwiegend wird die Auffassung vertreten, eine von einer außenstehenden Stelle durchgeführte Wartung sei keine Datenverarbeitung (im Auftrag), da die Verarbeitung der personenbezogenen Daten nicht Zweck der Wartung sei. Da es ferner nicht zum Zweck der Wartung gehöre, die Daten mit ihrem Informationsgehalt der Wartungsfirma zur Nutzung und weiteren Verarbeitung zu überlassen, stelle die sich als Nebenfolge ergebende Möglichkeit einer Kenntnisnahme personenbezogener Daten auch keine Datenübermittlung dar.

Gleiches gilt für externe Hilfstätigkeiten bei der Datenverarbeitung. Hierunter sind z.B. das Verteilen, das Vorbereiten zur Versendung oder das Transportieren von Datenträgern zu verstehen. Auch hier besteht ein vergleichbares Schutzbedürfnis. Durch die Einbeziehung dieser Hilfstätigkeiten werden Abgrenzungsprobleme zur „echten“ Datenverarbeitung vermieden.

Es besteht keine Notwendigkeit, diese schwierigen Fragen im Gesetz definitiv zu beantworten. Allerdings muss gewährleistet sein, dass sowohl von der datenverarbeitenden öffentlichen Stelle als auch von der mit Wartungsarbeiten oder Hilfstätigkeiten beauftragten Stelle Sicherheitsmaßnahmen zu treffen sind, die einen Datenmissbrauch ausschließen. Absatz 4 ordnet daher hierfür die entsprechende Geltung der Absätze 1 bis 3 an, soweit ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Die Auftragserledigung nach Absatz 4 setzt – ebenso wie die gesamte Auftragsdatenverarbeitung nach den Absätzen

1 bis 3 – bei Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, eine Befugnis zur Offenbarung der Daten voraus (siehe auch §203 StGB). Eine solche Befugnis ergibt sich nicht aus §3 selbst, sondern aus einer besonderen Einwilligung oder aus bereichsspezifischen Vorschriften oder auch aus einer Güterabwägung, wenn die auftraggebende Stelle zwingend auf die Unterstützung der auftragnehmenden Stelle angewiesen ist. In diesen Fällen ist die Auftragserteilung nur zulässig, wenn der Datenschutz bei der auftragnehmenden Stelle nach der Art der zu verarbeitenden Daten den Anforderungen genügt, die für die auftraggebende Stelle zur Wahrung des Berufs- oder besonderen Amtsgeheimnisses gelten.

Zu §4 (Begriffsbestimmungen)

Die Vorschrift enthält aus Gründen der Übersichtlichkeit alle für das Datenschutzgesetz wesentlichen Begriffsbestimmungen.

Absatz 1 geht vom Begriff der Einzelangabe aus. Damit sind alle Angaben über persönliche und sachliche Verhältnisse gemeint, die über eine lebende natürliche Person etwas aussagen, unabhängig davon, in welcher technischen Form (z.B. Bildaufnahme) dies geschieht. Der Begriff hält die Einbeziehung neuer technischer Verfahren in das Gesetz offen. Bestimmbar ist eine Person auch dann, wenn nur unter Verwendung eines Zusatzwissens der Personenbezug hergestellt werden kann, aber immer nur für diejenige Stelle, die selbst über das erforderliche Zusatzwissen verfügt oder verfügen kann.

Absatz 2 bezieht sieben Phasen (Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen, Nutzen) in den Datenverarbeitungsbegriff ein. Nach wie vor kommt der Legaldefinition einzelner Verarbeitungsphasen Bedeutung zu, weil nicht darauf verzichtet werden kann, für sie im Gesetz besondere Zulässigkeitsanforderungen vorzugeben. Um für den Umgang mit personenbezogenen Daten keine Regelungslücke offen zu lassen, wird in Satz 1 auch das (sonstige) Nutzen personenbezogener Daten im Sinne jedweder Verwendung als besondere Phase definiert und den übrigen Phasen gleichgestellt. Auch das Bundesverfassungsgericht bindet das Recht auf informationelle Selbstbestimmung nicht an bestimmte Phasen der Datenverarbeitung, sondern spricht allgemein von der Verwendung personenbezogener Daten.

Absatz 2 Satz 1 definiert die Phasen der Datenverarbeitung in Übereinstimmung mit dem Regelungszustand in anderen Ländern und – bei etwas abweichender Diktion – dem Bund.

Absatz 2 Satz 2 Nummer 1 definiert die Datenverarbeitungsphase der Erhebung. Der Begriff umfasst nicht die zufällig erlangten oder aufgedrängten Informationen, für die aber Regelungen über die Zweckbindung gelten (vgl. §13 Absatz 1 Satz 2). Das Erheben setzt nach allgemeiner Auffassung ein finales, zielgerichtetes Beschaffen personenbezogener Daten voraus. Hierzu gehört der „schweifende Blick“ des Streifenbeamten ebenso wenig wie die nicht auf personenbezogene Informationsbeschaffung abzielende Unterhaltung eines Verwaltungsbediensteten mit einem Bürger, selbst wenn dabei personenbezogene Zusammenhänge wahrgenommen werden. Auch Beobachtungen für Lagebeurteilungen der Polizei, bei denen keine zielgerichtete Identifizierung von Personen erfolgt, stellen kein Erheben dar. Zum anderen werden Probleme, die sich aus der Geltung des Gesetzes bei der Datenerhebung über Personenkreise ergeben können, durch den neuen §12 Absatz 2 Satz 2 gelöst, der in notwendigem Zusammenhang mit dem gegenüber früherem Recht erweiterten Begriff der Erhebung zu sehen ist.

Das Gesetz geht verfassungskonform in erster Linie vom Beschaffen personenbezogener Daten bei Betroffenen selbst aus, muss jedoch bei der Unterschiedlichkeit der Aufgabenstellung auch andere Formen der Informationsbeschaffung mit einbeziehen. Die der öffentlichen Stelle zugewiesene Tätigkeit kann es erforderlich machen, Informationen bei anderen Stellen oder Personen zu beschaffen. Das Erheben umfasst folglich jede Form gezielt betriebener Gewinnung personenbezogener Daten unter Mitwirkung Betroffener, anderer öffentlicher Stellen oder privater Dritter sowie durch zweckgerichtete Beobachtung.

In Absatz 2 Satz 2 Nummer 4 umfasst der Übermittlungsbegriff auch solche Daten, die noch nicht auf einem Datenträger (vgl. §4 Absatz 8) erfasst sind, sondern sich (zunächst) nur „im Kopf“ einer oder eines Bediensteten einer in §2 Absatz 1 Satz 1 genannten Stelle befinden.

Mit den Wörtern „zur Einsicht bereitgehalten“ in Absatz 2 Satz 2 Nummer 4 wird ein weiterer Bereich des Übermittelns erfasst. Dies ist sachgerecht, da beispielsweise im Planfeststellungsverfahren der Plan für eine bestimmte Dauer zur Einsicht auszulegen ist (vgl. §73 Absatz 3 Satz 1 HmbVwVfG) und die Behörden im Verwaltungsverfahren den Vorschriften des Hamburgischen Datenschutzgesetzes unterliegen, soweit sie personenbezogene Daten verarbeiten (§3a HmbVwVfG).

Auch das Veröffentlichen von Daten, das keinen von vornherein klar bestimmten Adressatenkreis hat, gehört zum Begriff des Übermittelns. Das Bundesverfassungsgericht hat in einem Beschluss vom 24. Juli 1990 (NVwZ 1990, 1162) ausgeführt, die öffentliche Bekanntmachung (eine besondere Form der Veröffentlichung) personenbezogener Daten stelle die „intensivste Form einer Übermittlung personenbezogener Daten“ dar.

In Absatz 2 Satz 2 Nummer 5 wird auch das Sperren als zusätzliche Datenverarbeitungsphase definiert; es bedarf nicht der ausdrücklichen Erwähnung im Gesetz, dass das Löschen als die regelmäßig dem Interesse der Betroffenen dienende und noch stärker wirkende Maßnahme ggf. möglich bleibt. Nummer 6 berücksichtigt, dass das Vernichten eine häufige Form des Löschens z.B. bei der Datenverarbeitung in Akten ist. In Nummer 7 wird jede Verwendung von Daten als das Nutzen von Daten definiert und den sonstigen Datenverarbeitungsphasen gleichgestellt. Sofern eine Stelle Daten aber lediglich auswertet, um das Ergebnis anonymisiert einer anderen Stelle für deren Zwecke zur Verfügung zu stellen, liegt keine Verwendung personenbezogener Daten vor.

Absatz 3 verwendet den Begriff der „Daten verarbeitenden“ Stelle, da es auf das Kriterium der Speicherung für die Anwendung des Gesetzes nicht wesentlich ankommt. Der Daten verarbeitenden Stelle entspricht der Begriff des „für die Verarbeitung Verantwortlichen“ im Sinne von Artikel 2 Buchstabe d der EG-Datenschutzrichtlinie. Die Formulierung „allein oder gemeinsam mit anderen“ stellt klar, dass im Fall verteilter Datenverarbeitung jede beteiligte Stelle als Daten verarbeitende Stelle gilt. Besondere Vorschriften über die datenschutzrechtliche Verantwortung, z.B. nach §11a Absatz 1 Satz 4, bleiben hiervon allerdings unberührt.

In Absatz 4 wird der Begriff der Dritten in Übereinstimmung mit Artikel 2 Buchstabe f der EG-Datenschutzrichtlinie definiert. Mit den Worten „Mitgliedstaaten der Europäischen Union“ wird die Anordnung des Artikels 1 Absatz 2 der EG-Datenschutzrichtlinie vollzogen, wonach die Mitgliedstaaten den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten nicht unter Berufung auf Gründe des Datenschutzes beschränken oder untersagen dürfen.

Diejenigen Untergliederungen einer Stelle, die bloße Hilfstätigkeiten für die von der Stelle zu erfüllenden Aufgaben erbringen (z.B. zentrale Schreibdienste, Hausdruckerei), sind mangels eigenen Aufgabenbereichs keine Dritten.

Absatz 5 definiert den auch von der EG-Datenschutzrichtlinie verwendeten Begriff der Empfängerinnen und Empfänger. Zu den Empfängerinnen und Empfängern zählen neben den (dritten) Stellen, denen Daten übermittelt werden (bisherige „empfangende Stellen“), auch Auftragsdatenverarbeiter sowie innerhalb einer Daten verarbeitenden Stelle solche Daten empfangenden Untergliederungen, die andere Aufgaben wahrnehmen als diejenigen Untergliederungen, von denen sie die Daten erhalten.

Absatz 6 enthält eine vereinfachte Definition des Dateibegriffs. Die Definition hat nur geringe Bedeutung, da die Anwendbarkeit des Gesetzes nicht an den Dateibegriff anknüpft. Der Dateibegriff bedarf aber der Legaldefinition zur Abgrenzung von der konventionellen Datenverarbeitung in und aus Akten, für die einige Sonderregelungen gelten müssen. Unterschieden wird zwischen automatisierter und nicht-automatisierter Verarbeitung, an die teilweise auch unterschiedliche Rechtsfolgen anknüpfen: Grundsätzlich fallen alle Sammlungen von personenbezogenen Daten, die unabhängig von der Art der Speicherung durch automatisierte Verfahren verarbeitet werden können, unter den Dateibegriff (automatisierte Datei).

Es wird nicht gefordert, dass solche Datensammlungen gleichartig aufgebaut sein müssen. Zu einer automatisierten Datei zählen aber weder Fernkopierer, da sie keine Datensammlung enthalten, noch Schreibautomaten, soweit mit ihnen keine Daten automatisiert verarbeitet werden können. Dadurch sind solche Verfahren, die auf Grund ihrer Verwendungsmöglichkeiten und ihrer Zweckbestimmung zu keiner Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung führen können, von der Anwendung des Gesetzes ausgenommen, ohne dass es dazu einer ausdrücklichen Regelung bedarf.

Dem verarbeitungstechnisch geprägten Dateibegriff werden diejenigen nicht-automatisierten Datensammlungen gleichgestellt, die gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können (nicht-automatisierte Datei). Dieser Dateibegriff ist damit gegenüber der sonstigen nicht-automatisierten Datenverarbeitung, der konventionellen oder manuellen Verarbeitung in Akten, abgegrenzt, ohne dass der Begriff der Akte im Gesetz definiert wird. Die allein maßgeblichen materiellen Kriterien der Datenzugänglichkeit und Datenauswertung (oder die Möglichkeit dazu) verdeutlichen, dass auf das besondere Gefährdungspotential solcher gleichartig aufgebauter Datensammlungen abgestellt wird.

Die Definition in Absatz 6 entspricht den Erfordernissen des Artikels 2 Buchstabe c der EG-Datenschutzrichtlinie. Danach ist eine Datei jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. In Erwägungsgrund 27 der Richtlinie wird ausgeführt, dass Akten und Aktensammlungen sowie ihre

Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, nicht in den Anwendungsbereich der Richtlinie fallen. Dies bedeutet im Umkehrschluss, dass – im Hinblick auf die in ihnen enthaltenen personenbezogenen Daten – „strukturierte“ Akten und Aktensammlungen durchaus unter den Dateibegriff fallen können. Eine strukturierte Aktensammlung liegt dann vor, wenn z.B. die zu einer Person geführte Akte in einer Hängeregistratur abgelegt wird, deren Ordnung an die alphabetische Reihenfolge der Namen anknüpft.

In den Anwendungsbereich des Gesetzes werden grundsätzlich auch diejenigen nicht-automatisierten Dateien einbezogen, aus denen keine personenbezogenen Daten übermittelt werden sollen (sog. interne Karteien), weil bereits Erhebung und Speicherung solcher Daten Eingriffe in das Grundrecht auf informationelle Selbstbestimmung darstellen können, selbst wenn (ursprünglich) keine Übermittlung beabsichtigt ist. Auch Daten, die nur zum internen Gebrauch gespeichert werden, können Grundlage für Entscheidungen sein, die die Betroffenen belasten.

Absatz 7 ermöglicht es, den Gesetzeswortlaut dort kürzer zu fassen, wo alle in Betracht kommenden Personen, Behörden (vgl. die Erläuterung zu §2 Absatz 1 Satz 1) oder sonstige verselbständigte Handlungseinheiten erfasst werden sollen.

In Absatz 9 ist die Definition des Anonymisierens enthalten, die für die §§27 und 30 sowie für Sonderregelungen in bereichsspezifischen Gesetzen Bedeutung hat, falls dort nicht eine andere – nach §2 Absatz 7 vorrangige – Regelung getroffen wurde. Die Definition stellt klar, dass personenbezogene Daten nicht nur dann anonymisiert sind, wenn ein Personenbezug überhaupt nicht mehr herstellbar ist, sondern auch dann, wenn die Zuordnung nur noch mit unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft möglich wäre (faktische Anonymisierung).

Absatz 10 enthält im Anschluss an die Definition des Anonymisierens in Absatz 9 auch eine Definition des Pseudonymisierens. Pseudonymisieren ist das Verändern identifizierbarer, direkt personenbezogener Daten durch Verwendung einer Zuordnungsregel derart, dass die Einzelangaben – mit einem verhältnismäßigen Aufwand – nur in Kenntnis dieser Regel einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden kann. An die Stelle identifizierbarer Daten tritt ein Pseudonym, dass es ermöglicht, personenbezogene Daten ohne Kenntnis der Identität des Betroffenen zu nutzen.

Pseudonyme können unterschiedlich gestaltet werden: Selbst generierte Pseudonyme werden ausschließlich vom Betroffenen vergeben und nicht mit dessen Identitätsdaten gleichzeitig verwendet oder gespeichert. Damit kann gewährleistet werden, dass die unter Pseudonym gespeicherten Daten nur durch den Betroffenen selbst diesem wieder zugeordnet werden können. Bei Referenz-Pseudonymen kann die Zuordnung zu dem Träger des Pseudonyms über entsprechende Referenzlisten erfolgen. Ohne Verwendung entsprechender Listen ist die Identität des Betroffenen jedoch nicht zu ermitteln. Einweg-Pseudonyme zeichnen sich dadurch aus, dass sie mittels Einweg-Funktionen aus personenbezogenen Identitätsdaten gebildet werden. Die Auflösung von Einweg-Pseudonymen setzt die Kenntnis der bei der Pseudonymisierung verwendeten Identitätsdaten des Betroffenen und der Zuordnungsfunktionen voraus.

Zu §4a (Schriftform)

Überholt durch Aufhebung der Vorschrift

Zu §5 (Zulässigkeit der Datenverarbeitung)

Absatz 1 enthält die allgemeinen Zulässigkeitsvoraussetzungen einer jeden Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung. Es werden nicht nur einzelne, sondern alle Phasen der Verarbeitung unter Schutz gestellt.

In Satz 1 soll mit dem Wort „soweit“ verdeutlicht werden, dass eine Datenverarbeitung nur in dem Umfange zulässig ist, den die gesetzliche Grundlage oder die Einwilligung vorgibt.

Die Sätze 2 und 3 setzen die Bestimmungen des Artikels 8 der EG-Datenschutzrichtlinie über die Verarbeitung besonderer Kategorien personenbezogener Daten (sogenannte sensitive Daten) um. Die Richtlinienbestimmung wird in der Literatur als „zu den problematischsten Elementen der Richtlinie“ gehörig bezeichnet (vgl. Simitis, EG-Datenschutzrichtlinie, Kommentar, 1997, Artikel 8 Rdnr. 3 m.w.N.). Da sie eindimensional nur an – zudem nur ganz bestimmte – Dateninhalte anknüpfe und den Verarbeitungskontext außer Acht lasse, laufe sie Gefahr, zugleich übermäßig und defizitär zu wirken. Aufgrund der Richtlinienvorgabe war die Vorschrift jedoch ungeachtet möglicher Probleme, die ihre Anwendung nach sich ziehen kann, zwingend in das Hamburgische Datenschutzgesetz aufzunehmen. Mit Schwierigkeiten ist insbesondere in Fällen zu rechnen, in denen Betroffene selbst der Verwaltung Daten der genannten Art offenbaren, ohne dass eine besondere Rechtsvorschrift die Datenverarbeitung zulässt. Zu denken ist etwa an Eingaben, in denen Petenten ihre politischen Anschauungen oder gesundheitlichen Verhältnisse kundtun. Um die mit der Anwendung der Regelung verbundenen Probleme in Grenzen zu halten, sind die besonderen Voraussetzungen für die Verarbeitung sensitiver Daten entsprechend dem Anwendungsbereich der EG-Datenschutzrichtlinie beschränkt worden.

Satz 2 regelt die Verarbeitungsbefugnisse nach Maßgabe der Richtlinienbestimmungen.

Nummer 1 verweist auf anderweitige besondere Vorschriften über den Datenschutz und beruht auf Artikel 8 Absatz 4 der EG-Datenschutzrichtlinie. Soweit bereichsspezifische Vorschriften wie z.B. Regelungen zur Kirchensteuererhebung oder die im Hamburgischen Gesetz über die Datenverarbeitung der Polizei, im Hamburgischen Verfassungsschutzgesetz oder im Hamburgischen Sicherheitsüberprüfungsgesetz enthaltenen Befugnisnormen eine Verarbeitung auch der sensitiven Daten im Sinne des Artikels 8 der EG-Datenschutzrichtlinie voraussetzen, stellen sie besondere Rechtsvorschriften im Sinne der Nummer 1 dar. Dasselbe gilt im Hinblick auf die Verarbeitungsbefugnisse des Rechnungshofs aus der Landeshaushaltsordnung. Die dort enthaltenen Vorlage- und Auskunftspflichten bedeuten auch, dass der Rechnungshof die übermittelten Daten zur Erfüllung seiner Aufgaben weiterverarbeiten darf.

Nach Nummer 2 ist die Verarbeitung sensitiver Daten in Übereinstimmung mit Artikel 8 Absatz 2 Buchstabe a der EG-Datenschutzrichtlinie mit Einwilligung der Betroffenen zulässig. Die Einwilligung muss ausdrücklich erfolgen und sich auf diese Daten beziehen.

Nummer 3 macht von der Verarbeitungsmöglichkeit des Artikels 8 Absatz 2 Buchstabe e 1. Alternative der EG-Datenschutzrichtlinie Gebrauch. Daten, die von den Betroffenen selbst offensichtlich öffentlich gemacht wurden, verlangen keinen besonderen Schutz mehr.

Nummer 4 beruht auf Artikel 8 Absatz 2 Buchstabe c der EG-Datenschutzrichtlinie und nimmt Bezug auf

lebenswichtige Individualinteressen.

Nummer 5 beruht auf Artikel 8 Absatz 2 Buchstabe e 2. Alternative der EG-Datenschutzrichtlinie.

Nummer 6 beruht auf Artikel 8 Absatz 4 der EG-Datenschutzrichtlinie.

Nummer 7 setzt Artikel 8 Absatz 3 der EG-Datenschutzrichtlinie um. Wie die Nummern 3 bis 6 kommt auch sie nur zur Anwendung, soweit keine bereichsspezifischen Vorschriften die Verarbeitungsbefugnis regeln.

Satz 3 schließt anknüpfend an den beschränkten Geltungsbereich der EG-Datenschutzrichtlinie (Artikel 3) die Datenverarbeitung zur Wahrnehmung von Gefahrenabwehr- und Strafverfolgungsaufgaben sowie die nicht-automatisierte Verarbeitung außerhalb von Dateien von der Anwendung des Satzes 2 aus. Damit bleibt es insbesondere auch in den eingangs genannten Fällen möglich, sensitive Daten in nicht weiter strukturierten Vorgangsakten zu führen, so dass den Anforderungen einer ordnungsgemäßen Verwaltung in jedem Fall genügt werden kann. Die Aussage des Satzes 3, dass Satz 2 in den genannten Fällen „nicht gelte“, führt im Übrigen nicht dazu, dass die Verarbeitung sensitiver Daten in diesen Fällen stets zulässig wäre. Vielmehr bleibt es aufgrund der Nichtgeltung des Satzes 2 bei den allgemeinen Voraussetzungen für die Zulässigkeit der Datenverarbeitung nach §5 Absatz 1 Satz 1. Auch die schon bisher aus grundrechtlichen Erwägungen herzuleitende Forderung, dass bestimmte Datenverarbeitungen aufgrund ihrer Sensitivität in jedem Falle einer bereichsspezifischen Grundlage bedürfen, bleibt unberührt.

Das Anhörungserfordernis nach Satz 4 stellt die angemessene Garantie nach Artikel 8 Absatz 4 der EG-Datenschutzrichtlinie dar. Vor einer ausnahmsweisen Datenverarbeitung zur Abwehr erheblicher Nachteile für das Gemeinwohl besteht auf diese Weise eine zusätzliche Sicherungsvorkehrung.

Absatz 2 Satz 1 bestimmt, dass Einwilligungen regelmäßig schriftlich zu erteilen sind. Für elektronische Einwilligungen ist §4a zu beachten.

Satz 2 legt der öffentlichen Verwaltung verstärkte Aufklärungspflichten auf, verbessert dadurch den Schutz der Betroffenen bei freiwilligen Angaben und entspricht damit dem Anliegen des Rechts auf informationelle Selbstbestimmung. Die Ergänzung zum Widerruf einer Einwilligung soll klarstellen, dass eine Rückwirkung und Rückabwicklung erfolgter Datenverarbeitungen nicht in Betracht kommt.

In Satz 3 ist die Abgabe der Einwilligungserklärung bei Zusammenfassung mehrerer Erklärungen geregelt. Im Interesse einer verwaltungsökonomischen Handhabung ist bei zusammengefassten Erklärungen kein besonderer schriftlicher Hinweis, sondern eine Hervorhebung der Einwilligungserklärung erforderlich, aber auch ausreichend.

Satz 4 erklärt die Einwilligung für unwirksam, wenn sie fehlerhaft erlangt wurde.

Absatz 3 setzt Artikel 14 Buchstabe a der EG-Datenschutzrichtlinie über den „Widerspruch der betroffenen Person“ um. Der Begriff des Widerspruchs wird allerdings vermieden und durch den des Einwandes ersetzt, um Verwechslungen mit dem verwaltungsprozessualen Widerspruch zu vermeiden. Der Einwand richtet sich nicht wie der Widerspruch gegen rechtswidriges oder unzweckmäßiges Verwaltungshandeln, sondern gibt den Betroffenen Gelegenheit, besondere persönliche Gründe geltend zu machen, die gegen die an sich recht- und zweckmäßige Verarbeitung ihrer Daten oder eine bestimmte Art und Weise der Verarbeitung sprechen mögen.

Vom Einwendungsrecht ausgenommen werden in Satz 2 die Fälle, in denen die Datenverarbeitung auf einer Einwilligung der Betroffenen beruht oder zur Erfüllung rechtlicher Verpflichtungen der Daten verarbeitenden Stelle erforderlich ist. Rechtlich stützt sich diese Einschränkung darauf, dass Artikel 14 Buchstabe a der EG-Datenschutzrichtlinie zwar auf Artikel 7 Buchstaben e und f, nicht aber auf die Buchstaben a und c verweist. Der Sache nach ist das Einwendungsrecht in Einwilligungsfällen (Nummer 1) verzichtbar, weil den Betroffenen bereits das Recht zusteht, ihre Einwilligung für die Zukunft – ganz oder teilweise – zu widerrufen (§5 Absatz 2 Satz 2 2. Halbsatz). Sind sie der Auffassung, dass einer Datenverarbeitung besondere persönliche Gründe entgegenstehen, so ist ihnen zuzumuten, ihre Einwilligung zu verweigern oder von ihrem Widerrufsrecht Gebrauch zu machen, anstatt durch das Vorbringen persönlicher Gründe gegen die Datenverarbeitung eine unter Umständen aufwendige Prüfung seitens der Verwaltung in Gang zu setzen. In den Fällen, in denen die Datenverarbeitung erforderlich ist, um einer bestehenden rechtlichen Verpflichtung der Daten verarbeitende Stelle nachzukommen (Nummer 2), ist ebenfalls kein Raum für das Einwendungsrecht, da es gegebenenfalls ein rechtswidriges Verhalten der Daten verarbeitenden Stelle erzwingen würde.

Werden Einwände außerhalb der Ausnahmen nach Satz 2 erhoben, ist die Daten verarbeitende Stelle gehalten zu

prüfen, ob die geltend gemachten Gründe dem öffentlichen Interesse an der Verarbeitung vorgehen. Fällt die Abwägung zugunsten der vorgebrachten persönlichen Gründe aus, so ist die weitere Datenverarbeitung unzulässig. Möglich ist auch ein Teilerfolg in dem Sinne, dass nur eine bestimmte Modalität oder Phase der Datenverarbeitung unzulässig wird. Insgesamt werden die Anwendungsfälle der Vorschrift voraussichtlich gering bleiben.

Die Daten verarbeitenden Stellen haben Übermittlungen personenbezogener Daten in jedem Einzelfall zuverlässig zu dokumentieren, soweit dies erforderlich ist, um den Betroffenen Auskunft über die Empfängerinnen oder Empfänger zu erteilen und um die Empfängerinnen oder Empfänger von der Tatsache, dass dem Einwand der Betroffenen entsprochen wurde, sowie von der Benachrichtigung, Sperrung und Löschung personenbezogener Daten unverzüglich verständigen zu können.

Im Falle eines erfolgreichen Einwandes sind unverzüglich auch die Stellen zu verständigen, denen die Daten übermittelt worden sind. Diese „Nachberichtspflicht“ ist an die entsprechende Verpflichtung aus §19 Absatz 5 angelehnt. Sie entfällt, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Letzteres wird insbesondere dann der Fall sein, wenn die Datenempfänger die Daten zwar weiterverarbeiten, dabei aber eine besondere Modalität der Datenverarbeitung, gegen die sich der Einwand (nur) richtete, ersichtlich keine Rolle spielt.

Wird dem Einwand nicht entsprochen, so sind die Betroffenen wie im Falle der verweigerten Auskunft (§18 Absatz 6) auf die Möglichkeit hinzuweisen, sich an die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten zu wenden. Die Erhebung eines verwaltungsprozessualen Widerspruchs gegen den ablehnenden Bescheid bleibt hiervon unberührt.

Im Übrigen gilt das Einwendungsrecht nur im Anwendungsbereich des Hamburgischen Datenschutzgesetzes. Nach Artikel 14 Buchstabe a der EG-Datenschutzrichtlinie besteht es auch im Anwendungsbereich der Richtlinie nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung. Wann eine bereichsspezifische Datenverarbeitungsvorschrift, die kein Einwendungsrecht vorsieht, in dem Sinne abschließend ist, dass sie dieses Recht ausschließt, also für eine ergänzende Anwendung des Hamburgischen Datenschutzgesetzes keinen Raum lässt, muss die Auslegung der jeweiligen bereichsspezifischen Vorschrift selbst ergeben.

In Absatz 4 wird der Grundsatz des Datenschutzes durch Datenvermeidung ausdrücklich geregelt. Das Bundesverfassungsgericht hat bereits im Volkszählungsurteil – bezogen auf den dort in Rede stehenden Sachbereich – erwähnt, dass schon bei der Erhebung personenbezogener Angaben zu prüfen ist, „ob das Ziel der Erhebung nicht auch durch eine anonymisierte Ermittlung erreicht werden kann“, und dass außerdem das Gebot einer möglichst frühzeitigen (faktischen) Anonymisierung, verbunden mit Vorkehrungen gegen eine Deanonymisierung“ zu beachten ist (BVerfGE 65, 1, 48 f.).

Bei der gesamten Datenverarbeitung ist demnach darauf zu achten, dass möglichst keine oder nur wenige personenbezogene Daten verwendet werden. Bei der Ausgestaltung der Datenverarbeitungsverfahren einschließlich der Auswahl und Gestaltung technischer Einrichtungen ist diese Zielsetzung zu berücksichtigen. Dies kann insbesondere durch anonyme oder pseudonyme Verarbeitung erreicht werden.

Die anonyme Verarbeitung umfasst einerseits die Anonymität von Anfang an, z.B. durch Angaben nur über eine bestimmte Gruppe, die statistisch erfasst werden soll, ohne Merkmale mit Bezug auf einzelne Personen (so BVerfGE a.a.O.); dazu gehört andererseits bei zunächst personenbezogen ermittelten Daten, dass eine möglichst frühzeitige (faktische) Anonymisierung gemäß der Begriffsbestimmung im neuen §4 Absatz 9 geprüft wird und dabei eine Deanonymisierung verhindert wird (siehe BVerfGE a.a.O.). Eine pseudonyme Datenverarbeitung führt zwar nicht dazu, dass der Personenbezug ganz vermieden wird; daher bleiben die Daten personenbezogen. Die identifizierten Angaben, die der datenverarbeitenden Stelle ohne weiteres zugänglich sind (z.B. Name, Anschrift, Aktenzeichen) werden hierbei aber durch andere Namen und Bezeichnungen oder durch eine individuelle Zeichenfolge ersetzt, die aus sich heraus die Bestimmung der jeweiligen Person nicht ermöglicht oder nur in einem besonders gesicherten Verfahren für besondere Zwecke oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft.

Zu §5a (Automatisierte Einzelentscheidungen)

Der neue §5a setzt Artikel 15 der EG-Datenschutzrichtlinie um. Dies geschieht in einer gesonderten Vorschrift, die nur locker an die Vorschriften über die Zulässigkeit der Datenverarbeitung anknüpft, weil sie sich gerade nicht mit der Zulässigkeit einer bestimmten Datenverarbeitung befasst, sondern mit der Befugnis, Rechtsfolgen an eine bestimmte

Art der Datenverarbeitung zu knüpfen.

Absatz 1 beruht auf dem Grundgedanken, dass Entscheidungen, die auf einer Bewertung der Persönlichkeit der Betroffenen beruhen und damit ihr Persönlichkeitsrecht im Kern berühren, nicht allein einem technischen System überlassen werden sollen, sondern letztlich von einem Menschen verantwortet werden müssen.

Absatz 2 macht von den Ausnahmemöglichkeiten des Artikels 15 Absatz 2 der EG-Datenschutzrichtlinie Gebrauch.

Nummer 1 enthält lediglich einen klarstellenden deklaratorischen Verweis auf die Möglichkeit abweichender bereichsspezifischer Vorschriften.

Nummern 2 und 3 greifen die Ausnahmemöglichkeiten des Artikels 15 Absatz 2 Buchstabe a der EG-Datenschutzrichtlinie auf. Die erneute Prüfung unter Berücksichtigung der Stellungnahme der oder des Betroffenen (Nummer 3 3. Halbsatz) darf nicht ausschließlich automatisiert erfolgen.

Zu §5b (Mobile Datenverarbeitungsmedien)

Der neue §5b regelt Pflichten, die die ausgebenden Stellen im Zusammenhang mit der Herausgabe von Chipkarten und vergleichbaren mobilen Datenverarbeitungsmedien treffen. Die Datenverarbeitungsvorgänge, die mit Hilfe solcher Datenverarbeitungsmedien ablaufen, lassen sich zwar mit den geltenden Vorschriften über die Zulässigkeit der Verarbeitung personenbezogener Daten und die Modalitäten der zulässigen Datenverarbeitung bewältigen. Die Herausgabe mobiler Datenverarbeitungsmedien ist aber mit dem besonderen Risiko verbunden, dass sie einerseits, insbesondere auch im Falle kontaktloser Chipkarten, für die Betroffenen nicht ohne weiteres erkennbare Datenverarbeitungsvorgänge ermöglichen und den Betroffenen andererseits oftmals nicht deutlich ist, wo und in welcher Weise sie die ihnen auch in Bezug auf die Datenverarbeitungsmedien zustehenden datenschutzrechtlichen Rechte geltend machen können. Die Vorschrift beugt diesen Gefahren vor, indem sie die ausgebende Stelle verpflichtet sicherzustellen, dass die Betroffenen Datenverarbeitungsvorgänge erkennen und ihre datenschutzrechtlichen Rechte geltend machen können.

Für die Erkennbarkeit des Datenaustauschs genügt es, wenn jeweils erkannt werden kann, dass überhaupt ein Datenaustausch stattfindet. Die Sicherstellungspflicht überlässt es der ausgebenden Stelle, inwieweit sie selbst für die Verwirklichung der Betroffenenrechte sorgt oder sicherstellt, dass andere Stellen dies übernehmen. Die Betroffenen sind bei der Ausgabe der Datenverarbeitungsmedien entsprechend aufzuklären.

Zu §6 (Rechte der Betroffenen)

In Absatz 1 werden die Rechte der Betroffenen in einer vollständigen Aufzählung zusammengefasst, so dass die Betroffenen über ihre an verschiedenen Stellen im Gesetz geregelten einzelnen Rechte besser informiert werden. Die Voraussetzungen, unter denen die aufgeführten Rechte wahrgenommen werden können, ergeben sich aus den jeweils angegebenen Einzelvorschriften.

Gemäß Absatz 2 ist ein vorheriger Verzicht rechtlich nicht wirksam.

Zu §7 (Datengeheimnis)

Während die bei der Datenverarbeitung beschäftigten Personen im nicht-öffentlichen Bereich ausdrücklich auf das Datengeheimnis verpflichtet werden müssen, unterliegen die Personen, die im öffentlichen Bereich dienstlichen oder sonst berechtigten Zugang zu personenbezogenen Daten haben, materiell dem Datengeheimnis, ohne dass es eines besonderen Verpflichtungsakts bedarf. Durch das Wort „insbesondere“ wird verdeutlicht, dass auch das Bekanntgeben und Zugänglichmachen Unterformen des Verarbeitens sind.

Zu §8 (Technische und organisatorische Maßnahmen; Vorabkontrolle)

Jede Verwendung personenbezogener Daten durch öffentliche Stellen im Rahmen der Selbst- oder der Auftragsdatenverarbeitung erfordert technische und organisatorische Maßnahmen, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten (Absatz 1 Satz 1). Dabei gilt der Grundsatz der Zweck-Mittelrelation (Satz 2), sowohl bei der automatisierten (Absatz 2) als auch bei der nicht-automatisierten Datenverarbeitung (Absatz 3). Aufgrund der unterschiedlichen Verarbeitungsbedingungen werden jedoch für die automatisierte und nicht-automatisierte Datenverarbeitung differenzierte Maßnahmen vorgeschrieben.

Die bei automatisierter Verarbeitung zu treffenden Maßnahmen haben sich an fünf übergeordneten Sicherungszielen

zu orientieren, die im Wesentlichen selbsterklärend sind (Absatz 2 Nummern 1 bis 5):

– Das Sicherungsziel der Vertraulichkeit verlangt, dass kein unbefugter Informationsgewinn stattfinden kann;
– Integrität bedeutet, dass keine nicht beabsichtigten Veränderungen der Daten herbeigeführt werden können;
– Verfügbarkeit verlangt, dass die Daten und damit das Datenverarbeitungssystem zu den vorgegebenen Zeiten in erforderlichem Maß zur Verfügung steht;
– Authentizität ist gegeben, wenn die Urheberschaft der Daten sicher festgestellt werden kann;
– Revisionsfähigkeit verlangt die Nachvollziehbarkeit der Datenverarbeitung. Hierzu gehört auch die Dokumentation der Verarbeitungsverfahren, soweit sie erforderlich ist um festzustellen, in welcher Weise personenbezogene Daten verarbeitet werden.

Diese Sicherungsziele orientieren sich möglichst technologieunabhängig an den Sicherungszielen, die sich zur Datensicherheit herausgebildet haben und auch den in der hamburgischen Verwaltung angewandten Sicherungskonzepten zugrunde liegen. Sie weisen eine hinreichende Flexibilität auf, wodurch das Gesetz praxisnah und zukunftsoffen anwendbar ist.

Mit welchen konkreten Maßnahmen die Ziele erfüllt werden, bleibt den verantwortlichen Stellen überlassen. Die Erforderlichkeit und das angemessene Verhältnis zur Schutzwürdigkeit der Daten im Einzelfall lässt sich immer nur anhand der konkreten Gegebenheiten bestimmen. Mehrere Faktoren (Art und Schutzwürdigkeit der Daten, Schulung und Zuverlässigkeit des Personals, räumliche und technische Gegebenheiten, Abgeschlossenheit der Dienststelle usw.) sind dabei zu berücksichtigen. Die Entscheidung liegt bei der jeweiligen öffentlichen Stelle, der insoweit ein organisatorischer Handlungsspielraum zusteht. Dass Maßnahmen nach dem jeweiligen Stand der Technik zu treffen sind, bedarf dabei keiner ausdrücklichen gesetzlichen Festlegung.

Absatz 3 stellt klar, dass angemessene technische und organisatorische Maßnahmen auch bei nicht-automatisierter Verarbeitung zu treffen sind. Gegenüber der automatisierten Datenverarbeitung sind allerdings die Gewichte der Maßnahmen unterschiedlich gesetzt: hier kommt der Verhinderung des Zugriffs durch Unbefugte zentrale Bedeutung zu (Vertraulichkeit); wird dies sichergestellt, können auch die anderen Sicherungsziele erreicht werden.

Absatz 4 verpflichtet die Stellen, die automatisierte Verfahren zur Verarbeitung personenbezogener Daten betreiben wollen, vor der Entscheidung über die Einführung oder die wesentliche Änderung eines solchen Verfahrens, eine Risikoanalyse durchzuführen. Hierin sind die Risiken des geplanten Verfahrens abzuschätzen sowie mögliche Alternativen mit geringerer Eingriffstiefe für die Betroffenen zu prüfen. Form und Tiefe der vorzunehmenden Prüfung haben sich an der Sensibilität der zu verarbeitenden Daten und an den technischen und organisatorischen Rahmenbedingungen der geplanten Datenverarbeitung zu orientieren. Ein in bestimmter Weise formalisiertes Prüfverfahren wird dabei nicht vor geschrieben.

Nur soweit die Risiken durch technische und organisatorische Maßnahmen – bei Geltung der Verhältnismäßigkeitsregelung des Absatzes 1 Satz 2 – beherrschbar sind, ist der Einsatz des Verfahrens zulässig.

Diese Vorschrift beinhaltet eine Regelung des sogenannten vorgezogenen Datenschutzes; schon vor dem Einsatz oder der Änderung eines ADV-Verfahrens hat sich die Daten verarbeitende Stelle bewusst zu machen, welche Risiken für den Datenschutz mit einem bestimmten Verfahren verbunden sind und wie diese beherrscht werden können. Zudem ist die Daten verarbeitende Stelle dazu verpflichtet, das Ergebnis der Risikoanalyse der oder dem behördlichen Datenschutzbeauftragten bzw. der oder dem Hamburgischen Datenschutzbeauftragten zur Stellungnahme vorzulegen, soweit danach von einem Verfahren eine besondere Gefährdung für die Rechte der Betroffenen ausgeht (Absatz 4 Satz 3). Der Hamburgische Datenschutzbeauftragte geht davon aus, dass mit dem Ergebnis der Untersuchung jeweils auch deren Begründung zugeleitet wird. Im Zusammenhang mit §10a Absatz 5 Satz 3 Nummer 3 setzt diese Vorschrift Artikel 20 der EG-Datenschutzrichtlinie über die Vorabkontrolle von Datenverarbeitungen um, die spezifische Risiken für die Rechte und Freiheiten Betroffener mit sich bringen können.

Der Begriff der „besonderen Gefährdung“ kann als unbestimmter Rechtsbegriff nur einzelfallbezogen konkretisiert werden. Als Beurteilungskriterien kommen insbesondere die Art und der Umfang der zu verarbeitenden Daten sowie Zweck, Art und Umfang ihrer Verarbeitung in Betracht. Eine besondere Gefährdung liegt in jedem Fall nur vor, wenn die Gefahren, die von einem Datenverarbeitungsverfahren für die Rechte der Betroffenen ausgehen, deutlich das übliche Maß der Gefährdung übersteigen, das jede automatisierte Datenverarbeitung mit sich bringt. Im Hinblick auf Art und Umfang der Daten kann eine besondere Gefährdung z.B. vorliegen, wenn sensitive Daten im Sinne von §5 Absatz 1 Satz 2 Gegenstand der Verarbeitung sind oder Daten der einzelnen Betroffenen in einem Umfang verarbeitet werden, der weitreichende Schlüsse auf die Persönlichkeit oder den Lebenswandel der Betroffenen

ermöglicht. Aus Zweck, Art und Umfang der Verarbeitung können sich besondere Gefährdungen z.B. ergeben, wenn es sich um Verarbeitungen nach den §§5a und 5b handelt oder aus den Ergebnissen der Verarbeitung gravierende nachteilige Folgen für die Betroffenen gezogen werden sollen.

Da es im Übrigen wenig sinnvoll erscheint, Datenverarbeitungen, die besondere Gefährdungen beinhalten, vorab und abstrakt zu definieren – es ist vielmehr gerade Inhalt der Risikoanalyse, solche Risiken aufzudecken –, sieht das Gesetz eine verfahrensmäßige Lösung vor. Danach hat die Risikoanalyse selbst sich zu der Frage etwaiger besonderer Gefährdungen zu äußern. Bejahendenfalls findet eine weitere Prüfung durch die behördlichen bzw. durch die oder den Hamburgischen Datenschutzbeauftragten statt. Die Frage, ob es sich überhaupt um ein vorabkontrollpflichtiges Verfahren handelt, ist von ihnen allerdings eigenständig zu beurteilen und somit Gegenstand der weiteren Prüfung. Die behördlichen bzw. die oder der Hamburgische Datenschutzbeauftragte haben vor Einführung oder wesentlicher Änderung des Verfahrens somit die Gelegenheit, aufgrund ihrer Prüfung eine Stellungnahme abzugeben. Die Verantwortung der Daten verarbeitenden Stelle für die Entscheidung über die Einführung des Datenverarbeitungsverfahrens bleibt hiervon unberührt.

Der Hamburgische Datenschutzbeauftragte wird bis Ende 2002 dem Rechtsausschuss/Unterausschuss Datenschutz gemäß §23 Absatz 3 Satz 3 HmbDSG über die Auswirkungen berichten, die sich aus der vorgesehenen Beteiligung des Hamburgischen Datenschutzbeauftragten an der Vorabkontrolle nach dem neuen §8 Absatz 4 Satz 3 HmbDSG ergeben.

Zu §9 (Verfahrensbeschreibung)

Hintergrund für die Regelung sind die Artikel 18 und 19 der EG-Datenschutzrichtlinie. Danach sind die Daten verarbeitenden Stellen verpflichtet, automatisierte Datenverarbeitungen unter Mitteilung bestimmter, in Artikel 19 Absatz 1 der EG-Datenschutzrichtlinie genannter Angaben einer Kontrollstelle zu melden. Von der Meldung kann nach Artikel 18 Absatz 2 2. Spiegelstrich bei Bestellung behördlicher Datenschutzbeauftragter (s. dazu §10 a) zwar abgesehen werden. Ein Verzeichnis mit den entsprechenden Angaben ist allerdings auch in diesem Fall zu führen. Dies ergibt sich aus Artikel 21 Absatz 3 der EG-Datenschutzrichtlinie, wonach diese Angaben auf Antrag jedermann in geeigneter Weise verfügbar zu machen sind.

Die Verfahrensbeschreibung nach Absatz 1 Satz 1 verlangt nicht die Bezeichnung bestimmter – auch manueller – Datensammlungen, sondern nur die Beschreibung von Verfahren zur (zumindest teil-)automatisierten Verarbeitung personenbezogener Daten, die ihrerseits naturgemäß eine ganze Reihe von Dateien beinhalten können. Dabei ist der Begriff des Verfahrens nicht programmtechnisch, sondern unter dem Gesichtspunkt von Arbeitsabläufen zu verstehen (z.B. Verfahren zur Bearbeitung von Bauanträgen oder dgl.). Die Verfahrensbeschreibung muss in Übereinstimmung mit Artikel 19 Absatz 1 der EG-Datenschutzrichtlinie die in den Nummern 1 bis 9 genannten Daten umfassen.

Nummer 5 verlangt in Übereinstimmung mit Artikel 19 Absatz 1 Buchstabe d der EG-Datenschutzrichtlinie die Bezeichnung der Empfängerinnen oder Empfänger oder Empfängerkreise, die Daten aus dem Verfahren erhalten können. Zu beachten ist dabei, dass der Empfängerbegriff weiter ist als der der bisherigen „empfangenden Stellen“ (vgl. zu §4 Absatz 5). Nicht zu den in die Verfahrensbeschreibung aufzunehmenden Empfängern gehören Prüfungsbehörden – z.B. der Rechnungshof –, denen gesetzliche Vorlagerechte zustehen.

Nach Nummer 6 sind beabsichtigte Übermittlungen an Drittländer anzugeben. Hiermit wird Artikel 19 Absatz 1 Buchstabe e der EG-Datenschutzrichtlinie entsprochen.

Nummer 9 trägt den erweiterten Schutzrechten der Betroffenen (§12a) Rechnung.

Absatz 1 Satz 2 gibt die Möglichkeit, Beschreibungen gleichartiger Verfahren in einer einzigen Verfahrensbeschreibung zusammenzufassen. Die Vorschrift bezweckt eine Verwaltungsvereinfachung, die gleichzeitig auch die Transparenz der Verfahrensbeschreibung erhöhen kann.

Absatz 2 sieht in Übereinstimmung mit Artikel 18 Absätze 2 und 3 Ausnahmen von der Beschreibungspflicht für Verfahren der Registerführung vor, sofern das Register zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, offen steht, sowie für Verfahren der allgemeinen Bürokommunikation. Letztere gehören heute zu der durchweg üblichen Grundausstattung jeder Verwaltung. Sie lassen im Allgemeinen auch keine Gefährdungen des Rechts auf informationelle Selbstbestimmung erwarten. Das Verlangen von Verfahrensbeschreibungen, die praktisch von jeder Daten verarbeitenden Stelle in gleicher Weise erstellt werden müssten, würde als aufwendiger Formalismus keinen messbaren Nutzen für den Datenschutz ergeben.

Absatz 3 setzt die Meldepflicht nach Artikel 18 Absatz 1 der EG-Datenschutzrichtlinie für die Stellen, die keine behördlichen Datenschutzbeauftragten bestellt haben, sowie den Artikel 21 der EG-Datenschutzrichtlinie über die Öffentlichkeit der Verarbeitungen um. Das Einsichtsrecht steht jeder Person unabhängig davon zu, ob sie durch eine Datenverarbeitung betroffen ist. Die Wahrnehmung des Einsichtsrechts erfolgt bei den Daten verarbeitenden Stellen selbst. Diese Regelung dient der Vereinfachung, Transparenz und Bürgernähe des Verfahrens. Die Ausnahmen vom Einsichtsrecht in Satz 3 sind EG-rechtlich durch den insofern beschränkten Anwendungsbereich der Richtlinie gerechtfertigt.

Zu §10 (Durchführung des Datenschutzes)

Die Vorschrift begründet die Pflicht der öffentlichen Stellen, die Beachtung aller Datenschutzvorschriften sicherzustellen.

Zu §10a (Behördliche Datenschutzbeauftragte bzw. behördlicher Datenschutzbeauftragter)

Die neu eingefügte Vorschrift macht von der Möglichkeit des Artikels 18 Absatz 2 2. Spiegelstrich der EG-Datenschutzrichtlinie Gebrauch, anstelle der in der Richtlinie vorgesehenen Meldepflichten gegenüber der Kontrollstelle (hier: Hamburgische Datenschutzbeauftragte bzw. Hamburgischer Datenschutzbeauftragter) behördliche Datenschutzbeauftragte zu bestellen. Die Bestellung behördlicher Datenschutzbeauftragter stellt das Gesetz in das Ermessen der Daten verarbeitenden Stellen und ermöglicht damit eine flexible, an den jeweiligen Bedürfnissen und Problemen der Daten verarbeitenden Stelle orientierte Handhabung. Für Daten verarbeitende Stellen, die behördliche Datenschutzbeauftragte bestellen, gelten gegenüber den anderen Daten verarbeitenden Stellen die folgenden Besonderheiten bzw. Erleichterungen:

– Verfahrensbeschreibungen Daten verarbeitender Stellen mit behördlichen Datenschutzbeauftragten werden von Letzteren geführt und zur Einsicht bereitgehalten (§9 Absatz 3). Andere Daten verarbeitende Stellen haben die Verfahrensbeschreibungen der bzw. dem Hamburgischen Datenschutzbeauftragten zu übersenden, um ihm mögliche Kontrollbedarfe anzuzeigen.
– Die Vorabkontrolle von Datenverarbeitungsverfahren, von denen besondere Gefährdungen für die Rechte Betroffener ausgehen (Artikel 20 der EG-Datenschutzrichtlinie), obliegt den behördlichen Datenschutzbeauftragten, hingegen, wenn behördliche Datenschutzbeauftragte nicht bestellt werden, der bzw. dem Hamburgischen Datenschutzbeauftragten (§8 Absatz 4).
– Vor pauschalen Entscheidungen über das Absehen von Benachrichtigungen nach §12a Absatz 3 Satz 2 sind die behördlichen Datenschutzbeauftragten zu hören. Sind solche nicht bestellt, ist die bzw. der Hamburgische Datenschutzbeauftragte einzuschalten.
– Absatz 1 ermöglicht den in §2 Absatz 1 Satz 1 genannten Stellen die Bestellung behördlicher Datenschutzbeauftragter. Die Befugnis, eine Beschäftigte oder einen Beschäftigten einer anderen Stelle zur bzw. zum behördlichen Datenschutzbeauftragten zu bestellen, ermöglicht es insbesondere kleinen Stellen, gemeinsame behördliche Datenschutzbeauftragte zu bestellen. Ein besonderer rechtlicher Status der „gemeinsamen“ behördlichen Datenschutzbeauftragten folgt hieraus allerdings nicht. Sie sind jeweils Datenschutzbeauftragte der jeweiligen besonderen Stelle.

Absatz 2 regelt die erforderliche Qualifikation und Zuverlässigkeit der behördlichen Datenschutzbeauftragten.

Absatz 3 regelt den Widerruf der Bestellung zur bzw. zum behördlichen Datenschutzbeauftragten. Im Hinblick auf die unabhängige Stellung der für einen unbestimmten Zeitraum zu bestellenden behördlichen Datenschutzbeauftragten (Absatz 4 Satz 2) ist der Widerruf zum Ausschluss von Missbräuchen an enge Voraussetzungen geknüpft. Eine zusätzliche Verfahrenssicherung bietet die obligatorische Anhörung der bzw. des Hamburgischen Datenschutzbeauftragten vor der Entscheidung über den Widerruf. Der Sache nach ist der Widerruf lediglich bei Eintritt eines wichtigen Grundes im Sinne von §626 des Bürgerlichen Gesetzbuchs zulässig.

Absatz 4 beschreibt den unabhängigen Status der behördlichen Datenschutzbeauftragten. Sie können sich in dieser Funktion unmittelbar an die Leitung der Daten verarbeitenden Stelle wenden. Bei ihrer Tätigkeit sind sie weisungsfrei und dürfen auch im Nachhinein wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. Die Pflicht, sie in erforderlichem Umfang von der Erfüllung anderer Aufgaben freizustellen und sie bei der Erfüllung ihrer Aufgaben zu unterstützen, schließt eine angemessene Ausstattung mit sächlichen und unter Umständen auch personellen Ressourcen ebenso ein wie die Pflicht zur Information über für ihre Aufgabenwahrnehmung bedeutsame Vorgänge.

Absatz 5 benennt die Aufgaben der behördlichen Datenschutzbeauftragten. Satz 1 beschreibt die Grundregel, dass die behördlichen Datenschutzbeauftragten die Daten verarbeitenden Stellen in der Ausführung datenschutzrechtlicher Vorschriften zu unterstützen haben. Die Aufgabe der behördlichen Datenschutzbeauftragten ist demnach primär nicht auf die nachgängige Kontrolle von Verwaltungshandeln auf seine Datenschutzkonformität, sondern darauf ausgerichtet, der Daten verarbeitenden Stelle begleitende Hilfestellung für datenschutzgerechtes Handeln zu geben.

Satz 2 erlaubt es den behördlichen Datenschutzbeauftragten, sich zur Wahrnehmung ihrer Aufgaben jederzeit an die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten zu wenden.

Satz 3 konkretisiert die Aufgaben der behördlichen Datenschutzbeauftragten in einer beispielhaften Aufzählung:

Nach Nummer 1 haben sie, insbesondere im Zusammenhang mit der Implementation neuer Datenschutzvorschriften, deren Handlungserfordernisse sie aufgrund ihrer Sachkenntnis am ehesten werden einschätzen können, auf deren Umsetzung und im Übrigen auf ihre Einhaltung hinzuwirken. Hierzu gehört es auch, Hinweisen auf datenschutzrechtliche Mängel in der Daten verarbeitenden Stelle nachzugehen. Auch die Information über datenschutzrechtliche Erfordernisse und eine entsprechende Schulung von Bediensteten der Daten verarbeitenden Stelle kommen als Maßnahmen der Hinwirkung auf die Umsetzung und Einhaltung von Datenschutzvorschriften in Betracht.

Nach Nummer 2 führen die behördlichen Datenschutzbeauftragten die – von den zuständigen Fachämtern und -abteilungen zu erstellenden – Verfahrensbeschreibungen und halten sie zur Einsicht bereit. Diese Aufgabe folgt aus Artikel 18 Absatz 2 2. Spiegelstrich 2. Beistrich der EG-Datenschutzrichtlinie. Die Führung der Verfahrensbeschreibungen schließt neben deren Sammlung auch ihre Kontrolle auf Plausibilität, Vollständigkeit und Aktualität ein.

Nummer 3 regelt die Prüfungszuständigkeit der behördlichen Datenschutzbeauftragten im Rahmen der Vorabkontrolle nach Artikel 20 der EG-Datenschutzrichtlinie (vgl. auch zu §8 Absatz 4). Die Verpflichtung, in Zweifelsfällen die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten zu hören, beruht auf Artikel 20 Absatz 2 der EG-Datenschutzrichtlinie.

Satz 4 gibt den behördlichen Datenschutzbeauftragten ein grundsätzlich umfassendes Einsichtsrecht. Aufgrund des Vorbehalts entgegenstehender Rechtsvorschriften ist ihnen allerdings insbesondere die Einsicht in Unterlagen mit personenbezogenen Daten, deren Schutz bereichsspezifisch geregelt ist, nur dann erlaubt, wenn die bereichsspezifischen Vorschriften dies zulassen oder eine Einwilligung der Betroffenen vorliegt.

Absatz 6 räumt den Betroffenen sowie den Beschäftigten der Daten verarbeitenden Stellen, ohne Rücksicht darauf, ob diese im Einzelfall auch Betroffene sind, das Recht ein, sich jederzeit unmittelbar an die behördlichen Datenschutzbeauftragten zu wenden. Das Maßregel- und Benachteiligungsverbot entspricht dem aus §26 Absatz 2 Satz 1.

Absatz 7 verpflichtet die behördlichen Datenschutzbeauftragten zur Verschwiegenheit über die Identität und die Identität erhellende Umstände solcher Personen, die sich an sie gewandt haben. Hierdurch soll das Vertrauen in die behördlichen Datenschutzbeauftragten zusätzlich gestärkt werden. Ausnahmen von der Verschwiegenheitspflicht bestehen für den Fall der Einwilligung und im Verhältnis zur bzw. zum Hamburgischen Datenschutzbeauftragten.

Die in Absatz 8 vorgesehene Meldung der Bestellung bzw. des Widerrufs der Bestellung oder sonstigen Beendigung des Amtes behördlicher Datenschutzbeauftragter verschafft der bzw. dem Hamburgischen Datenschutzbeauftragten die für die Wahrnehmung ihrer bzw. seiner Kontrollaufgaben notwendige Kenntnis, insbesondere darüber, ob eine Daten verarbeitende Stelle verpflichtet ist, Verfahrensbeschreibungen zu übersenden.

Zu §11 (Automatisiertes Abrufverfahren)

Den Verfahren zur automatisierten Direktabfrage von personenbezogenen Datenbeständen (Online-Anschlüsse) als Informationsaustausch kommt unter dem Aspekt des Datenschutzes besondere Bedeutung zu, weil die abrufende Stelle nach Einrichtung eines solchen Anschlusses über den gesamten Bestand der von der Daten verarbeitenden Stelle bereitgehaltenen Daten verfügen kann. Die mögliche Übermittlung einer sehr umfangreichen Anzahl personenbezogener Daten birgt erhebliche Gefahren für das Recht auf informationelle Selbstbestimmung in sich. Aus diesem Grund und wegen der besonderen Risiken der Online-Anschlüsse wird die Einrichtung solcher Verfahren an besondere Zulässigkeitsvoraussetzungen gebunden.

Nach Absatz 1 ist in der öffentlichen Verwaltung die Einrichtung derartiger automatisierter Abrufverfahren prinzipiell

nur auf der Grundlage ausdrücklicher Rechtsvorschriften zugelassen; die Einrichtung solcher Verfahren wird nicht dem Ermessen und der Einzelabwägung der beteiligten Behörden überlassen. Nicht betroffen sind dagegen Online-Anschlüsse, mit denen nicht personenbezogene (z.B. statistische) Einzelangaben übermittelt werden. Absatz 1 findet ferner keine Anwendung auf diejenigen Fälle, in denen Behörden als auftraggebende Stellen im Rahmen der Auftragsdatenverarbeitung ihre personenbezogenen Datenbestände bei auftragnehmenden Stellen (Rechenzentren) abrufen.

In Absatz 2 Satz 1 wird der Senat ermächtigt, automatisierte Abrufverfahren durch Rechtsverordnung einzuführen. Voraussetzung ist, dass die Einrichtung solcher Verfahren nach Abwägung der betroffenen Interessen angemessen ist. Satz 2 sichert die Unterrichtung der oder des Hamburgischen Datenschutzbeauftragten, damit sogleich oder auch später eine datenschutzrechtliche Kontrolle durchgeführt werden kann. Die Sätze 3 bis 5 schreiben den erforderlichen Regelungsinhalt der Verordnung vor. Satz 6 stellt klar, dass §11 lediglich die Einrichtung des automatisierten Abrufverfahrens regelt; die materiell-rechtliche Zulässigkeit des einzelnen Abrufs bestimmt sich nach den §§12 ff.

Es bedarf keiner besonderen Erwähnung durch den Gesetzgeber, dass automatisierte Abrufverfahren nur in Betrieb genommen werden dürfen, wenn vorher die technischen und organisatorischen Maßnahmen nach §8 sowohl bei der übermittelnden Stelle als auch bei den Stellen, denen die Daten übermittelt werden, getroffen sind.

Absatz 3 berücksichtigt wegen der gleichen Interessenlage die Einrichtung automatisierter Abrufverfahren innerhalb einer Behörde für den Fall, dass die übermittelnde Einheit und der Einheit, der die Daten übermittelt werden, unterschiedliche Aufgaben wahrnehmen. Die Zulassung erfolgt unter den gleichen Voraussetzungen wie beim Abruf durch Dritte (vgl. Absatz 2), doch tritt an die Stelle einer Rechtsverordnung des Senats ein innerdienstlicher Organisationsakt der Behördenleitung. Nach Satz 2 soll auch vor der Einrichtung stelleninterner automatisierter Abrufverfahren die Anhörung der bzw. des Hamburgischen Datenschutzbeauftragten obligatorisch sein.

Nach Absatz 4 sind automatisierte Abrufverfahren nicht zulässig im Verhältnis der öffentlichen Verwaltung zu Stellen außerhalb des öffentlichen Bereichs. Privaten Stellen soll kein unmittelbarer Zugriff auf Datenbanken der öffentlichen Verwaltung mit personenbezogenem Inhalt ermöglicht werden. Dies gilt nicht in den Fällen, in denen die Betroffenen ihre eigenen Daten abrufen können.

Wenn die Daten verarbeitende Stelle die Daten veröffentlichen dürfte oder es sich um einen Anschluss an Datenbestände handelt, die jedem ohne oder nach besonderer Zulassung offen stehen, bestehen gegen automatisierte Abrufverfahren ebenfalls keine Bedenken; in diesen Fällen kommen die Absätze 1 bis 4 nicht zur Anwendung (Absatz 5).

Zu §11a (Gemeinsame und verbundene automatisierte Dateien)

Mit dieser Vorschrift werden rechtliche Rahmenbedingungen für die Datenverarbeitung aus gemeinsamen oder verbundenen automatisierten Dateien in einem Datenschutz-Querschnittsgesetz festgelegt.

§11 regelt den Fall, dass eine Stelle, die als Daten verarbeitenden Stelle identifiziert werden kann, personenbezogene Daten zum automatisierten Abruf für eine oder mehrere andere Stellen bereithält; hierfür werden wegen der Gefahren für das informationelle Selbstbestimmungsrecht schon bisher rechtliche Festlegungen verlangt. Diese Konstellation soll auch weiterhin allein von §11 erfasst bleiben. An ihr ändert sich auch nichts dadurch, dass andere Stellen ihre Daten z.B. nach Maßgabe des §14 der genannten Daten verarbeitende Stelle übermitteln, die diese Daten in ihre Datensammlung eingibt und dann nach Maßgabe des §11 zum automatisierten Abruf bereithält.

Die Gefährdungslage bezüglich der informationellen Selbstbestimmung und damit der Regelungsbedarf verdichten sich in den Fällen, in denen mehrere Stellen in einem automatisierten Verfahren lesend (Abruf) und schreibend (Eingabe, Veränderung, Löschung) unmittelbar auf einen Datenbestand zugreifen können, der entweder als gemeinsame (zentrale) Datei oder als Dateienverbund konzipiert ist. Diese Fälle sind dadurch gekennzeichnet, dass der Datenbestand ohne zentrale Kontrolle durch eine bestimmte Daten verarbeitende Stelle von allen angeschlossenen Stellen unmittelbar bedient werden kann und dass die eingebende Stelle keine Kontrolle darüber hat, wer eine von ihr eingegebene Information abruft. Neben dem Umfang der Verarbeitungsbefugnis der einzelnen beteiligten Stellen sind hier vor allem die datenschutzrechtlichen Verantwortlichkeiten gegenüber den Betroffenen zu regeln und zu bestimmen, welche Stelle die technischen und organisatorischen Maßnahmen trifft.

Bereichsspezifische Beispiele für Regelungen über gemeinsame Dateien finden sich in Hamburg in §14 Absatz 6 des Hamburgischen Vermessungsgesetzes vom 30. Juni 1993 (Hamburgisches Gesetz- und Verordnungsblatt Seite 135) und auf Bundesebene z.B. in §6 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (Bundesgesetzblatt

I Seiten 2954, 2970).

Die Vorschrift orientiert sich in Aufbau und Inhalt an §11. Nach Absatz 1 Satz 1 bedarf die Einrichtung der näher bezeichneten automatisierten Dateien, in oder aus denen mehrere hamburgische öffentliche Stellen personenbezogene Daten verarbeiten dürfen, der ausdrücklichen Zulassung durch eine Rechtsvorschrift. In einer Parallele zu §11 Absatz 2 Satz 1 ermächtigt Satz 2 den Senat, die Einrichtung solcher Dateien durch Rechtsverordnung zuzulassen. In Satz 3 (durch Verweisung auf einzelne Bestimmungen des §11) und Satz 4 sind Voraussetzungen und Inhalt einer solchen Verordnung näher umrissen; außerdem ist die obligatorische Beteiligung der oder des Hamburgischen Datenschutzbeauftragten festgeschrieben. Satz 5 stellt klar, dass §11a lediglich die Einrichtung des automatisierten Verfahrens regelt, die materiell-rechtliche Zulässigkeit der Datenverarbeitung im Einzelnen sich hingegen nach den §§12 ff. oder nach bereichsspezifischen Regelungen richtet.

Absatz 2 regelt in Anlehnung an §11 Absatz 3 den Fall, dass gemeinsame oder verbundene Dateien innerhalb einer öffentlichen Stelle zwischen Einheiten mit unterschiedlichen Aufgaben eingerichtet werden sollen. Die Zulässigkeitsvoraussetzungen sind die gleichen wie beim externen Verbund, nur entfällt hier das Erfordernis einer Rechtsvorschrift. An seine Stelle tritt die Zulassung durch die Leiterin oder den Leiter der Stelle.

Zu §12 (Datenerhebung)

In §12 wird das Erheben personenbezogener Daten (in der Definition des §4 Absatz 2 Satz 2 Nummer 1) als eigene Phase der Datenverarbeitung geregelt.

Nicht unter den Erhebungsbegriff fallen personenbezogene Daten, die von den Betroffenen selbst oder von Dritten ohne Anforderung der in §2 Absatz 1 Satz 1 genannten Stelle geliefert werden, sowie Erkenntnisse, die der Verwaltungsbehörde durch Zufall bekannt werden. Aber auch in diesen Fällen ist nur eine eingeschränkte Verwertbarkeit im Rahmen rechtmäßiger Aufgabenerfüllung vorgesehen (vgl. §13 Absatz 1 Satz 2).

Grundsätzliche Voraussetzung jedes Erhebens ist, dass die Beschaffung personenbezogener Daten zur Aufgabenerfüllung der Daten verarbeitenden Stelle erforderlich ist (Absatz 1); es bedarf keiner Hervorhebung durch den Gesetzgeber, dass nur eine rechtmäßige Aufgabenerfüllung in Betracht kommt.

Erforderlich ist die Datenerhebung (oder – vgl. z.B. §§13, 14 und 16 – eine andere Maßnahme der Datenverarbeitung) nicht erst dann, wenn kein anderes Mittel zur Aufgabenerfüllung zur Verfügung steht (ultima ratio). Es genügt, wenn die Aufgabe auf andere Weise nur unter unverhältnismäßig großen Schwierigkeiten erfüllt werden könnte. Diese Formulierung darf allerdings nicht dazu führen, dass die Behörden sich jeweils für die bequemste aller möglichen Lösungen entscheiden; sie haben vielmehr sehr sorgfältig die privaten und öffentlichen Interessen gegeneinander abzuwägen, wobei die Abwägung um so genauer vorgenommen werden muss, je tiefer der Grundrechtseingriff ist.

Nach Absatz 2 haben zur Sicherung des Rechts auf informationelle Selbstbestimmung die Verwaltungsbehörden die von ihnen benötigten personenbezogenen Daten grundsätzlich unmittelbar bei den Betroffenen mit ihrer Kenntnis zu erheben. Denn nur auf diesem Wege können sie ihr Recht, selbst über die Preisgabe und Verwendung ihrer Daten bestimmen zu dürfen, wirksam ausüben. Die Erhebung personenbezogener Daten ohne ihre Kenntnis bei Behörden oder privaten Stellen oder auch durch eine verdeckte Beobachtung oder heimliche Videoüberwachung soll im Grundsatz ausgeschlossen sein. Der so umfassende Schutzgedanke lässt es aber zu, dass die Betroffenen eines Verwaltungsverfahrens z.B. dann personenbezogene Daten Dritter – sie sind ebenfalls Betroffene im Sinne des Gesetzes – selbst angeben, wenn das Gesetz ihre Rechtsposition von den persönlichen Verhältnissen dieser Personen abhängig macht (z.B. von Ehegatten, Eltern und Kindern).

Satz 2 nimmt die Anforderungen, die an die Datenerhebung mit Kenntnis der Betroffenen zu stellen sind, für den Fall der Datenerhebung nicht bei einzelnen Betroffenen, sondern bei bestimmbaren Personenkreisen insoweit zurück, als in diesem Fall nicht die positive Kenntnisnahme, sondern lediglich die zumutbare Möglichkeit einer Kenntnisnahme von der Datenerhebung gefordert wird. Damit wird insbesondere klar gestellt, dass Videoüberwachungen unter den Voraussetzungen einer Datenerhebung mit Kenntnis der Betroffenen zulässig sind, wenn auf solche Überwachungen z.B. durch deutlich sichtbare Hinweisschilder aufmerksam gemacht wird. Voraussetzung für die Anwendbarkeit der Bestimmung ist im Übrigen, dass es sich bei der jeweiligen Überwachungsmaßnahme überhaupt um die Erhebung personenbezogener Daten im Sinne des §4 Absatz 2 Satz 2 Nummer 1 handelt, also um das (zielgerichtete) Beschaffen personenbezogener Daten. Übersichtsaufnahmen ohne oder mit nur zufälligem Personenbezug fallen nicht hierunter, solange sie nicht personenbezogen ausgewertet werden.

Nach Satz 3 ist eine Erhebung bei anderen Stellen – unabhängig von einer Kenntnis der Betroffenen – unter den in

§13 Absatz 2 Satz 1 genannten Voraussetzungen zulässig. Damit wird klar gestellt, dass die in §§13 und 14 geregelten Fälle der Weitergabe und Übermittlung als weitere Fälle der Erhebung unter den dort genannten Voraussetzungen zulässig sind; denn eine jede Weitergabe an andere Einheiten einer öffentlichen Stelle (dem §13 unterliegendes Nutzen) oder eine jede Übermittlung an eine andere öffentliche Stelle (Übermittlung nach §14) auf deren Ersuchen hin ist zugleich im Sinne von §12 eine Erhebung. Satz 4 nimmt für die Erhebung bei Betroffenen ohne deren Kenntnis Beschränkungen vor: Sie ist zunächst auf Grund bereichsspezifischer Vorschriften zulässig, im Übrigen dann, wenn im Einzelnen genannte deutlich höherwertige Rechtsgüter diese besondere Form der Erhebung erforderlich machen. Für alle Fälle der Erhebung betont Satz 5 die besondere Geltung des Verhältnismäßigkeitsgrundsatzes im Datenschutzrecht; die Bestimmung soll unangemessene und unzumutbare Methoden bei der Erhebung, ebenso aber auch unzumutbare Fragen ausschließen.

Zu §12a (Unterrichtung bei der Erhebung)

Die neue Vorschrift des §12a fasst die Informationspflichten bei der Datenerhebung mit den aufgrund von Artikel 10 und 11 der EG-Datenschutzrichtlinie neu aufzunehmenden Bestimmungen zusammen. Dabei wird die bisherige Systematik beibehalten, die zwischen der Datenerhebung bei Betroffenen mit ihrer Kenntnis, der Erhebung bei Dritten und der Erhebung bei den Betroffenen ohne ihre Kenntnis unterscheidet. Die EG-Datenschutzrichtlinie unterscheidet demgegenüber nur zwischen der Datenerhebung bei der betroffenen Person (Artikel 10) und dem Fall, dass die Daten nicht bei der betroffenen Person erhoben werden (Artikel 11), wobei der Fall der Datenerhebung bei der betroffenen Person nur die Erhebung mit Kenntnis der Betroffenen umfasst.

Bereichsspezifische Vorschriften über die Benachrichtigung Betroffener, wie z.B. §8 Absatz 4 des Hamburgischen Verfassungsschutzgesetzes, gehen dem §12a vor.

Absatz 1 regelt die Aufklärungspflichten der erhebenden Stelle bei der Datenerhebung mit Kenntnis der Betroffenen entsprechend den Vorgaben des Artikels 10 Absatz 1 der EG-Datenschutzrichtlinie.

Satz 1 verlangt die Aufklärung über die Zweckbestimmungen der Datenverarbeitung und die – voraussichtlichen – Empfängerinnen oder Empfänger oder den Kreis der Empfängerinnen und Empfänger der Daten (vgl. Artikel 10 Buchstabe b und c 1. Spiegelstrich der EG-Datenschutzrichtlinie). Die Aufklärungspflicht hat in Übereinstimmung mit der Richtlinienbestimmung zur Voraussetzung, dass die Betroffenen nicht bereits anderweitig eine entsprechende Kenntnis erlangt haben. In solchen Fällen würde die – nochmalige – Aufklärung einen unnötigen und unter Umständen aufwendigen Formalismus darstellen. Die Aufklärung gemäß Nummer 1 über die „Zweckbestimmungen der Datenverarbeitung“ bedeutet eine Anpassung an den Sprachgebrauch der EG-Datenschutzrichtlinie. Inhaltlich entspricht die Bestimmung der Pflicht zur Aufklärung über den Verwendungszweck der Daten. Die Aufklärung über den Kreis der Empfängerinnen und Empfänger gemäß Nummer 2 ist davon abhängig gemacht worden, dass die Betroffenen nach den Umständen des Einzelfalls nicht bereits damit rechnen müssen, dass die entsprechenden Empfängerinnen und Empfänger die Daten erhalten. Diese Einschränkung ist EG-rechtlich durch die in Artikel 10 Buchstabe c a.E. der Richtlinie enthaltene Voraussetzung gerechtfertigt, dass die Aufklärung über die in Buchstabe c genannten Umstände nur erfolgen muss, wenn sie notwendig ist, um eine Datenverarbeitung nach Treu und Glauben sicherzustellen. Eine Aufklärung über Verarbeitungsvorgänge, mit denen die Betroffenen nach den Umständen des Einzelfalls bereits rechnen müssen, gehört hierzu nicht.

Nach Auffassung des Hamburgischen Datenschutzbeauftragten ist Satz 1 Nummer 2 (und entsprechend auch Absatz 2 Satz 1 Nummer 3) so auszulegen, dass von einer Aufklärung bzw. Benachrichtigung hinsichtlich der Empfängerinnen oder Empfänger oder des Kreises der Empfängerinnen und Empfänger nur dann abgesehen werden darf, wenn sich den Betroffenen aufdrängen muss, dass diese die Daten erhalten.

Sätze 2 und 3 erfüllen die Vorgabe des Artikels 10 Buchstabe c 2. Spiegelstrich der EG-Datenschutzrichtlinie.

Mit Satz 4 wird dem Artikel 10 Buchstabe c 3. Spiegelstrich Rechnung getragen. Die Beschränkung der Aufklärung auf den Fall der schriftlichen oder der Erhebung zur Niederschrift rechtfertigt sich wiederum aus dem Treu-und-Glauben-Vorbehalt der Richtlinienbestimmung.

Absatz 2 regelt die Benachrichtigungspflichten der erhebenden Stelle bei der Datenerhebung bei Dritten oder bei Betroffenen ohne deren Kenntnis. In der Diktion der EG-Datenschutzrichtlinie handelt es sich um den Fall, dass die Daten nicht bei der betroffenen Person erhoben werden (vgl. hierzu die Eingangsbemerkung zu §12 a). Die Bestimmung beruht auf den Vorgaben von Artikel 11 der EG-Datenschutzrichtlinie. Dem Inhalt nach entspricht die Unterrichtung im Wesentlichen der Aufklärung nach Absatz 1 Satz 1. Die zusätzliche Angabe über die

Art der erhobenen Daten nach Nummer 1 folgt aus dem Umstand, dass die Betroffenen hierüber in den von Absatz 2 geregelten Fällen, anders als bei der Datenerhebung mit ihrer Kenntnis, nicht orientiert sind. Satz 3 dient der Verwaltungsvereinfachung, indem er es erlaubt, die Benachrichtigung mit einer Mitteilung an die Betroffenen zu verbinden, wenn die Datenerhebung der Erstellung einer eben solchen Mitteilung dient.

Absatz 3 regelt die Ausnahmen von der Benachrichtigungspflicht nach Absatz 2. Von den Ausnahmemöglichkeiten, die sich aus dem beschränkten Anwendungsbereich der EG-Datenschutzrichtlinie sowie ihren Artikeln 11 Absatz 2 und 13 ergeben, wird dabei umfassend Gebrauch gemacht, um den andernfalls zu erwartenden Verwaltungsaufwand zu vermeiden, der in keinem angemessenen Verhältnis zu dem durch die Benachrichtigung verfolgten Schutzzweck stünde. In diesem Zusammenhang kann etwa auf hessische Erfahrungen verwiesen werden. Das Hessische Datenschutzgesetz sah in seinem §18 Absatz 2 eine umfassende Benachrichtigungspflicht vor. Die Begründung des Gesetzentwurfs der Landesregierung zur Anpassung des Gesetzes an die EG-Datenschutzrichtlinie (Landtagsdrucksache 14/3830 vom 27. April 1998, Seite 24) hat hierzu ausgeführt, dass die Erfahrung mit den bisherigen gesetzlichen Regelungen gezeigt habe, dass der mit der Benachrichtigung verbundene erhebliche Verwaltungsaufwand in keinem angemessenen Verhältnis zum Schutz der Rechte der Betroffenen stehe. Von einer völligen Streichung der Benachrichtigung werde lediglich im Hinblick auf die EG-Datenschutzrichtlinie abgesehen, deren Ausnahmemöglichkeiten aber genutzt.

Satz 1 schließt die Datenverarbeitung zur Wahrnehmung von Gefahrenabwehr- und Strafverfolgungsaufgaben von der Benachrichtigungspflicht aus. Grundlage hierfür ist Artikel 3 Absatz 2 der EG-Datenschutzrichtlinie.

Satz 2 nimmt einzelne Ausnahmemöglichkeiten in Anspruch, die die EG-Datenschutzrichtlinie selbst bietet:

Nummer 1 beruht auf Artikel 11 Absatz 2 Satz 1 der EG-Datenschutzrichtlinie. Verlangt wird, dass die Verarbeitung der Daten in einer bereichsspezifischen Vorschrift ausdrücklich vorgesehen ist.

Nummer 2 beruht ebenfalls auf Artikel 11 Absatz 2 Satz 1 der EG-Datenschutzrichtlinie. Unmöglich ist die Benachrichtigung, wenn die Betroffenen nicht ausreichend identifizierbar, insbesondere keine Adressen bekannt sind. Die Benachrichtigungspflicht selbst ist keine Rechtsgrundlage und begründet auch keine Rechtspflicht zur Erhebung von Daten mit dem alleinigen Zweck, die Benachrichtigung zu ermöglichen. Die Unverhältnismäßigkeit des Aufwandes ist im Einzelfall in Abwägung mit dem Informationsinteresse der Betroffenen zu bewerten.

Die Nummern 3 bis 5 beruhen auf Artikel 13 Absatz 1 der EG-Datenschutzrichtlinie. Soweit dabei in Nummer 3 die Gefährdung von Aufgaben der Gefahrenabwehr und die Verfolgung von Straftaten als Grund für einen Verzicht auf die Benachrichtigung genannt sind, kommt dem im Verhältnis zur Ausklammerung der Gefahrenabwehr und der Strafverfolgung in Satz 1 die Bedeutung zu, Fälle zu erfassen, in denen die Benachrichtigung die Erfüllung von Gefahrenabwehr- und Strafverfolgungsaufgaben gefährden würde, ohne dass die Datenverarbeitung selbst aber der Wahrnehmung dieser Aufgaben dient.

Satz 3 beruht auf Artikel 11 Absatz 2 Satz 2 der EG-Datenschutzrichtlinie. Danach sind in den auf Artikel 11 Absatz 2 Satz 1 gestützten Fällen des Absehens von einer Benachrichtigung „geeignete Garantien“ vorzusehen. Die Regelung will einer Aushöhlung der Benachrichtigungspflicht durch eine unangemessen weite Auslegung der Ausnahmebestimmungen vorbeugen. Diesem Anliegen wird verfahrensmäßig durch die obligatorische Anhörung der behördlichen Datenschutzbeauftragten bzw. der oder des Hamburgischen Datenschutzbeauftragten in Fällen, in denen pauschale Entscheidungen über das Absehen von Benachrichtigungen getroffen werden sollen, entsprochen.

Absatz 4 nimmt die Bestimmungen über die Aufklärung privater Dritter auf, bei denen Daten über Betroffene anstelle einer Datenerhebung bei den Betroffenen selbst erhoben werden.

Zu §13 (Zulässigkeit der weiteren Datenverarbeitung; Zweckbindung)

§13 soll die verfassungsrechtlich gebotene Zweckidentität zwischen der Erhebung bzw. Verarbeitung ohne Erhebung und der weiteren Verarbeitung personenbezogener Daten sicherstellen. Der Grundsatz der Zweckbindung gilt auch für die in §12 geregelte Erhebung, er wird durch die Ausrichtung der Erhebung an der rechtmäßigen Aufgabenerfüllung sichergestellt. §13 regelt weiterhin die zulässigen Ausnahmen vom Zweckbindungsgebot. Für die Übermittlungsphase gelten dabei die §§14 bis 17.

Absatz 1 Satz 1 enthält die zentrale Zweckbindungsregelung für die Datenverarbeitung durch eine öffentliche Stelle, die beim Bürger personenbezogene Daten zu bestimmten Zwecken zulässigerweise erhoben hat. Das mit der Einbeziehung der Erhebungsphase in den Schutzbereich des Gesetzes gewährleistete Recht der Betroffenen, im

Regelfall selbst über die Preisgabe und Verwendung ihrer Daten bestimmen zu dürfen, hat zur logischen Konsequenz, dass der Verwendungszweck der Daten bei der anschließenden Verarbeitung grundsätzlich nicht ohne Wissen der Betroffenen geändert werden darf. Die Zweckbindung gilt aber nicht nur für personenbezogene Daten, die zielgerichtet erhoben worden sind, sondern auch für solche Daten, die der Verwaltung ohne ihr Zutun zugehen oder erst, wie z.B. Einbürgerungen oder Namensänderungen, durch behördliches Handeln entstehen (Absatz 1 Satz 2). Werden diese Daten zulässigerweise im Rahmen der rechtmäßigen Aufgabenerfüllung gespeichert, dann setzt mit diesem zielgerichteten Handeln die Zweckbindung ein.

In Einzelfällen wird es auf Schwierigkeiten stoßen, den Umfang der Zweckidentität festzustellen. Eine abschließende Grenzziehung für jeden in der Praxis denkbaren Fall durch das Gesetz ist nicht möglich, insofern wird für besonders gelagerte Fälle die Praxis der Verwaltung und der Gerichte die erforderliche Abgrenzung vornehmen müssen. Es besteht aber keine Veranlassung, die Zweckidentität nach zu engen Kriterien zu bestimmen. Da der Zweck einer jeden Datenverarbeitung im Regelfall die Erreichung fachlicher Ziele ist, muss sich die Bestimmung einer Zweckidentität maßgebend nach der Art der fachlichen Aufgaben richten; es ist damit zunächst Aufgabe der öffentlichen Stelle, eine fachbezogene Abgrenzung vorzunehmen. Zweckidentität besteht z.B. in folgenden Fällen:

– Vorrangig zu nennen sind die Annexfälle. In den Zusammenhang einer Fachaufgabe gehören z.B. die Abwicklung von Schadensersatzansprüchen aus Anlass dieser Tätigkeit, die Beauftragung und Information von Rechtsanwälten, die Hinzuziehung von Sachverständigen, die Abrechnung der Kosten eines Verwaltungs- oder Gerichtsverfahrens.
– In behördlichen Abstimmungsverfahren, z.B. Planfeststellungen, haben mehrere öffentliche Stellen ihre fachlichen Ziele und Erfahrungen zu dem einen Zweck zusammenzufassen, die Zulässigkeit einer Maßnahme festzustellen (vgl. die deklaratorische Aussage in §14 Absatz 1 Satz 2).
– Zweckidentität besteht zwischen einer Gewerbeanmeldung und einer späteren erneuten Anmeldung für eine anderes Gewerbe.
– Ein Betrieb mit mehreren Produktgruppen ist auf Grund verschiedener Rechtsvorschriften zu überwachen; die aus diesem Anlass zu den verschiedenen Bereichen verarbeiteten Daten dienen dem gleichen Zweck, soweit die Zuverlässigkeit des Betreibers zu beurteilen ist.
– Zu dem behördlichen Zweck, Sorge für eine handlungsunfähige Person zu tragen, gehört die Information der Angehörigen über den Aufenthalt und Zustand der Person.
– Der Streifenbeamte der Polizei verarbeitet (als Handeln im ersten Zugriff) Daten auch für die Zwecke derjenigen Ordnungsbehörden, die fachliche Aufgaben im Zusammenhang mit den festgestellten Gefahr für die öffentliche Sicherheit und Ordnung wahrnehmen.
– Bei der Betreuung durch die Gesundheitsverwaltung wird es auf die Umstände ankommen, ob die betroffenen Bürger sich zu einem bestimmten Zweck (z.B. Betreuung allein der Körperbehinderung) oder zu einer umfassenden Betreuung in die Obhut der Verwaltung begeben.

Nach Absatz 2 Satz 1 ist die mit einer Zweckänderung verbundene Verarbeitung personenbezogener Daten nur bei Vorliegen besonderer eng begrenzter Ausnahmetatbestände zulässig. Die zulässigen Ausnahmen vom Zweckbindungsgebot sind in den Nummern 1 bis 8 aufgezählt.

Zulässig ist danach eine Zweckänderung – außer in denjenigen Fällen, in denen die Betroffenen ihre Einwilligung erteilt haben (die Anforderungen an eine rechtswirksame Einwilligung sind in §5 Absatz 2 niedergelegt) – nach Nummer 1 in den Fällen, in denen eine Rechtsvorschrift dies ausdrücklich erlaubt, ferner in den Fällen, in denen die Wahrnehmung einer durch Gesetz oder Rechtsverordnung begründeten Aufgabe die Verarbeitung ganz bestimmter personenbezogener Daten zwingend voraussetzt. Die Vorschrift soll den öffentlichen Stellen nicht prinzipiell die Möglichkeit einräumen, etwa ohne bereichsspezifische Normen Datenverarbeitung betreiben zu dürfen, sondern sie nur in denjenigen Fällen zur Datenverarbeitung legitimieren, in denen der Zweck vorhandener Normen eine andere Interpretation ausschließt.

Nummer 2 berücksichtigt die rechtlichen Interessen der Freien und Hansestadt Hamburg z.B. als Gläubiger privatrechtlicher Forderungen. Sie soll nicht schlechter behandelt werden als ein privater Gläubiger, dem bei Vorliegen der gleichen Voraussetzungen personenbezogene Daten übermittelt werden.

Nach Nummer 3 dürfen personenbezogene Daten, die zu einem anderen Zweck gespeichert sind oder übermittelt werden, von der Behörde zur Überprüfung von Angaben der Betroffenen verwendet werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Angaben unrichtig sind. In diesen Fällen wird dem Grundsatz rechtmäßiger

Aufgabenerfüllung Priorität zuerkannt. Dies liegt auch im Interesse der Betroffenen, die sich sonst möglicherweise später Erstattungsansprüchen oder sonstigen Maßnahmen der öffentlichen Verwaltung ausgesetzt sehen.

Eine Zweckbindung entfällt nach Nummer 4, wenn es gilt, erhebliche Nachteile für das Gemeinwohl – dazu gehört auch die öffentliche Sicherheit und Ordnung – abzuwehren. In der Regel wird hierbei allerdings als Rechtsgrundlage eine bereichsspezifische Bestimmung vorrangig eingreifen. Andererseits können sich aus bereichsspezifischen abschließenden Regelungen, z.B. dem SGB X, insoweit auch gewisse Einschränkungen ergeben. Die Zweckbindung ist ebenfalls aufgehoben zum Schutze der Rechte einer anderen Person. Werden deren Rechte schwerwiegend gefährdet (z.B. Leib, Leben, Freiheit, aber auch wesentliche Vermögensinteressen), muss das Grundrecht der Betroffenen auf informationelle Selbstbestimmung zurücktreten.

Nummer 5 sieht Durchbrechungen der Zweckbindung vor, die die Verfolgung von Straftaten oder Ordnungswidrigkeiten, die Strafvollstreckung oder den Strafvollzug und weitere gerichtliche Maßnahmen ermöglichen sollen. Für die rechtspflegende Tätigkeit der Gerichte bleiben insoweit allein die besonderen gesetzlichen Verfahrensvorschriften (z.B. der Strafprozessordnung) maßgeblich.

Mit der Regelung in Nummer 6 soll die anderweitige Nutzung bereits bei der öffentlichen Stelle vorhandener personenbezogener Daten in solchen Fällen ermöglicht werden, in denen die Verarbeitung der personenbezogenen Daten nach pflichtgemäßer Prüfung offensichtlich im Interesse der Betroffenen liegt, Nachteile für diese nicht zu befürchten sind und deshalb davon ausgegangen werden kann, dass diese ihre Einwilligung zur Zweckänderung erteilen würden. Aber auch in diesen Fällen muss die Verwaltung sich darum bemühen, zunächst die Einwilligung der Betroffenen zu erlangen.

Eine Zweckänderung bei der Verarbeitung gespeicherter Daten ist auch in denjenigen Fällen zulässig (Nummer 7), in denen die Daten von der öffentlichen Stelle unmittelbar aus allgemein zugänglichen Quellen entnommen wurden oder werden können oder die Daten verarbeitende Stelle sie veröffentlichen dürfte. Da die in Betracht kommenden Daten bereits in der Öffentlichkeit verfügbar sind oder publiziert werden dürfen, bestehen keine Bedenken, wenn unter diesen Voraussetzungen eine Zweckänderung zugelassen wird; gleichwohl ist dies in denjenigen Fällen unzulässig, in denen das Geheimhaltungsinteresse der Betroffenen einer solchen Verwendung der Daten offensichtlich entgegensteht.

Die in Nummer 8 geregelte Bearbeitung von Eingaben sowie von Großen und Kleinen Anfragen ist eingebettet in den Kontrollauftrag der Bürgerschaft und dient da mit regelmäßig einem anderen Zweck als die zugrunde liegende Verwaltungsaufgabe. Der hohe Wert der parlamentarischen Aufgabe rechtfertigt den Eingriff in das Grundrecht auf informationelle Selbstbestimmung, zumal dieser Eingriff z.B. bei Ein gaben an die Bürgerschaft dem Interesse der Petenten entspricht. Die Formulierung berücksichtigt zugleich, dass schutzwürdige Belange anderer Personen (z.B. bei der Behauptung einer Ungleichbehandlung gegenüber sonstigen Personen) der Zweckdurchbrechung entgegenstehen können. Nummer 8 regelt lediglich die Zuarbeit der Verwaltung an die Bürgerschaft, während die Bearbeitung in der Bürgerschaft selbst sich nach der Datenschutzordnung der Hamburgischen Bürgerschaft vom 19. Oktober 1999 (HmbGVBl. S. 243) bestimmt. Der Anwendungsbereich der Nummer 8 erfasst auch Eingaben an den Bürgermeister und an die Behördenleitungen.

Nach Absatz 2 Satz 2 kommt eine Zweckänderung bei amtlich zur Verfügung gestellten personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, wegen ihrer besonderen Sensibilität ohne Einwilligung der Betroffenen und ohne Rechtsnorm nicht in Betracht. Die Formulierung „zur Verfügung gestellt“ berücksichtigt, dass es auch Fälle gibt, in denen die zur Verschwiegenheit verpflichtete Person derjenigen Daten verarbeitenden Stelle angehört, um deren weitere Datenverarbeitungsbefugnis es in §13 geht; innerhalb einer öffentlichen Stelle gibt es aber gemäß §4 Absatz 2 Satz 2 Nummer 4 und Absatz 4 begrifflich keine Übermittlung. Der Schutz besonders sensibler Daten genießt nunmehr auch in den Fällen des Satzes 1 Nummer 8 Vorrang.

Absatz 3 stellt klar, dass die Nutzung personenbezogener Daten im Rahmen von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung (dazu gehört auch die Vorprüfung nach §100 LHO und §56 Absatz 3 HGrG) oder auch von Organisationsuntersuchungen nicht als Zweckänderung anzusehen ist. Die angesprochenen Tätigkeiten sind einer rechtmäßigen Aufgabenerfüllung der Verwaltung notwendig akzessorisch und stellen keine spürbare Gefährdung des Grundrechts auf informationelle Selbstbestimmung dar. Zulässig ist auch grundsätzlich die Verarbeitung personenbezogener Daten im Rahmen von Ausbildungs- und Prüfungszwecken, zumal in diesen Fällen ein eigentliches Interesse an dem Personenbezug der Daten nicht besteht.

Zu §14 (Übermittlung innerhalb des öffentlichen Bereichs)

Die Übermittlungsregelungen des Gesetzes orientieren sich – dies gilt insbesondere für den Nachrichtenaustausch von Behörden – an dem aus dem Grundrecht auf informationelle Selbstbestimmung abzuleitenden Zweckbindungsgebot. So weit nicht bereichsspezifische gesetzliche Vorschriften etwas anderes bestimmen, ist eine gegenseitige Informationshilfe öffentlicher Stellen unter Durchbrechung der Zweckbindung nur unter den in dieser Vorschrift aufgeführten Voraussetzungen zulässig.

Absatz 1 Satz 1 setzt zunächst voraus, dass die Datenübermittlung im Rahmen der Aufgabenerledigung der übermittelnden Stelle oder der Stelle, der die Daten übermittelt werden, erforderlich ist. Darüber hinaus müssen jedoch für die Übermittlung weitere Zulässigkeitsvoraussetzungen gegeben sein: Die Datenübermittlung ist zunächst zulässig, wenn Zweckidentität zwischen der Speicherung und der weiteren Verarbeitung nach §13 Absatz 1 besteht, wenn also die übermittelnde Stelle oder die Stelle, der die Daten übermittelt werden, eine Aufgabe erfüllen, die sich mit dem Speicherungszweck deckt. Liegen diese Voraussetzungen nicht vor, so ist gleichwohl eine Datenübermittlung zugunsten der Stelle, der die Daten übermittelt werden, zulässig, wenn die Zweckänderung nach den Ausnahmevorschriften des §13 Absatz 2 Satz 1 legitimiert ist. Für die Betroffenen macht es nämlich keinen prinzipiellen Unterschied, ob eine öffentliche Stelle erhobene Daten zu anderen Zwecken selbst verarbeitet oder ob die Zweckänderung in der Weise geschieht, dass diese Daten an eine andere öffentliche Stelle zur rechtmäßigen Aufgabenerfüllung übermittelt werden.

Die Verweisung auf die Voraussetzungen des §13 bedeutet für die Zulässigkeit der Übermittlung von personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (§13 Absatz 2 Satz 2), dass die Übermittlung zur rechtmäßigen Aufgabenerfüllung erforderlich sein muss und zusätzlich entweder die Voraussetzung des §13 Absatz 1 – die Stelle, der die Daten übermittelt werden, benötigt die Daten zur Erfüllung des gleichen Zwecks, zu dem sie die übermittelnde Stelle erhalten hat – oder die Voraussetzungen nach §13 Absatz 2 Satz 1 Nummer 1 oder Nummer 2 erfüllt sein müssen.

Die Weitergabe von Daten zur Wahrnehmung der in §13 Absatz 3 erwähnten Aufgaben ist – sofern dienlich – immer zulässig, da insoweit keine Verarbeitung und damit auch keine Übermittlung vorliegt.

Die in Absatz 1 Satz 2 vorgesehene Regelung entspricht den Erfordernissen komplexer Verwaltungsverfahren, bei denen mehrere öffentliche Stellen an einem Entscheidungsprozess beteiligt sind. Die Beteiligung kann durch Gesetz oder durch Verwaltungsvorschrift, z.B. durch Organisationsanordnung des Senats nach Artikel 57 Satz 2 der Hamburger Verfassung, vorgeschrieben sein. Die Regelung des Satzes 2 ist im Grunde nur eine deklaratorische Klarstellung. Der Begriff des Verwaltungsverfahrens ist hier weiter als in §9 HmbVwVfG.

Absatz 2 trägt den Besonderheiten bei der Übermittlung personenbezogener Daten in und aus Akten Rechnung. Während sich bei automatisierter Datenverarbeitung in der Regel diejenigen Daten aussondern lassen, die zur jeweiligen Aufgabenerfüllung nicht erforderlich sind und deshalb nicht übermittelt werden dürfen, ist eine solche Trennung bei Akten nicht ohne weiteres möglich. Statt dessen muss eine Vielzahl aktuell nicht relevanter personenbezogener Daten während der Bearbeitung zur Kenntnis genommen, übermittelt oder innerhalb der Daten verarbeitenden Stelle weitergegeben werden, weil diese untrennbar mit Daten verbunden sind, deren Verarbeitung für die jeweilige Aufgabenerfüllung erforderlich ist. Diese Problematik ist von besonderer Bedeutung bei der Übermittlungsphase. Soweit daher nicht berechtigte Interessen der Betroffenen oder Dritter an der Geheimhaltung der für die Bearbeitung nicht erforderlichen Daten offensichtlich überwiegen, soll die Übermittlung vollständiger Aktenunterlagen zulässig sein; bezüglich der nicht zur Aufgabenerfüllung erforderlichen personenbezogenen Daten gilt allerdings ein Verwertungsverbot.

Absatz 3 regelt die Verantwortlichkeit für die datenschutzrechtliche Zulässigkeit von Datenflüssen zwischen öffentlichen Stellen. Nach Satz 1 trägt grundsätzlich die übermittelnde Stelle die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten, es sei denn, sie wird von der Stelle, der die Daten übermittelt werden sollen, um die Übermittlung ersucht. In diesem Fall kann der übermittelnden Stelle in der Regel keine Verantwortung für eine Entscheidung aufgebürdet werden, deren Notwendigkeit und Auswirkungen sie nicht beurteilen kann. Sie hat daher im Ersuchensfall nur die Plausibilität des Übermittlungsersuchens zu prüfen (Satz 2). Die Vorschrift des Satzes 2 bezieht sich allerdings nur auf die in der Sphäre der ersuchenden Stelle liegenden Zulässigkeitsvoraussetzungen (z.B. die Erforderlichkeit, d.h. der Informationsbedarf im konkreten Fall). Dagegen bleibt es für diejenigen Übermittlungsvoraussetzungen, die in die Sphäre der übermittelnden Stelle fallen, bei deren Verantwortung (z.B. Prüfung, ob an die ersuchende Stelle überhaupt übermittelt werden darf; Vornahme einer ggf. vorgeschriebenen Interessenabwägung etc.). Eine andere Auslegung würde letztlich mit Amtshilfeerwägungen die im Einzelnen geregelten Bestimmungen über die Zulässigkeit der Datenübermittlung überspielen und damit gegen eine Grundregel

des Datenschutzrechtes verstoßen, nämlich den Grundsatz der Amtshilfefestigkeit der Datenverwendungsregelungen (vgl. BVerfGE 65, 1, 46).

Die übermittelnde Stelle muss ferner die Zulässigkeit der Übermittlung prüfen, wenn sie im Einzelfall Anhaltspunkte besitzt, an der Rechtmäßigkeit des Ersuchens zu zweifeln. In diesem Fall besteht für die ersuchende Stelle eine besondere Informationsverpflichtung (Satz 3). Bei Abruf in einem automatisierten Verfahren (§§11, 11a) trägt die abrufende Stelle die (alleinige) Verantwortung für die Rechtmäßigkeit des Abrufs (Satz 4).

Die Datenweitergabe innerhalb einer Daten verarbeitenden Stelle ist keine Übermittlung i. S. d. §4 Absatz 2 Satz 2 Nummer 4. Gefahren für das Grundrecht auf informationelle Selbstbestimmung können dadurch nicht entstehen, da die Weitergabe eine Vorstufe zur Nutzung durch die anderen Einheiten innerhalb der Daten verarbeitenden Stelle darstellt und nur im Rahmen des §13 zulässig ist. Absatz 4 sieht aber in Anpassung an die Besonderheiten der Datenverarbeitung in Akten eine Vereinfachung vor: Akten können unter den Voraussetzungen des Absatzes 2 auch dann weitergegeben werden, wenn sie nicht benötigte Daten enthalten.

Zu §15 (Übermittlung an öffentlich-rechtliche Religionsgesellschaften)

Bei der Anwendung dieser Vorschrift ist §14 in Verbindung mit §13 zu beachten. Die vom Gesetz geforderte Zweckbindung ist in diesen Fällen gewahrt, wenn die Stelle, der die Daten übermittelt werden sollen, den Verwendungszweck der angeforderten Daten angibt und sich verpflichtet, diese nur für den angegebenen Zweck zu verwenden.

Zusätzlich muss geprüft werden, ob die öffentlich-rechtliche Religionsgesellschaft ausreichende Datenschutzmaßnahmen, die im Ergebnis mit den Regelungen des Hamburgischen Datenschutzgesetzes vergleichbar sind, getroffen hat. Sofern Kirchen Datenschutzregelungen erlassen haben, die im Wesentlichen den staatlichen Datenschutzgesetzen entsprechen, kann von gleichwertigen Datenschutzmaßnahmen ausgegangen werden; Religionsgesellschaften können nach Artikel 140 Grundgesetz in Verbindung mit Artikel 137 Absatz 3 Weimarer Verfassung „ihre Angelegenheiten selbstständig innerhalb der Schranken des für alle geltenden Gesetzes“ ordnen.

Ist dieses nicht der Fall oder liegt weder eine allgemeine förmliche noch eine spezialgesetzliche Feststellung über ausreichende Datenschutzvorhaben vor, sind solche Maßnahmen vor jeder Datenübermittlung im Einzelfall – insbesondere anhand einer nachprüfbaren Erklärung der Stelle, der die Daten übermittelt werden sollen, – nachzuweisen.

Zu §16 (Übermittlung an Stellen außerhalb des öffentlichen Bereichs)

Die Vorschrift stellt auf die im Vergleich zu §§14 und 15 unterschiedliche Interessenlage bei der Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs ab.

In Absatz 1 Satz 1 Nummer 1 wird eine Übermittlung entsprechend der Regelung in §14 Absatz 1 Satz 1 an die Erforderlichkeit und an das Zweckbindungsgebot in §13 Absatz 1 gebunden.

In Absatz 1 Satz 1 Nummer 2 ist geregelt, dass solche Datenübermittlungen auch dann zulässig sind, wenn die Voraussetzungen des §13 Absatz 2 Satz 1 Nummern 1, 4, 6, 7 oder 8 erfüllt sind, weil hier das Grundrecht auf informationelle Selbstbestimmung zurückzutreten hat oder nur unwesentlich berührt wird. Soweit einem Berufs- oder besonderen Amtsgeheimnis unterliegende personenbezogene Daten betroffen sind, ist allerdings wegen §13 Absatz 2 Satz 2 eine Übermittlung in den Fällen des §13 Absatz 2 Satz 1 Nummern 4, 6, 7 und 8 nicht zulässig (vgl. die Erläuterung zu §13).

Nach Absatz 1 Satz 1 Nummer 4 ist eine Übermittlung weiterhin in zwei Fällen zulässig: Entweder besteht ein öffentliches Interesse an der Übermittlung oder der Dritte macht ein berechtigtes Interesse an der Übermittlung geltend; in beiden Fällen ist den Betroffenen vorher die qualifizierte (vgl. Satz 2) Gelegenheit zu einem die Verwaltung dann bindenden Widerspruch zu geben.

Bereichsspezifische Sonderregelungen (z.B. für Auskünfte aus öffentlichen Registern) bleiben unberührt.

Regelungen für die Übermittlung an Behörden oder Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen sind in einer selbstständigen Vorschrift enthalten (vgl. §17).

Die übermittelnde Stelle hat die Stelle, der die Daten übermittelt werden, darauf hinzuweisen, dass sie die Daten nur

für den Zweck erhält, zu dem sie ihr übermittelt werden.

Zu §17 (Übermittlung an Stellen außerhalb der Bundesrepublik Deutschland)

Nach Absatz 1 gelten die Übermittlungsregelungen des Hamburgischen Datenschutzgesetzes für innerstaatliche Übermittlungen auch für Übermittlungen in Mitgliedstaaten der Europäischen Union und an Organe und Einrichtungen der Europäischen Union. Neben den allgemeinen Übermittlungsbestimmungen der §§14 und 16 war dabei auch §28 zu nennen, der für Beschäftigtendaten bereichsspezifische Übermittlungsvorschriften enthält. Mit der Gleichstellung innerstaatlicher und EU-weiter Übermittlungen wird dem Artikel 1 Absatz 2 der EG-Datenschutzrichtlinie Rechnung getragen. Danach sind Übermittlungsbeschränkungen aus Datenschutzgründen im Datenverkehr unter den Mitgliedstaaten nicht mehr zulässig.

Die Gleichstellung der innerstaatlichen mit den EU-weiten Übermittlungen erstreckt sich grundsätzlich auf die Mitgliedstaaten und Organisationen und Einrichtungen der Europäischen Union unabhängig davon, ob sich eine Datenübermittlung im Anwendungsbereich der EG-Datenschutzrichtlinie bewegt. Diese Generalisierung nimmt Rücksicht darauf, dass eine Differenzierung zwischen Daten im Anwendungsbereich und außerhalb des Anwendungsbereiches dieser Richtlinie die Rechtsanwender in vielen konkreten Einzelfällen überfordern dürfte. Andererseits erscheint die Gleichstellung auch außerhalb des Anwendungsbereichs der Richtlinie angesichts des festzustellenden Zusammenwachsens der europäischen Rechtsordnungen generell vertretbar. Dies gilt jedenfalls für Daten, die in den Geltungsbereich des Hamburgischen Datenschutzgesetzes fallen und nicht wegen ihrer Sensibilität oder der Sensibilität des jeweiligen Verarbeitungszusammenhangs von vornherein nur einer bereichsspezifischen Regelung zugänglich sind. Im Übrigen stellen die Übermittlungsvorschriften des Hamburgischen Datenschutzgesetzes Übermittlungsermächtigungen dar, ziehen aber keine Übermittlungspflichten nach sich, so dass eine Datenübermittlung außerhalb des Anwendungsbereichs der EG-Datenschutzrichtlinie im Rahmen der Ermessensausübung versagt werden kann (und unter Umständen auch muss), wenn im Einzelfall Anlass zu der Annahme besteht, dass mangelnder Datenschutz in dem empfangenden EU-Mitgliedstaat zu einer ungerechtfertigten Beeinträchtigung der Rechte Betroffener führen würde. Dasselbe gilt für Datenübermittlungen im Anwendungsbereich der EG-Datenschutzrichtlinie in Länder, die die Richtlinie nicht oder nicht vollständig umgesetzt haben.

In Umsetzung des Artikels 25 Absatz 2 der EG-Datenschutzrichtlinie stellt Absatz 2 die Übermittlungen in Drittländer mit einem angemessenen Schutzniveau den innerstaatlichen und EU-weiten Übermittlungen gleich (siehe die Erläuterungen zu Absatz 1). Die Angemessenheit des Schutzniveaus ist unter Berücksichtigung aller Umstände zu beurteilen, die für die Datenübermittlung von Bedeutung sind. Zu hoffen ist, dass die Feststellung eines angemessenen Schutzniveaus in den praktisch häufigen und bedeutsamen Fällen nach Artikel 25 Absatz 6 der EG-Datenschutzrichtlinie durch die Kommission erfolgen und die Einzelfallprüfung entlasten wird.

Absatz 3 regelt die Datenübermittlung in Drittländer ohne angemessenes Schutzniveau nach Maßgabe des Artikels 26 der EG-Datenschutzrichtlinie. Die – engen – Übermittlungsvoraussetzungen des Satzes 1, mit dem Artikel 26 Absatz 1 der Richtlinie umgesetzt wird, sind abschließend, während die Übermittlung nach Satz 2, der in Verbindung mit den Sätzen 3 bis 5 den Artikel 26 Absatz 2 der Richtlinie umsetzt, wiederum lediglich nach Maßgabe der innerstaatlichen Übermittlungsregelungen zulässig sind. Die Zulassung der Übermittlung nach Satz 3 (Genehmigung im Sinne von Artikel 26 Absatz 2 der Datenschutzrichtlinie) kann sich auf eine einzelne Übermittlung oder auf eine Kategorie von Übermittlungen beziehen. Die besonderen Regularien der Zulassung liegen in den von ihr ausgelösten Folgen (vgl. Artikel 26 Absatz 3 der EG-Datenschutzrichtlinie) begründet. Die Mitteilung zu gelassener Übermittlungen an eine zuständige Behörde ist erforderlich, um das Meldewesen nach Artikel 26 Absatz 3 der EG-Datenschutzrichtlinie sicherzustellen.

Zu §18 (Auskunft)

Der Auskunftsanspruch Betroffener gehört zu den wesentlichen Datenschutzrechten der Bürger. Um die Bedeutung dieser Rechte angemessen hervorzuheben, sieht das Gesetz einen eigenen (Dritten) Abschnitt für die Rechte der Betroffenen vor. Die differenziert gestaltete Vorschrift über das Auskunftsrecht hat sich zum Ziel gesetzt, die Rechtsstellung der Betroffenen zu verbessern. Mehr Transparenz im Rahmen der Datenverarbeitung soll dazu beitragen, die geeigneten Voraussetzungen zu schaffen, dass die Betroffenen ihre sonstigen Rechte auf Grund dieses Gesetzes wirksam geltend machen können. Dazu gehört auch, dass sie die sie betreffenden Informationen gebührenfrei erhalten.

Das Auskunftsrecht erstreckt sich über die zur Person in Dateien und Akten gespeicherten Daten (Absatz 1 Satz 1

Nummer 1) hinaus auf die Zweckbestimmungen und die Rechtsgrundlage der Speicherung der Daten (Nummer 2), die Herkunft der Daten und die Empfängerinnen oder Empfänger oder den Kreis der Empfängerinnen und Empfänger, soweit sie die Daten nicht im Einzelfall zur Verfolgung von Straftaten, Ordnungswidrigkeiten oder berufsrechtlichen Vergehen erhalten (Nummer 3), die an einem automatisierten Abrufverfahren teilnehmenden Stellen (Nummer 4) sowie in den Fällen des §5a auf den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten (Nummer 5).

Wegen Artikel 12 Buchstabe a 1. Spiegelstrich der EG-Datenschutzrichtlinie ist grundsätzlich über sämtliche Empfängerinnen und Empfänger oder Empfängerkreise Auskunft zu geben (Nummer 3). Die Entscheidung, einzelne Empfängerinnen oder Empfänger oder aber Empfängerkreise zu benennen, trifft die Auskunft erteilende Stelle. Die Daten verarbeitenden Stellen haben Übermittlungen personenbezogener Daten in jedem Einzelfall zuverlässig zu dokumentieren, soweit dies erforderlich ist, um den Betroffenen Auskunft über die Empfängerinnen oder Empfänger erteilen zu können. Die Beschränkung der Auskunft im Hinblick auf Empfängerinnen und Empfänger, die Daten im Einzelfall zur Verfolgung von Straftaten, Ordnungswidrigkeiten oder berufsrechtlichen Vergehen erhalten, beruht auf Artikel 2 Buchstabe g der EG-Datenschutzrichtlinie, der diese Stellen bereits generell aus dem Empfängerbegriff ausklammert. Diese Ausklammerung vollzieht das Gesetz zwar nicht nach, nimmt die Benennung der entsprechenden Empfänge rinnen und Empfänger aber von der Auskunft aus. Dies erscheint geboten, da so einerseits das Risiko der ungewollten Gefährdung von Ermittlungen ausgeschlossen wird und andererseits den Betroffenen im Rahmen von Ermittlungen besonders geregelte Rechte z.B. strafprozessualer Art zustehen, die die Wahrung ihrer – auch informationellen – Belange hinreichend sicherstellen.

Nummer 5 setzt Artikel 12 Buchstabe a 3. Spiegelstrich der EG-Datenschutzrichtlinie um. Die Auskunft muss sich nicht auf sämtliche durch die eingesetzte Software ermöglichten Verarbeitungen beziehen, sondern nur auf die tatsächlich vorgesehenen bzw. praktizierten Verarbeitungen. Die Auskunft über den logischen Aufbau der Verarbeitung erfordert keine softwaretechnischen Erörterungen, sondern allgemein verständliche Darlegungen darüber, in welcher Weise aus den konkret verarbeiteten personenbezogenen Daten welche Bewertungen von Persönlichkeits- oder Verhaltensmerkmalen gewonnen und welche Entscheidungskriterien dabei herangezogen werden.

Die Auskunftspflicht nach §18 kann sich naturgemäß nur auf solche Daten erstrecken, die auch gespeichert sind. Eine Pflicht, die Herkunft von Daten zu speichern, wird durch dieses Gesetz nicht begründet. Das Auskunftsverfahren ist bei Akten aus Gründen der Verwaltungspraktikabilität (Auffindbarkeit) an qualifizierte Voraussetzungen gebunden (Satz 3). Die Betroffenen müssen wegen des sachnotwendig größeren Verwaltungsaufwandes bei Auskunftsbegehren aus Akten jedenfalls so konkrete Angaben machen, dass die Daten aufgefunden werden können; der zu leistende Aufwand darf dabei nicht außer Verhältnis zu dem nicht näher begründeten oder dem im Einzelfall dargelegten Informationsinteresse stehen.

Die Regelung in Absatz 1 Satz 4, 2. Halbsatz über die Gewährung der Akteneinsicht oder einen Ausdruck stellt klar, dass aus der Erwähnung von §29 in Satz 5 nicht der Gegenschluss gezogen werden darf, der Daten verarbeitenden Stelle sei außerhalb eines Verwaltungsverfahrens eine Auskunftserteilung im Wege der Akteneinsicht verwehrt. Hierüber entscheidet sie vielmehr nach pflichtgemäßem Ermessen. Die öffentlichen Stellen werden nach ihrem Ermessen das Informationsinteresse der Betroffenen an einer Akteneinsicht oder an einem Ausdruck insbesondere dann erfüllen, wenn es einem wirtschaftlichen Verwaltungshandeln dient. Sind in einer Akte Daten von Betroffenen mit Daten Dritter oder mit sonstigen geheimhaltungsbedürftigen Angaben derart verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre, kommt eine Akteneinsicht allerdings in der Regel nicht in Betracht. Die Regelungen des §29 HmbVwVfG über die Akteneinsicht durch Verfahrensbeteiligte gehen aber unter den entsprechenden Voraussetzungen vor (Satz 5).

Absatz 2 enthält die Ausnahmen von der Auskunftspflicht; sie erstrecken sich auf ausschließlich zum Zwecke der Datensicherung oder der Datenschutzkontrolle gespeicherte Daten und auf gesperrte, nicht mehr benötigte Daten, die auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen. In diesen Fällen ist eine Auskunftspflicht entbehrlich, da die Daten ohne sonderliches Interesse für die Betroffenen sind und auch nicht mehr weiterverarbeitet werden dürfen.

In Absatz 3 sind die Ausnahmen von der Auskunftserteilung an die Ausnahmegründe des Artikels 13 der EG-Datenschutzrichtlinie angepasst worden. Da diese Ausnahmegründe bereits im Zusammenhang mit der Unterrichtung nach §12a zu beachten sind, war eine Verweisung auf §12a Absatz 3 Satz 2 insoweit möglich, als die dortigen Ausnahmegründe auf Artikel 13 der EG-Datenschutzrichtlinie beruhen. Die darüber hinausgehende Ausnahme für

Verarbeitungen zu wissenschaftlichen oder statistischen Zwecken beruht auf Artikel 13 Absatz 2 der EG-Datenschutzrichtlinie.

Nach Absatz 4 bedarf die Auskunftsverweigerung grundsätzlich einer Begründung. Wird die Auskunft zu Recht verweigert und ist eine Offenlegung der Gründe gegenüber den Betroffenen nicht möglich, so sind die wesentlichen Gründe für diese Entscheidung in einer Weise zu dokumentieren, die eine Nachprüfung durch die zuständigen Stellen, in der Regel durch die bzw. den Hamburgischen Datenschutzbeauftragten ermöglicht.

Eine Sonderregelung enthält Absatz 5: Danach sind Auskunftserteilung und Akteneinsichtsgewährung durch öffentliche Stellen über die Herkunft personenbezogener Daten von den Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, unter bestimmten Voraussetzungen von den Landesfinanzbehörden sowie von den in §19 Absatz 3 BDSG aufgeführten Dienststellen des Bundes im Sicherheitsbereich nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten an diese Behörden. Die Verweisung auf das BDSG umfasst „Verfassungsschutzbehörden, den Bundesnachrichtendienst, den militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung“. Damit wird bei prinzipieller Anerkennung des Auskunftsrechts der Notwendigkeit Rechnung getragen, dass über solche Auskunftsbegehren letztlich nur die in der Sache betroffenen Stellen entscheiden können (z.B. im Interesse des Quellenschutzes); bei der Versagung der Zustimmung gelten aber die Absätze 3 und 4 entsprechend, soweit es sich um Landesbehörden handelt.

Absatz 6 stellt sicher, dass die Betroffenen mit Hilfe der bzw. des Hamburgischen Datenschutzbeauftragten eine Nachprüfung der Auskunftsverweigerung erreichen können. Dies gilt nach Auffassung des Hamburgischen Datenschutzbeauftragten auch dann, wenn die Auskunft entgegen dem Antrag der Betroffenen nicht im Wege der Akteneinsicht oder der Überlassung eines Ausdrucks aus automatisierten Dateien erteilt wird.

Zu §19 (Berichtigung, Sperrung und Löschung)

Die Vorschrift regelt die Rechtsposition der Betroffenen bei den Korrekturansprüchen. Von besonderer Bedeutung ist die obligatorische Löschungsverpflichtung für die Daten verarbeitenden öffentlichen Stellen in den Fällen, in denen die Kenntnis der Daten für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

In Absatz 1 bedeutet „zu berichtigen“, dass die gespeicherten Daten in Übereinstimmung mit der Realität gebracht werden müssen. Dies kann durch eine Veränderung (inhaltliche Umgestaltung der gespeicherten Daten), eine ganze oder teilweise Löschung oder durch die Speicherung ergänzender (bei Unvollständigkeit), neu erhobener (Fortschreibung) oder der berichtigten Angaben (bei ursprünglicher Unrichtigkeit) geschehen. Bei der automatisierten Datenverarbeitung ist in der Regel das unrichtige Datum zu verändern, doch ist bei entsprechender Interessenlage auch die lediglich ergänzende Speicherung des richtigen Datums geboten; in manchen Fällen wäre den Betroffenen (z.B. bei der beabsichtigten Verfolgung von Schadensersatzansprüchen) nicht damit gedient, wenn das später als fehlerhaft erkannte Datum einfach durch das richtige Datum ersetzt wird. Ein modifiziertes Berichtigungsverfahren schreibt Satz 2 für die Daten außerhalb automatisierter Dateien vor, ohne jedoch Art und Weise vorzugeben. Bei Akten soll die Berichtigung in der Weise gestaltet werden, wie Schutzzweck der Norm und Eigenart der jeweiligen Akte es am sinnvollsten erscheinen lassen. Deshalb braucht z.B. ein in umfangreichen Akten mehrfach enthaltenes personenbezogenes Datum nicht an jeder einzelnen Stelle berichtigt zu werden, dies kann auch durch einen der Akte vorangestellten Vermerk geschehen.

In Absatz 2 Satz 1 Nummern 1 bis 3 sind die Sperrungsfälle definiert: Nach Nummer 1 müssen die Betroffenen substantiiert die Richtigkeit bestreiten. Die bloße Behauptung, die gespeicherten Daten seien unrichtig, zwingen die Daten verarbeitende Stelle nicht zu einer Überprüfung oder gar Sperrung des Datenbestandes. Eine Sperrung nach Nummer 2 kommt angesichts der obligatorischen Löschungsverpflichtung nach Absatz 3 Nummer 1 nur in zwei Fallgruppen in Betracht. Die erste Fallgruppe umfasst die Fälle, in denen die Daten verarbeitende Stelle davon ausgehen muss, dass die Verwirklichung ihrer obligatorischen Löschungspflicht nach Absatz 3 dem Interesse der Betroffenen nicht entspricht, weil für sie die Möglichkeit, noch auf die Daten zugreifen zu können, als vorrangig angesehen werden muss. In der zweiten Fallgruppe müssen die Betroffenen ausdrücklich an Stelle der Löschung die Sperrung verlangt haben (erklärter Wille). Ein Anspruch der Betroffenen auf Sperrung besteht ferner, wenn die personenbezogenen Daten nur zu Zwecken der Datensicherung und der Datenschutzkontrolle gespeichert sind (Nummer 3).

Absatz 2 Satz 2 berücksichtigt ein besonderes Erfordernis bei der Datenverarbeitung in Akten: Eine Sperrung bestrittener Daten in Akten wäre mit dem typischerweise aus der Aktenführung sich ergebenden Anliegen, den

Verfahrensgang und die damit zusammenhängende Darstellung der unterschiedlichen Bewertungen und Rechtsauffassungen von Behörden und Betroffenen zu dokumentieren, nicht vereinbar. In welcher Form Daten zu sperren sind, wird die Verwaltung im Einklang mit dem Schutzzweck der Norm nach Praktikabilität entscheiden. Das Sperren in Akten wird regelmäßig sachgerecht durch Stempelaufdruck oder in vergleichbarer Weise durchgeführt werden. In Satz 4 wurde als weiterer Ausnahmetatbestand die Unerlässlichkeit einer weiteren Bearbeitung nach Maßgabe einer Güterabwägung aufgenommen.

Nach Absatz 3 Satz 1 Nummer 1 sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist; das hier gebrauchte Präsens erfasst auch den Fall, dass nicht mehr nach heutiger, wohl aber nach früherer Rechts- und Tatsachenlage die Speicherung unzulässig war.

Eine Ausnahme von der Löschungspflicht nach Wegfall der Erforderlichkeit im Sinne von Absatz 3 Satz 1 Nummer 2 gilt für die Speicherung in Akten, wenn die Datenkenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist (Satz 2). Die Löschung wird nur dann durchgeführt, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr benötigt wird; wird sie noch benötigt, sind die jeweiligen Daten zu sperren.

In der Praxis der öffentlichen Stellen wird regelmäßig in Aufbewahrungsbestimmungen nach fachlicher Einschätzung festgelegt, für welchen Zeitraum die Aufbewahrung von Akten zur Aufgabenerfüllung (dazu gehört auch die externe Rechnungsprüfung) noch erforderlich ist.

Die obligatorische Verpflichtung der öffentlichen Stelle, nicht mehr zur Aufgabenerfüllung benötigte personenbezogene Daten in Dateien zu löschen, darf allerdings nicht das öffentliche Interesse an einer Überlieferung historisch gewordener Vorgänge an die Nachwelt unmöglich machen. Absatz 4 bringt deshalb zum Ausdruck, dass eine Anbietungspflicht an das zuständige Archiv besteht und die Löschung grundsätzlich erst nach Verneinung der Archivwürdigkeit erfolgen darf (Archivklausel). Eine Ausnahme besteht nur bezüglich von Daten, deren Speicherung unzulässig ist; dies stimmt mit §3 Absatz 2 Satz 2 HmbArchG überein. Zuständig ist in der Regel das Staatsarchiv, doch kommt nach Maßgabe des Hamburgischen Archivgesetzes auch ein von einem Träger mittelbarer Staatsverwaltung errichtetes Archiv in Betracht.

Absatz 5 begründet die Pflicht der Daten verarbeitenden Stelle, alle Stellen, denen die Daten übermittelt worden sind, unverzüglich von der Berichtigung, Sperrung oder Löschung zu benachrichtigen. Das Recht auf informationelle Selbstbestimmung der Betroffenen ist nur dann in angemessenem Umfang gewahrt, wenn die Stellen, denen solche Daten übermittelt worden sind, von den erforderlich gewordenen Korrekturen Kenntnis erlangen und sich entsprechend verhalten können.

Um einer erheblichen Überforderung der Verwaltung vorzubeugen, wird die Nachberichtspflicht allerdings insgesamt unter den Vorbehalt des unverhältnismäßigen Aufwandes gestellt. Andererseits haben die Daten verarbeitenden Stellen Übermittlungen in jedem Einzelfall zuverlässig zu dokumentieren, soweit dies erforderlich ist, um die Stellen, denen die Daten übermittelt worden sind, von der Berichtigung, Sperrung und Löschung personenbezogener Daten unverzüglich verständigen zu können. Die Nachberichtspflicht erfasst nicht die Fälle der Löschung nach Absatz 3 Satz 1 Nummer 2. Der Daten verarbeitenden Stelle steht insofern vielmehr nach Satz 2 ein Ermessen zu.

Die Regelung in Absatz 6 beschränkt die Pflicht zur regelmäßigen Überprüfung auf automatisierte Dateien.

Zu §20 (Schadensersatz)

Die Regelung setzt Artikel 23 der EG-Datenschutzrichtlinie um. Danach ist der Schadenersatzanspruch weder auf automatisierte Datenverarbeitungen beschränkt noch der Höhe nach begrenzt. Dafür haben die verantwortlichen Stellen die Möglichkeit, sich von der Schadenersatzpflicht teilweise oder vollständig zu befreien, wenn sie nachweisen, dass der Umstand, durch den der Schaden eingetreten ist, ihnen nicht zur Last gelegt werden kann (Artikel 23 Absatz 2 der EG-Datenschutzrichtlinie). Satz 3 sieht eine dementsprechende Exkulpationsmöglichkeit vor. Satz 4 gewährt einen der Höhe nach begrenzten, aber keiner Exkulpation zugänglichen Schadenersatzanspruch bei unzulässiger oder unrichtiger automatisierter Datenverarbeitung. Ein Mitverschulden der Betroffenen mindert entsprechend den BGB-Vorschriften die Haftung. Ebenso gelten die Verjährungsvorschriften des BGB entsprechend.

Zu §21 (Berufung)

Der institutionalisierten Fremdkontrolle wird durch das Amt der bzw. des Hamburgischen Datenschutzbeauftragten Rechnung getragen. Sie bzw. er ist Beamtin bzw. Beamter auf Zeit. Der Senat kann nur eine von der Bürgerschaft gewählte Kandidatin bzw. einen von der Bürgerschaft gewählten Kandidaten bestellen. Das Vorschlagsrecht des

Senats sichert ihm maßgeblichen Einfluss auf die Auswahl der bzw. des Datenschutzbeauftragten.

Nach der früheren Fassung des Absatzes 1 wurde der Hamburgische Datenschutzbeauftragte von der Bürgerschaft „mit mehr als der Hälfte der gesetzlichen Zahl ihrer Mitglieder“ gewählt. Diese Vorschrift stimmte nicht mit Artikel 19 Hamburger Verfassung überein, wonach zu einem Beschluss der Bürgerschaft die einfache Stimmenmehrheit erforderlich ist, sofern die Verfassung nicht ein anderes Stimmenverhältnis vorschreibt. Deshalb sind in der jetzigen Fassung des Absatzes 1 keine Aussagen über die Mehrheitsverhältnisse mehr enthalten, so dass die einfache Stimmenmehrheit erforderlich und ausreichend ist.

Die Zulässigkeit der Wiederwahl ermöglicht es, den Sachverstand und die Erfahrungen einer bzw. eines Datenschutzbeauftragten für eine zweite Amtszeit zu nutzen. Das Amt soll jedoch nicht als Dauertätigkeit wahrgenommen werden können.

Absatz 3 trägt der Notwendigkeit zur kontinuierlichen Aufgabenerfüllung Rechnung. Kommt die bzw. der Datenschutzbeauftragte der Verpflichtung zur Weiterführung des Amtes nicht nach, muss sie bzw. er entlassen werden.

Zu §22 (Rechtsstellung)

Die bzw. der Hamburgische Datenschutzbeauftragte muss bei der Ausübung der Aufgaben unabhängig sein, um eine wirksame Kontrolle durchführen zu können. Sie bzw. er ist deshalb in Ausübung des Amtes fachlich unabhängig und nur dem Gesetz unterworfen. Sie bzw. er unterliegt lediglich der Dienstaufsicht des Senats.

Mit der in Absatz 1 Satz 1 normierten Unabhängigkeit und bloßen Gesetzesunterworfenheit der bzw. des Hamburgischen Datenschutzbeauftragten ist eine Rechtsaufsicht, die letztlich auch die Weisungsbefugnis hinsichtlich bestimmter Rechtsauffassungen beinhaltet, kaum zu vereinbaren. Im Übrigen besteht für eine Rechtsaufsicht in der Regel kein Bedarf, da es dem Senat und den Behörden unbenommen ist, den Rechtsauffassungen der bzw. des Hamburgischen Datenschutzbeauftragten z.B. in den Stellungnahmen zu Beanstandungen oder zu den Tätigkeitsberichten entgegenzutreten. Daher ist die früher bestehende Rechtsaufsicht entfallen. Hiermit ist im Übrigen eine Harmonisierung mit den Datenschutzgesetzen der anderen Bundesländer erreicht, die unabhängig von der konkreten Anbindung der bzw. des jeweiligen Landesdatenschutzbeauftragten eine Rechtsaufsicht nicht vorsehen.

Aus dieser Unabhängigkeit ergibt sich auch die Befugnis, als „oberste Dienstbehörde“ bzw. „oberste Aufsichtsbehörde“ die Entscheidung über die Vorlage von Akten und die Erteilung von Auskünften aus dem eigenen Bereich aufgrund von §96 StPO und §99 VwGO sowie in eigener Verantwortung die beamtenrechtlichen Entscheidungen nach §§65 und 66 HmbBG zu treffen.

Gemäß Absatz 2 soll die bzw. der Hamburgische Datenschutzbeauftragte zur Stärkung der Unabhängigkeit auf die personelle und sachliche Ausstattung der Dienststelle Einfluss haben. Sie bzw. er kann auch verhindern, dass Mitarbeiterinnen bzw. Mitarbeiter gegen ihren bzw. seinen Willen versetzt oder abgeordnet werden.

Im Übrigen wird durch Satz 4 klargestellt, dass die bzw. der Hamburgische Datenschutzbeauftragte auch über die in Absatz 1 Satz 2 geregelten Fälle hinaus Dienstvorgesetzte bzw. Dienstvorgesetzter (§3 Absatz 2 Satz 1 HmbBG) der Mitarbeiterinnen und Mitarbeiter ist. Diese unterstehen zur Sicherung der Unabhängigkeit der bzw. des Hamburgischen Datenschutzbeauftragten auch allein ihren bzw. seinen Weisungen.

Die Bedeutung der Institution unabhängiger Datenschutzbeauftragter für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung (BVerfGE 65, 1, 46) erfordert es, dass die gesetzlichen Aufgaben auch bei Verhinderung der Amtsinhaberin bzw. des Amtsinhabers in voller Weise und ohne Verzögerung wahrgenommen werden können. Dies wird durch Absatz 3 gewährleistet.

Die Geschäfte der bzw. des Hamburgischen Datenschutzbeauftragten werden im Fall einer vorübergehenden Verhinderung infolge Erholungsurlaubs oder kürzerer Krankheit durch die dienststellenintern zur Vertretung berufene Person wahrgenommen. Herausgehobene Handlungen können nur durch die zur bzw. zum Hamburgischen Datenschutzbeauftragten bestellte Person selbst oder durch von ihr bzw. ihm hierzu ausdrücklich bestimmte Personen vorgenommen werden. Dabei handelt es sich um Beanstandungen (§25), um dienststellenbezogene Personalentscheidungen (§22 Absätze 1 und 2) sowie um die Kontrolle besonders sensibler Verwaltungsbereiche

(§22 Absatz 6). Die Sätze 1 und 2 stellen klar, dass auch die zur Vertreterin bzw. zum Vertreter bestimmte Person die vollen Befugnisse hat, die das Gesetz an die Person der bzw. des bestellten Hamburgischen Datenschutzbeauftragten knüpft.

Die Sätze 1 und 2 legen ferner fest, dass die bzw. der Hamburgische Datenschutzbeauftragte für den Regelfall die Vertretung selbst regelt. Nur bei (ununterbrochen) längeren Verhinderungen hat der Senat die Möglichkeit, eine Vertreterin oder einen Vertreter zu bestellen (Satz 3). Ein solcher Fall kann allerdings auch dann vorliegen, wenn – z.B. bei schwerer Erkrankung – schon bei Beginn der Verhinderung von einer längeren Dauer als zwei Monate auszugehen ist. Vor einer Vertreterbestellung durch den Senat soll die bzw. der Hamburgische Datenschutzbeauftragte gehört werden, falls das die Art der Verhinderung zulässt.

Satz 4 erfasst den bislang nicht ausdrücklich geregelten, aber bereits einmal aktuell gewordenen Fall, dass die bzw. der Hamburgische Datenschutzbeauftragte vor Ablauf der Amtszeit (einschließlich der Regelung des §21 Absatz 3 Satz 1, zweiter Halbsatz) aus dem Amt ausscheidet, z.B. durch die Entlassung auf eigenen Antrag. Hier ist die entsprechende Anwendung der für eine vorübergehende Verhinderung geltenden Regelungen sachgerecht. Die Vertreterbestellung durch den Senat nach Satz 3 kommt hier nur dann in Betracht, wenn Wahl und Bestellung einer Nachfolgerin oder eines Nachfolgers innerhalb von zwei Monaten nicht zustande kommen. Infolge des Endes der Amtszeit ist hier eine Anhörung der bzw. des (ehemaligen) Hamburgischen Datenschutzbeauftragten nicht mehr möglich bzw. nicht mehr sachgerecht.

Zu §23 (Aufgaben)

Die Kontrolle der Einhaltung des Datenschutzes durch unabhängige Beauftragte für den Datenschutz stellt nach den Aussagen des Bundesverfassungsgerichts in seiner Entscheidung vom 15. Dezember 1983 (BVerfGE 65, 1, 46) eine wesentliche Voraussetzung dar, um das Recht des Einzelnen auf informationelle Selbstbestimmung zu gewährleisten.

Die Kontrolltätigkeit der bzw. des Hamburgischen Datenschutzbeauftragten erfasst den gesamten, in §2 Absatz 1 Satz 1 und Absatz 2 genannten hamburgischen öffentlichen Bereich (und den in §3 Absatz 3 genannten privatrechtlichen Bereich der Auftragsdatenverarbeitung).

Absatz 1 Satz 2 bestimmt, dass nicht nur die Gerichte, sondern auch die Bürgerschaft und der Rechnungshof wegen ihrer besonderen verfassungsrechtlichen Stellung der Überwachung durch die bzw. den Hamburgischen Datenschutzbeauftragten nur unterliegen, soweit sie in Verwaltungsangelegenheiten tätig werden, weil auch sie unabhängig in ihrer Aufgabenwahrnehmung sind.

Der an Absatz 1 Satz 2 angefügte Halbsatz stellt klar, dass die für Gerichte grundsätzlich geltende Beschränkung der Datenschutzkontrolle auf Verwaltungsangelegenheiten (siehe aber auch Satz 3) für Gerichtsvollzieherinnen und Gerichtsvollzieher nicht gilt. Ob die Klarstellung konstitutiven oder nur deklaratorischen Charakter hat, kann dahinstehen.

Zur Verstärkung des Grundrechts auf informationelle Selbstbestimmung, das gegenüber allen staatlichen Gewalten besteht (Artikel 1 Absatz 3 GG), geht die Datenschutzkontrolle über den Bereich der von den Gerichten wahrgenommenen Verwaltungsangelegenheiten hinaus (zur Abgrenzung der Rechtspflegeaufgaben und der Verwaltungsangelegenheiten der Gerichte vgl. Bürgerschafts-Drs. 14/3826, S. 6, 7 vom 30. März 1993). Der verstärkte Einsatz elektronischer Datenverarbeitung im Gerichtswesen kann eine gesteigerte Gefährdung des Datenschutzgrundrechts mit sich bringen (vgl. die Ausführungen im Volkszählungsurteil des Bundesverfassungsgerichts, BVerfGE 65, 1, 42). Aber auch beim Umgang mit Akten sind die Gefahren z.B. durch Zugriffsmöglichkeiten Unbefugter groß. §8 des Gesetzes, der uneingeschränkt auch für die Gerichte gilt, fordert hier differenzierte Maßnahmen zur Datensicherung.

Die bzw. der Hamburgische Datenschutzbeauftragte kann daher gemäß Absatz 1 Satz 3 bei den Gerichten auch insoweit, als sie im Rechtspflegebereich tätig werden, prüfen, ob die in §8 oder in bereichsspezifischen Rechtsvorschriften genannten technischen und organisatorischen Maßnahmen getroffen und eingehalten werden. Der Bereich der Datensicherung gehört zur äußeren Ordnung der Erledigung von Rechtspflegeaufgaben; insoweit genießen Richterinnen und Richter nicht die richterliche Unabhängigkeit (vgl. Drucksache 14/3826, Seiten 4 bis 6). Dabei kann es unter Umständen erforderlich sein, dass die bzw. der Hamburgische Datenschutzbeauftragte von den gespeicherten Daten Kenntnis nimmt. Denn die Prüfung, ob die erforderlichen technischen und organisatorischen Maßnahmen getroffen sind, ist grundsätzlich nur möglich bei Kenntnis der Schutzwürdigkeit der Daten (§8 Absatz 1 Satz 2). Doch wird eine solche Kenntnisnahme regelmäßig nicht erforderlich sein, da es in der Regel genügt zu

wissen, um welche Art von Daten es geht, und da die von Gerichten verarbeiteten Daten meistens sensibel sind. Aber selbst bei einer ausnahmsweise doch einmal notwendigen Kenntnisnahme konkreter personenbezogener Daten würde die richterliche Unabhängigkeit noch nicht berührt. Denn der bzw. dem Hamburgischen Datenschutzbeauftragten steht keinerlei Befugnis zur Prüfung und Bewertung zu, ob bestimmte Daten zu Recht verarbeitet werden; insbesondere besteht kein Recht, die Erforderlichkeit der Erhebung, Speicherung und weiteren Verarbeitung von Daten zu prüfen. Dies alles gehört vielmehr zum Kernbereich der richterlichen Rechtspflege, in dem eine Datenschutzkontrolle auszuscheiden hat.

Die Abgrenzung „Gerichte“ anstatt „Richterinnen und Richter“ bedeutet, dass bei den Rechtspflegeangelegenheiten der Gerichte stets nur eine (äußere) Daten sicherungs-, keine (materielle) Datenverarbeitungskontrolle stattfindet, und zwar unabhängig davon, ob eine konkrete Tätigkeit im Rechtspflegebereich von Richterinnen und Richtern oder von anderen im Gericht beschäftigten Personen wahrgenommen wird.

Laut Absatz 1 Satz 2 ist die Rechtspflegetätigkeit der Staatsanwaltschaft nicht von der Datenschutzkontrolle freigestellt. Entscheidend ist, dass die Staatsanwaltschaften nicht in richterlicher Unabhängigkeit als dritte Gewalt tätig werden. Zwar wäre es schwer vereinbar mit der im Übrigen weitgehend unabhängigen Stellung der Staatsanwaltschaften als Organe der Rechtspflege, wollte die Datenschutzkontrolle durch amtliche Prüfungen, öffentlich wirkende Stellungnahmen und Beanstandungen Einfluss auf die fachlichen Entscheidungen im Rahmen der Ermittlungstätigkeit nehmen. Eine solche Gefahr ist aber nicht zu befürchten. Gegenstand der Datenschutzkontrolle ist allein die Einhaltung von Vorschriften über den Datenschutz – zu ihnen gehört auch der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit –, nicht aber die Kontrolle der rechtsfehlerfreien Beurteilung. So erstreckt sich die Datenschutzkontrolle nicht auf die Ausübung des Ermessens. Im Übrigen wird die Datenschutzkontrolle auch bei der Handhabung unbestimmter Rechtsbegriffe einen Beurteilungsspielraum der Staatsanwaltschaft anerkennen und sich auf grundsätzliche und gewichtige Fragen beschränken; die Frage z.B., ob es erforderlich ist, zusätzliche Daten über Beschuldigte oder Zeugen zu erheben, kann in aller Regel nicht Gegenstand der Datenschutzkontrolle sein.

Satz 3 bezieht sich außer auf die Gerichte auch auf den Rechnungshof. Die Prüfungsbefugnis der bzw. des Hamburgischen Datenschutzbeauftragten besteht im soeben beschriebenen Rahmen auch bei der Prüfungstätigkeit des Rechnungshofs. Wie schon bei der Beratung des Hamburgischen Datenschutzgesetzes vom 5. Juli 1990 ausgeführt wurde (vgl. Bürgerschafts-Drs. 13/3282, S. 32; 13/6067, S.16), sollen Ausnahmen von der Datenschutzkontrolle möglichst eng gefasst werden. Eine Gleichbehandlung der Gerichte und des Rechnungshofs, die der Rechnungshof im Übrigen – wenn auch von anderem Ausgangspunkt aus – bei der Beratung des früheren Gesetzes ausdrücklich gefordert hatte (vgl. Bürgerschafts-Drs. 13/3282 Seite 31), ist auch von der rechtlichen Stellung des Rechnungshofs her geboten. Gemäß Artikel 71 Absatz 1 Satz 1 Hamburger Verfassung (HV) und §1 Absatz 1 Satz 2 des Gesetzes über den Rechnungshof der Freien und Hansestadt Hamburg (RHG) ist der Rechnungshof unabhängig und nur dem Gesetz unterworfen. Seine Mitglieder haben bei ihrer Prüftätigkeit die gleiche Rechtsstellung wie Richterinnen und Richter (Artikel 71 Absatz 5 Satz 1 HV, §6 Satz 2 RHG).

Die nach Absatz 2 vorgesehene empfehlende und beratende Tätigkeit der bzw. des Hamburgischen Datenschutzbeauftragten bezieht sich auf den gesamten hamburgischen öffentlichen Bereich nach §2 Absatz 1 Satz 1 und Absatz 2 und damit auch auf sämtliche Datenschutzfragen bei der Bürgerschaft, den Gerichten und dem Rechnungshof, ohne die Einschränkung wie bei der Kontrolltätigkeit nach Absatz 1.

Die in Absatz 3 festgelegten besonderen Befugnisse und Pflichten der bzw. des Hamburgischen Datenschutzbeauftragten gegenüber Senat und Bürgerschaft erleichtern die Wahrnehmung der Aufsichtsaufgaben im Bereich des Datenschutzes. Durch die Regelung über den Tätigkeitsbericht werden Senat und Bürgerschaft in die Lage versetzt, sich über die Arbeit der bzw. des Hamburgischen Datenschutzbeauftragten zu unterrichten.

Gemäß Satz 2 ist ein Tätigkeitsbericht nicht mehr starr jedes Jahr, sondern flexibel mindestens alle zwei Jahre zu erstatten. Außerdem wird es durch Satz 3 der bzw. dem Hamburgischen Datenschutzbeauftragten ermöglicht, sich jederzeit – auch mit bestimmten Schwerpunktthemen – an die Bürgerschaft zu wenden. Der Hamburgische Datenschutzbeauftragte hat – neben einer ausführlichen zweijährigen Berichterstattung – für die Zwischenjahre Ergebnisberichte in Kurzfassung vorgelegt.

Satz 3 bekräftigt die unabhängige Stellung der bzw. des Hamburgischen Datenschutzbeauftragten. Sie bzw. er ist im Verkehr mit der Bürgerschaft nicht nur auf die Tätigkeitsberichte und etwaige Berichte aufgrund eines Verlangens nach Satz 1 angewiesen. Sie bzw. er hat vielmehr auch die Möglichkeit, sich z.B. mit Zwischenberichten zu aktuellen Themen an die Bürgerschaft zu wenden. Mit diesem Vorschlag wird auch einem Wunsch des vom Rechtsausschuss der Bürgerschaft eingesetzten Unterausschusses „Datenschutz“ nach einem intensiven Meinungsaustausch zwischen

Parlament und der bzw. dem Hamburgischen Datenschutzbeauftragten zwischen den Tätigkeitsberichten Rechnung getragen.

In den Fällen, in denen sich die bzw. der Hamburgische Datenschutzbeauftragte schriftlich an die Bürgerschaft wendet, muss der Senat damit rechnen, der Bürgerschaft oder – z.B. bei schriftlichen Anfragen – einzelnen ihrer Mitglieder kurzfristig Rede und Antwort zu stehen. Um den Senat hierzu in die Lage zu versetzen und auch im Hinblick darauf, dass die bzw. der Hamburgische Datenschutzbeauftragte Teil der Exekutive ist, ist es erforderlich, dass schriftliche Äußerungen gegenüber der Bürgerschaft gleichzeitig auch dem Senat vorgelegt werden (Absatz 3 Satz 4), wie dies im Übrigen gemäß Absatz 3 Satz 2 für den Tätigkeitsbericht bereits gilt.

Absatz 4 stellt sicher, dass die Belange des Datenschutzes schon bei Planungen neuer Anwendungen zur Nutzung der Informations- und Kommunikationstechnik berücksichtigt werden sollen. Dies erfordert eine rechtzeitige Einflussnahme der bzw. des Hamburgischen Datenschutzbeauftragten auf deren datenschutzgerechte Ausgestaltung.

Die Absätze 5 und 6 treffen eine differenzierte Regelung zur Ausübung des Kontrollrechts durch die bzw. den Hamburgischen Datenschutzbeauftragten und ihre bzw. seine Beauftragten. Nach der Grundsatzregelung in Absatz 5 Sätze 1 und 2 haben die öffentlichen Stellen uneingeschränkt Auskunft sowie Einsicht in alle relevanten Unterlagen und Akten, auch Zutritt zu allen Diensträumen zu gewähren.

Wie Satz 3 ausdrücklich klarstellt, können gesetzliche Geheimhaltungsvorschriften dem Auskunfts- oder Einsichtsverlangen nicht entgegengehalten werden; die bzw. der Datenschutzbeauftragte und die Mitarbeiterinnen und Mitarbeiter unterliegen ihrerseits der Amtsverschwiegenheit. Diese Aussage gilt auch, wenn die Geheimhaltung durch Bundesrecht vorgeschrieben wurde, es sei denn, eine Auslegung der bundesrechtlichen Vorschrift ergibt eine ausdrücklich auch gegenüber der Datenschutzkontrolle gewollte Sperre. Davon ist aber im Zweifel wegen der vom Bundesverfassungsgericht betonten hohen Bedeutung der unabhängigen Datenschutzkontrolle für den Individualdatenschutz und für die Allgemeinheit nicht auszugehen; dies gilt auch in den Fällen des §24 Absatz 2 i. V. m. Absatz 6 BDSG (siehe Rechtsgutachten gemäß Anlage 1 zur Bürgerschafts-Drs. 14/2845). Insbesondere bei der Anwendung des §203 StGB ergibt sich die Befugung aus den (landesrechtlichen) Vorschriften über die Datenschutzkontrolle.

Eine Besonderheit gilt nach Absatz 6 für die dort genannten Sicherheitsbehörden und Landesfinanzbehörden: Sie haben die Unterstützung nur der bzw. dem Hamburgischen Datenschutzbeauftragten selbst und den von ihr bzw. ihm schriftlich besonders damit betrauten Beauftragten zu gewähren. Doch kann ihnen die Akteneinsicht dann verweigert werden, wenn im Einzelfall der Senat feststellt, dass die Einsicht die Sicherheit des Bundes oder eines Landes gefährdet.

Absatz 7 stellt klar, dass der Senat der bzw. dem Hamburgischen Datenschutzbeauftragten auch die Aufgaben der Aufsichtsbehörde für die Datenverarbeitung im nicht-öffentlichen Bereich übertragen kann. Eine solche Übertragung hat der Senat bereits im Jahre 1982 vorgenommen.

Zum anderen wird die früher schon geübte Praxis, dass auch über die Aufsichtstätigkeit im nicht-öffentlichen Bereich in einem eigenen Teil des Tätigkeitsberichts berichtet wird, gesetzlich abgesichert. Dieser Berichtsteil steht, da es sich bei der Kontrolle gemäß §38 BDSG um staatliche Kontrolltätigkeit handelt, allerdings unter der Verantwortung des Senats.

Zu §24 (Dateiregister)

Die Vorschrift war mit der Änderung des Gesetzes vom 18. März 1997 als entbehrlich aufgehoben worden.

Zu §25 (Beanstandungen)

Die Vorschrift regelt, wie die bzw. der Hamburgische Datenschutzbeauftragte auf die Klärung und vor allem die Behebung von Mängeln bei der Verarbeitung personenbezogener Daten, die von ihr bzw. ihm festgestellt worden sind, hinwirken kann. Der erste Schritt ist gemäß Absatz 1 die Beanstandung, die die Pflicht zur Stellungnahme auslöst.

Nach Absatz 1 Satz 1 Nummer 1 wird bei Mängeln oder Verstößen im Bereich der unmittelbaren Verwaltung die Beanstandung zunächst gegenüber dem Senator der betroffenen Behörde ausgesprochen; betrifft die Beanstandung den Bereich der Bezirksverwaltung, wird sie gegenüber dem Senator der Aufsichtsbehörde ausgesprochen.

Da die der Datenschutzkontrolle unterliegenden Tätigkeitsbereiche der Gerichte auch der Dienstaufsicht unterliegen, ist es sachgerecht, eine etwaige Beanstandung in diesem Bereich an das zuständige Senatsmitglied zu richten (Satz 1 Nummer 1).

Beanstandungen im Bereich der in §2 Absatz 1 Satz 1 Nummer 2 aufgeführten öffentlich-rechtlich organisierten Einrichtungen von juristischen Personen des öffentlichen Rechts sind an den Vorstand oder das sonst vertretungsberechtigte Organ zu richten (Satz 1 Nummer 2).

Wegen der verfassungsrechtlichen Stellung der Bürgerschaft und des Rechnungshofs kommt hier eine Beanstandung nur gegenüber der jeweiligen Präsidentin bzw. dem jeweiligen Präsidenten in Betracht; dies gilt auch für eine etwaige weitere Beanstandung (Satz 1 Nummer 3).

Am Ende des Satzes 1 ist bestimmt, dass die Aufforderung zur Stellungnahme mit der Aufforderung zur Behebung der Mängel verbunden wird und dass sich die Fristsetzung auf die Stellungnahme und die Mängelbehebung bezieht; dabei können die Fristen unterschiedlich lang sein.

Erst wenn die aufgezeigten Mängel nicht innerhalb einer gesetzten Frist behoben werden, wird die Beanstandung nach Satz 2 direkt dem Senat (bei Stellen der mittelbaren Verwaltung der Aufsichtsbehörde) gegenüber ausgesprochen. Damit wird das Instrument der Beanstandung einerseits aufgewertet, der Senat andererseits entlastet. Außerdem wird klargestellt, dass bei einer weiteren Beanstandung das Verfahren wie bei der ersten Beanstandung gilt.

Absatz 2 ermöglicht es der bzw. dem Hamburgischen Datenschutzbeauftragten, von der Beanstandung ganz oder teilweise abzusehen, wenn sie bzw. er diese förmliche Maßnahme zur Wahrung des Datenschutzes nicht für notwendig hält. Dies kann insbesondere bei geringen Mängeln der Fall sein oder wenn feststeht, dass die Mängel behoben sind oder behoben werden.

Verzichtet die bzw. der Hamburgische Datenschutzbeauftragte auf eine förmliche Beanstandung, so entfällt hiermit auch die Verpflichtung, hierzu Stellung zu nehmen. Wird aber eine Beanstandung ausgesprochen, dann ist auch Stellung zu nehmen.

Absatz 3 berücksichtigt, dass mit der Beanstandung vor allem die Beseitigung der Mängel für die Zukunft erreicht werden soll. Deshalb kann die bzw. der Hamburgische Datenschutzbeauftragte entsprechende Vorschläge machen und dabei auch ausdrücklich sonstige Verbesserungsvorschläge einbeziehen.

Die in Absatz 4 festgelegte Pflicht zum Bericht durch die betroffene Stelle über die Maßnahmen, die sie aufgrund der Beanstandung veranlasst hat, erleichtert der bzw. dem Hamburgischen Datenschutzbeauftragten die Wahrnehmung ihrer bzw. seiner Aufgaben. Zugleich wird klargestellt, dass auch zu einer weiteren Beanstandung eine Stellungnahme abzugeben ist.

Zu §26 (Anrufung)

Die bzw. der Hamburgische Datenschutzbeauftragte soll Ansprechpartner und Interessenwahrer der betroffenen Bürger sein. Die Vorschrift gewährt deshalb jedem das Recht, sie bzw. ihn anzurufen (Absatz 1). Für diesen Fall gilt ein Maßregelungs- und Benachteiligungsverbot (Absatz 2). Das Recht auf ungehinderte Anrufung erstreckt sich auf sämtliche Verstöße gegen alle Datenschutzvorschriften, die für hamburgische öffentliche Stellen im Sinne des §2 Absatz 1 Satz 1 gelten, sowie für andere Stellen, die sich aufgrund gesetzlicher Vorschriften der Überwachung durch die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten unterworfen haben.

Zu §27 (Datenverarbeitung zum Zwecke wissenschaftlicher Forschung)

§27 regelt als allgemeine „Forschungsklausel“ die Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke durch öffentliche Stellen einschließlich der Datenübermittlung an private Forschungsstellen. Eine solche Vorschrift ist unverzichtbar, denn die wissenschaftliche Forschung genießt, auch wenn ihr durch Artikel 5 Absatz 3 Satz 1 GG ein gewichtiger Stellenwert zugewiesen wurde, keinen Vorrang gegenüber dem Recht auf informationelle Selbstbestimmung; die einander prinzipiell gegenüberstehenden Interessen sind daher durch eine gesetzliche Forschungsklausel in Einklang zu bringen. Die mit dem Begriff der wissenschaftlichen Forschung angesprochenen

Sachverhalte sind jedoch so unterschiedlich, dass §27 nur allgemeine Grundsätze zur Auflösung des Spannungsverhältnisses zwischen Forschung und Selbstbestimmungsrecht aufzeigen kann; ergänzende oder modifizierende bereichsspezifische Datenschutzregelungen sind dadurch nicht ohne weiteres verzichtbar.

Im Grundsatz bedarf auch die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher Forschung in allen ihren Phasen der Einwilligung (dazu vgl. §5) der Betroffenen. Es ist aber nicht immer möglich und auch nicht immer notwendig, die Einwilligung der Betroffenen einzuholen. Nach Absatz 1 ist die Einwilligung zunächst dann verzichtbar, wenn schutzwürdige Belange der Betroffenen aus den in Satz 1 genannten Gründen nicht beeinträchtigt werden. Im Übrigen (Satz 2) kann auf die Einwilligung auch dann verzichtet werden, wenn das öffentliche Interesse erheblich überwiegt und der Forschungszweck anders nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Unter diesen Voraussetzungen ist die Datenverarbeitung in allen ihren Phasen zulässig.

Dies gilt auch für die Verarbeitung von Daten, die einem besonderen Geheimnisschutz (z.B. der ärztlichen Schweigepflicht) unterliegen. Die gesetzlichen Geheimhaltungsvorschriften stehen einer Datenverarbeitung zu Forschungszwecken nicht entgegen, so dass es sich um eine befugte Verarbeitung auch im Sinne von §203 StGB handelt.

Zusätzliche Anforderungen an die – bei der externen Forschung notwendige – Übermittlung regelt Absatz 2 (vgl. auch Absatz 6): Die Weitergabe personenbezogener Daten zu Forschungszwecken ohne Einwilligung und Kenntnis der Betroffenen erfordert zum Ausgleich besondere Verfahrensregelungen. Über die Weitergabe hat unter Nennung der entscheidenden Punkte die Behördenleitung zu entscheiden; der bzw. dem Hamburgischen Datenschutzbeauftragten ist Kenntnis zu geben. Die Behördenleitung kann die Befugnis auf eine bestimmte Mitarbeiterin bzw. einen bestimmten Mitarbeiter übertragen. Entsprechend allgemeinen Organisationsgrundsätzen kann die Befugnis im Bedarfsfall auch durch die jeweils vertretende Person ausgeübt werden.

Die Regelungen des Absatzes 3 stellen sicher, dass der Personenbezug der für die Forschung verarbeiteten Daten nur solange erhalten bleibt, wie das aus Gründen des Forschungszwecks erforderlich ist. „Anonymisieren“ verweist auf §4 Absatz 9.

Absatz 4 bringt erneut den Grundsatz der Zweckbindung zur Geltung.

Absatz 5 trifft eine Regelung über die Befugnisse zur Veröffentlichung personenbezogener Daten im Rahmen wissenschaftlicher Forschung. Sie wird an enge Zulässigkeitsvoraussetzungen gebunden: Prinzipiell ist die Einwilligung der Betroffenen erforderlich; nur in den Fällen, in denen die Veröffentlichung personenbezogener Daten für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist, soll das informationelle Selbstbestimmungsrecht zurücktreten. Damit ergeben sich Berührungspunkte zu den Archivregelungen.

Absatz 6 erfasst den Fall, dass auf die Stelle, der die Daten übermittelt werden, dieses Gesetz nicht anzuwenden ist, weil es sich um eine privatrechtliche oder ausländische Forschungsstätte handelt. Im Geltungsbereich des Grundgesetzes muss sich diese Stelle vor einer Übermittlung an sie der Kontrolle der bzw. des für sie zuständigen Datenschutzbeauftragten unterwerfen und sich zur Erfüllung der Anforderungen nach den Absätzen 3 und 5 verpflichten. Bei Forschungsvorhaben im Ausland ist dagegen eine Kontrolle durch eine bzw. einen Datenschutzbeauftragten nicht durchführbar. Für Forschungen außerhalb der Europäischen Union ist die Beachtung des ordre public weitere Voraussetzung der Übermittlung; für Übermittlungen in ein Mitgliedsland der Europäischen Union gilt für die Stelle, der die Daten übermittelt werden, das an die EG-Datenschutzrichtlinie angepasste nationale Datenschutzrecht.

Absatz 7 berücksichtigt die in der Praxis des öfteren auftretende Notwendigkeit, zur Vorbereitung von Rechtsnormen oder allgemeinen Verwaltungsvorschriften oder auch, um die Praxisnähe solcher Vorschriften zu überprüfen, „Rechtstatsachenforschung“ zu betreiben. Es mag zweifelhaft sein, ob die Auswertung einer Gruppe von Einzelfällen aus der Praxis zu diesem Zweck immer als „wissenschaftliche“ Forschung (planmäßige, methodisch kontrollierte, unbefangene Suche nach Erkenntnissen) anzusehen ist. Angesichts einer gleichen Interessenlage sind die Vorschriften über die wissenschaftliche Forschung für diese Fälle auch dann anzuwenden, wenn nicht alle Anforderungen an eine wissenschaftliche Tätigkeit erfüllt sind.

Zu §28 (Datenverarbeitung bei Beschäftigungsverhältnissen)

§28 regelt die Besonderheiten bei Beschäftigungsverhältnissen im Bereich der öffentlichen Verwaltung. Der Begriff der Beschäftigungsverhältnisse ist weit zu verstehen: Er umfasst neben den Beamten-, Angestellten- und

Arbeiterverhältnissen beispielsweise auch öffentlich-rechtliche Dienstverhältnisse eigener Art, öffentlich-rechtliche wie privat-rechtliche Ausbildungsverhältnisse und Nebentätigkeitsverhältnisse; auch die Versorgungsverhältnisse sind zu den Beschäftigungsverhältnissen zu zählen.

Der Hamburgische Datenschutzbeauftragte vertritt die Auffassung, dass diese Vorschrift nur die Datenverarbeitung erfasst, die die einzelnen Beschäftigten usw. in ihrem jeweiligen Beschäftigungsverhältnis betrifft. Dagegen bleiben nach seiner Auffassung die allgemeinen Vorschriften der §§13 ff. einschließlich §16 und auch §30 anwendbar, wenn die Daten einer Vielzahl von Beschäftigten für einen anderen Zweck verarbeitet werden, z.B. wenn Verzeichnisse mit personenbezogenen Daten für den Geschäftsbetrieb verwendet werden (u.a. Telefonverzeichnisse).

Die in den Absätzen 1 bis 6 neu gefasste Vorschrift bezweckt eine weitgehende Vereinheitlichung des Rechts der Verarbeitung personenbezogener Daten – hierunter auch Personalaktendaten (z.B. Akteneinsichtsrecht, vgl. die Begriffsbestimmung in §96 a) Absatz 1 Satz 2 HmbBG) – bei Beschäftigungsverhältnissen mit öffentlichen Stellen. Die durch das Zweite Gesetz zur Änderung dienstrechtlicher Vorschriften vom 9. März 1994 (Hamburgisches Gesetz- und Verordnungsblatt Seite 75) neu gefassten bzw. eingefügten Vorschriften der §§96 bis 96 h) HmbBG gehen in ihrem Anwendungsbereich den Regelungen des Hamburgischen Datenschutzgesetzes vor (§2 Absatz 7).

Die §§96 bis 96 h) HmbBG regeln den Datenschutz der Beamtinnen und Beamten sowie (über §8 Absatz 1 des Hamburgischen Richtergesetzes) der Richterinnen und Richter und gemäß der Erstreckung im Absatz 3 den der sonstigen Beschäftigten im öffentlichen Dienst nicht abschließend. Sie gelten, von Ausnahmen abgesehen, nur für diejenigen personenbezogenen Daten, die Personalaktendaten sind. Aber auch im Bereich der Personalaktendaten ist die Regelung des Datenschutzes nicht abschließend. Aus diesem Grund behalten die aus dem geltenden §28 im Wesentlichen übernommenen Regelungen weiterhin ihre Bedeutung.

Soweit nicht ausdrücklich etwas anderes bestimmt ist, erstreckt sich die Verarbeitungsbefugnis hinsichtlich personenbezogener Daten von Beschäftigten usw. im jeweils erforderlichen Umfang auch auf die Einleitung und Durchführung behördlicher und gerichtlicher Verfahren im Zusammenhang mit dem jeweiligen Verwendungszweck. Es gelten die übrigen Vorschriften des Gesetzes, soweit §28 nicht bei gleichem Sachverhalt Sonderregelungen trifft.

Nach Absatz 1 ist eine Datenverarbeitung bei Beschäftigungsverhältnissen zulässig, soweit eine Rechtsvorschrift dies vorsieht. Dieser Hinweis ist im Grunde nur deklaratorisch; der Vorrang bereichsspezifischer Rechtsvorschriften folgt bereits aus §2 Absatz 7. Wie bisher wird gesetzlich der Vorrang von Tarifvertrag und Dienstvereinbarung vorgesehen, soweit darin Regelungen über die Verarbeitung personenbezogener Daten enthalten sind. Neu aufgenommen wurde als Zwischenstufe zwischen Dienstvereinbarung und Tarifvertrag die Vereinbarung der obersten Dienstbehörde mit den Spitzenorganisationen der zuständigen Gewerkschaften und Berufsverbände gemäß §94 des Hamburgischen Personalvertretungsgesetzes bzw. mit den Berufsverbänden der Richterinnen und Richter gemäß §59 Absatz 1 des Hamburgischen Richtergesetzes. Im Gegensatz zum bisherigen Absatz 1 werden auch frühere Beschäftigte und Hinterbliebene ausdrücklich genannt. Sie sollten zwar auch bisher schon erfasst sein; doch könnte ohne die Änderung über Absatz 3 ein nicht beabsichtigter Gegenschluss zu §96 HmbBG gezogen werden.

Absatz 1 Satz 2 stellt klar, dass Satz 1 die „Einstiegsnorm“ darstellt; nur soweit Regelungen der in Satz 1 bezeichneten Art nicht existieren, kommen die nachfolgenden Absätze zum Zug.

Absatz 2 präzisiert für die Datenverarbeitung den allgemeinen Grundsatz der Zweckbindung (§13 Absatz 1 Satz 1 Nummer 2). Der Einschub „soweit die nachfolgenden Absätze keine besonderen Regelungen enthalten“ verdeutlicht, dass Absatz 2 gegenüber den nachfolgenden Absätzen eine subsidiäre Auffangnorm ist. Auf sie kann gleichwohl nicht verzichtet werden. Zwar enthält der über Absatz 3 entsprechend anzuwendende §96 Satz 1 HmbBG eine inhaltlich fast identische Regelung, doch gilt diese nur für die Erhebung, nicht für die weitere Verarbeitung der Daten.

Absatz 3 erstreckt den Anwendungsbereich der §§96 bis 96 h) HmbBG auf diejenigen Beschäftigungsverhältnisse bei hamburgischen öffentlichen Stellen, für die diese Vorschriften nicht ohnehin schon gelten.

Die Übermittlung als in der Praxis regelmäßig besonders bedeutsame Verarbeitungsphase ist für einige Sonderfälle in Absatz 4 gesondert angesprochen, wobei in Satz 1 verdeutlicht wird, dass es sich hierbei um eine Sonderregelung gegen über der Vorschrift über die Datenübermittlung an nicht-öffentliche Stellen (§16) handelt. Satz 3 weist auf den Vorrang des §96 e) HmbBG (vor allem dessen Absatz 2) für beamtenrechtliche Beschäftigungsverhältnisse hin; für Beamte und Richter ergibt sich (insoweit) der Vorrang des §96 e) HmbBG bereits aus §2 Absatz 7.

Absatz 5 Satz 1 verpflichtet die Stelle, die Untersuchungen verlangt, Anlass und Zweck der Untersuchung anzugeben. Soweit die Art des Beschäftigungsverhältnisses oder der Untersuchungsanlass dies zulassen, ist auch auf die der

betroffenen Person konkret obliegende Aufgabe hinzuweisen. Das setzt die untersuchende Stelle in die Lage, diejenigen Risikofaktoren zu bestimmen, die für die konkrete Untersuchung von Bedeutung sind. Die Vorschrift beschränkt sich außerdem nicht auf Untersuchungen zur Eingehung eines Beschäftigungsverhältnisses, sondern umfasst auch Untersuchungen während und ggf. nach dem Ende eines Beschäftigungsverhältnisses.

Satz 2 knüpft an der Befugnis der die Untersuchung verlangenden Stelle an; hiermit wird berücksichtigt, dass Ärztinnen und Ärzte sowie Psychologinnen und Psychologen, die nicht einer (hamburgischen) öffentlichen Stelle angehören, nicht den Regelungen des Hamburgischen Datenschutzgesetzes unterliegen. Nur soweit die Untersuchungen und Tests von öffentlichen Stellen selbst durchgeführt werden, kann die Weitergabebefugnis näher bestimmt werden (Satz 3). Der Begriff „weitergeben“ berücksichtigt, dass untersuchende und die Untersuchung verlangende Stelle in vielen Fällen dieselbe Stelle im organisatorischen Sinn sind, eine Übermittlung im eigentlichen Sinn (§4 Absatz 2 Satz 2 Nummer 4) somit nicht stattfindet.

Um einem Wunsch der Praxis Rechnung zu tragen, wird im zweiten Halbsatz des Satzes 2 klargestellt, dass dann auch Einzelheiten über die im ersten Halbsatz genannten Untersuchungsergebnisse und Risikofaktoren hinaus verlangt bzw. mitgeteilt werden dürfen, wenn dies im Einzelfall für die Entscheidung erforderlich ist, zu deren Vorbereitung die Untersuchung angeordnet wurde. Da Betroffene einen Anspruch auf eine auf richtigen Grundlagen beruhende Entscheidung haben, muss auch die Möglichkeit bestehen, dass die zur Entscheidung zuständige Stelle die notwendigen Entscheidungsgrundlagen erhält. Auch insoweit muss sich aber das Verlangen nach Weitergabe bzw. Übermittlung von Daten im Rahmen des Untersuchungsauftrags halten; ggf. ist die Erforderlichkeit der weiteren Daten von der auftraggebenden Stelle gegenüber der untersuchenden Stelle zu begründen.

Satz 4 macht klar, dass es jedenfalls beim jetzt erweiterten Umfang der Regelung nicht ausnahmslos auf die Einwilligung der betroffenen Person in die weitere Datenverarbeitung ankommen kann. Ansonsten könnte die betroffene Person bei einer gegen ihren Willen angeordneten Untersuchung, die ein für sie ungünstiges Ergebnis hat, zwar nicht die Weitergabe der Ergebnisse, aber deren Speicherung und Nutzung für die zu treffende Entscheidung verhindern; das wäre in keiner Weise sachgerecht. Dort wo es auf die Einwilligung ankommt, soll diese künftig stets schriftlich gegeben werden müssen; Satz 4 ist insofern vorrangig gegenüber §5 Absatz 2 Satz 1.

Absatz 6 enthält ein Gebot unverzüglicher Löschung zum Schutz der Bewerberinnen und Bewerber und der Beschäftigten. Eine Einschränkung dieses Grundsatzes enthält Satz 2 bei Vorliegen überwiegender berechtigter Interessen der Daten verarbeitenden Stelle. Bei bestimmten Behörden zeichnet sich das Bewerbungsverfahren durch Besonderheiten aus. So sind z.B. bei der Polizei die gesundheitlichen Voraussetzungen eingehend geregelt. Ansonsten geeignete Bewerberinnen und Bewerber können zunächst aus behebbaren Gründen scheitern. Da zudem ein berechtigtes Interesse an einer möglichst guten Personalauswahl besteht, kann es sachgerecht sein, bestimmte Daten zunächst abgelehnter Bewerberinnen und Bewerber weiter zu speichern, um nicht allein auf die jeweils eingehenden Bewerbungen beschränkt zu sein. Bei einer größeren Zahl von Wiederholungsbewerbungen kann es auch sachgerecht sein, das Einstellungsverfahren nicht jedes Mal wieder in allen Stufen durchzuführen, wenn eine erhebliche Anzahl solcher Bewerbungen schon durch einen Rückgriff auf frühere Unterlagen ausgeschlossen werden kann.

Die weitere Speicherung kann aber auch im Interesse der Bewerberin oder des Bewerbers liegen, z.B. einer beabsichtigten erneuten Bewerbung auf eine demnächst freiwerdende Stelle. Deshalb enthält Satz 2 mit der Einwilligung der Betroffenen eine weitere Ausnahme vom Gebot unverzüglicher Löschung.

Absatz 7 stellt sicher, dass die gespeicherten Daten von Beschäftigten im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden. Ansonsten träte auch eine Ungleichbehandlung gegenüber den Beschäftigten ein, die nicht an Datenverarbeitungsgeräten tätig sind.

Die Vorschrift hindert aber nicht eine Nutzung, die gerade aus Gründen der Datensicherung erforderlich ist (z.B. Überprüfung, ob ein Beschäftigter und ggf. welcher Beschäftigte personenbezogene Daten sachgerecht und rechtmäßig verarbeitet hat, einschließlich von Straf- und Disziplinarmaßnahmen).

Nach Absatz 8 ist die „Forschungsklausel“ auch in dem speziellen Bereich der Beschäftigungsverhältnisse anwendbar. Insbesondere soweit es um zeitgeschichtliche Forschung geht, haben Mitarbeiter des öffentlichen Dienstes keine Sonderstellung.

Zu §29 (Fernmessen und Fernwirken)

Die Vorschrift trifft generelle Bestimmungen über die Zulässigkeit der Einrichtung von Fernmess- und Fernwirkdiensten durch öffentliche Stellen oder öffentliche Wettbewerbsunternehmen in Wohn- und Geschäftsräumen Privater. Dieser erhebliche Eingriff in das Recht auf informationelle Selbstbestimmung ist nach Absatz 1 Sätze 1 und 2 nur zulässig, wenn die Betroffenen nach einer im einzelnen vorgeschriebenen Unterrichtung durch die einrichtende Stelle ihre Einwilligung schriftlich – oder gemäß §4a in elektronischer Form mit digitaler Signatur – erklärt haben. Die Betroffenen müssen ferner erkennen können, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist (Satz 3). Die Betroffenen können darüber hinaus die Einwilligung jederzeit widerrufen; dies muss allerdings mit der Zweckbestimmung des Dienstes vereinbar sein. Im Zweifel gilt das Abschalten des Dienstes als Widerruf (Absatz 1 Sätze 4 und 5). „Betroffene“ sind bei Geschäftsräumen die für den Betrieb Verantwortlichen, nicht dagegen die einzelnen Beschäftigten.

Nach Absatz 2 Satz 1 besteht ein Junktim-Verbot, die vertragliche Leistung, den Abschluss oder die Abwicklung des Vertragsverhältnisses von der Einwilligung der Betroffenen zur Einrichtung der Dienste abhängig zu machen. Damit soll die Entscheidungsfreiheit der Betroffenen soweit wie möglich gewahrt bleiben. Ihnen dürfen im Fall der Verweigerung oder des Widerrufs nur die nachweisbaren Mehr kosten, die durch eine andere Art der Datenerhebung entstehen, auferlegt werden (Satz 2).

Nach Absatz 3 Sätze 1 und 2 gelten eine strenge Zweckbindung bei der Verarbeitung personenbezogener Daten und ein obligatorisches Löschungsgebot.

Absatz 4 nimmt bestimmte Fernmess- und Fernwirkdienste von der Geltung der Absätze 1 und 2 aus. Schon bisher befinden sich häufig Messeinrichtungen von Versorgungsunternehmen, jedenfalls in größeren Wohnanlagen, an Stellen, zu denen die einzelnen Bewohnerinnen und Bewohner keinen direkten Zugang haben. So werden auch konventionelle Ablesevorgänge heute schon oft ohne Kenntnis der Betroffenen vorgenommen. Angesichts der relativ geringen Sensibilität der hierbei anfallenden Daten erscheint es sachgerecht, Versorgungsunternehmen von den Anforderungen der Absätze 1 und 2 freizustellen. Große Wohnungsunternehmen beziehen teilweise selbst Leistungen von Versorgungsunternehmen (z.B. Fernwärme) und liefern sie an die Bewohnerinnen und Bewohner der von ihnen verwalteten Gebäude weiter; dies rechtfertigt die diesbezügliche Gleichstellung mit Versorgungsunternehmen. Die Zweckbindungsregelung (Absatz 3) gilt allerdings auch hier.

Die Ausnahme ist indes nur für solche Unternehmen von Bedeutung, für die gemäß §2 Absatz 1 Satz 1 das Hamburgische Datenschutzgesetz gilt. Für Unternehmen, die unter §2 Absatz 1 Satz 2 fallen, wie z.B. die HEW oder die SAGA, gilt §29 von vornherein nicht.

Zu §30 (Datenverarbeitung für Planungszwecke)

Die Vorschrift berücksichtigt die Notwendigkeit von Planungen für eine den sozialen, kulturellen, wirtschaftlichen und ökologischen Erfordernissen entsprechende Entwicklung.

Die Planung ist häufig Bestandteil der jeweiligen Verwaltungsaufgabe und insoweit bereits nach §13 (und ggf. §14) zulässig. Die Regelung erfasst daher nur die Fälle, in denen Daten ausschließlich für Planungszwecke erhoben werden oder in denen für andere Zwecke gespeicherte Daten für Planungszwecke genutzt oder übermittelt werden sollen. Nicht unter die Regelung fällt die Aggregierung bereits gespeicherter personenbezogener Daten zu Planungszwecken, bei der lediglich anonymisierte Daten gewonnen und weiterverarbeitet werden.

Die Vorschrift lässt die Verarbeitung für Planungszwecke in Anlehnung an §27 (Datenverarbeitung zum Zwecke wissenschaftlicher Forschung) zu. Die Daten unterliegen gemäß Absatz 2 einer strikten Zweckbindung. Sie sind möglichst frühzeitig zu anonymisieren (vgl. §4 Absatz 9) und dürfen nicht übermittelt werden, soweit Rückschlüsse auf Einzelpersonen gezogen werden können.

Zu §32 (Straftaten)

Nach dieser Vorschrift ist Fehlverhalten im Zusammenhang mit der dateimäßigen und nicht dateimäßigen Verarbeitung personenbezogener Daten dann strafbar, wenn es sich um ein qualifiziertes Delikt handelt, die Täter also in Bereicherungs- oder Schädigungsabsicht vorgehen.

Die in Absatz 1 Nummern 1 und 2 aufgeführten Handlungsformen erfassen mit Ausnahme des Sperrens alle von diesem Gesetz behandelten Verarbeitungsphasen. Das Abrufen und Sichverschaffen von Daten ebenso wie das Einsehen wurden als Unterformen des Erhebens nicht gesondert aufgeführt. Nach der Begriffsbestimmung in §4 Absatz 2 Satz 2 Nummer 4 werden alle Formen des Übermittelns erfasst; dies gilt auch, wenn man – wie früher

ausdrücklich geregelt – Daten weitergibt oder zum Abruf bereithält. Auch der Versuch ist strafbar. Die Tat wird nur auf Antrag verfolgt; die bzw. der Hamburgische Datenschutzbeauftragte kann die Betroffenen gegebenenfalls auf ihr Antragsrecht hinweisen.

Andere Strafvorschriften, insbesondere solche des Bundesrechts (z.B. §§202 a, 303 a, 303b StGB), gehen vor (Absatz 4).

Zu §33 (Ordnungswidrigkeiten)

Da in §32 nur noch qualifizierte Delikte unter Strafe gestellt sind, enthält §33 einen Katalog von Ordnungswidrigkeitentatbeständen für die nicht qualifizierten Verhaltensweisen; vorsätzliches Fehlverhalten im Umgang mit personenbezogenen Daten bleibt nicht sanktionsfrei. Der Tatbestandskatalog deckt sich mit dem Katalog des §32.

Zu §34 (Verwaltungsgebühren)

Absatz 1 Satz 1 begründet in Anknüpfung an die Diktion des § 1 Absatz 1 GebG eine Gebührenpflicht für Amtshandlungen der Aufsichtsbehörde im nicht-öffentlichen Bereich. Erfasst wird der gesamte Aufsichtsbereich der Aufsichtsbehörde nach § 38 BDSG und anderen Rechtsvorschriften über den Datenschutz (zum Beispiel § 915 e Absatz 4, § 915 f Absatz 4 der Zivilprozessordnung, § 155 b Absatz 3, § 476 Absatz 8 der Strafprozessordnung, § 5 Satz 2 des Hamburgischen Ausführungsgesetzes zur Insolvenzordnung, § 57 des Hamburgischen Mediengesetzes).

Die Vorschrift weicht insoweit von § 3 Absatz 1 Nummer 3 GebG ab, als dort eine Gebührenpflicht lediglich für Amtshandlungen vorgesehen ist, die einer „besonderen“ Überwachung dienen; dazu gehört die anlassunabhängige Regelüberwachung durch die Aufsichtsbehörde nicht. Die spezialgesetzliche Anordnung der Gebührenpflicht beschränkt sich ihrerseits auf die eigentlichen Kontrollhandlungen der Aufsichtsbehörde. Die etwaige Gebührenpflichtigkeit ihrer sonstigen Amtshandlungen bestimmt sich hingegen weiter nach den allgemeinen Vorschriften des Gebührengesetzes, die auch im Übrigen entsprechend anzuwenden sind (vgl. § 1 Absatz 2 GebG). Die Beschreibung der gebührenpflichtigen Amtshandlungen mit dem Begriff der Kontrolle nimmt Bezug auf die Diktion des neuen § 38 BDSG. Während in § 38 Absatz 1 BDSG alter Fassung der Begriff der Überprüfung die Anlassaufsicht und in § 38 Absatz 2 BDSG der Begriff der Überwachung die auch bisher schon für einen begrenzten Bereich angeordnete anlassunabhängige Aufsicht beschrieb, wird die neue umfassende anlassunabhängige Aufsicht mit dem Begriff der Kontrolle bezeichnet. Hieran knüpft die Gebührenregelung an.

Satz 2 ermächtigt den Senat zum Erlass einer Gebührenordnung, die bei der Bemessung der Gebührensätze von dem der Aufsichtsbehörde entstehenden Kontrollaufwand ausgehen und auf diese Weise den durch die Aufgabenmehrung beim Hamburgischen Datenschutzbeauftragten eintretenden Mehraufwand abdecken wird.

Absatz 2 Satz 1 spricht den Grundsatz aus, wonach die kontrollierte Stelle zur Zahlung der Gebühren verpflichtet ist. Die besondere Regelung ist notwendig, weil § 9 Absatz 1 Nummer 3 GebG in Anknüpfung an die beschränkte Gebührenpflicht für Überwachungen nach § 3 Absatz 1 Nummer 3 GebG lediglich die Kostentragungspflicht für den Fall „besonderer“ Überwachungen regelt.

Nach Satz 2 gilt die Kostentragungspflicht der kontrollierten Stelle uneingeschränkt jedoch nur für den Fall, dass die Kontrolle durch die Aufsichtsbehörde selbst – im Rahmen ihrer Arbeitsplanung – oder durch die oder den Datenschutzbeauftragten der kontrollierten Stelle veranlasst worden ist. Erfolgt die Kontrolle hingegen auf Veranlassung Dritter, so ist die kontrollierte Stelle nur kostentragungspflichtig, wenn Mängel festgestellt werden. Werden keine Mängel festgestellt, so sind nach Satz 3 die Dritten, die durch Beschwerden oder dergleichen die Kontrolle veranlasst haben, kostentragungspflichtig, soweit dies der Billigkeit entspricht. Die Regelung verhindert einerseits, dass kontrollierte Stellen aufgrund unberechtigter, unter Umständen sogar in Schädigungsabsicht grundlos geäußerter Beschuldigungen Dritter mit kostenpflichtigen Kontrollen überzogen werden. Auf der anderen Seite werden die Dritten nur insoweit zur Rechenschaft gezogen, als dies der Billigkeit entspricht. Hierdurch wird insbesondere gewährleistet, dass Dritte, denen sich aufgrund der Umstände des Einzelfalles die Vermutung einer nicht ordnungsgemäßen Verarbeitung ihrer personenbezogenen Daten aufdrängt, bei einer diesbezüglichen Eingabe an die Aufsichtsbehörde auch dann nicht mit einem Kostenrisiko belastet werden, wenn sich ihre Vermutung im Ergebnis nicht bestätigt. Im Übrigen sind bei der Beurteilung der Billigkeit sämtliche Umstände des einzelnen Falles in Betracht zu ziehen. Die Kostentragung, „soweit“ dies der Billigkeit entspricht, lässt auch eine nur teilweise Belastung mit den angefallenen Gebühren zu.