BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

Drucksache 21/11638

21. Wahlperiode

16. 01. 18

Mitteilung des Senats an die Bürgerschaft

Entwurf eines Gesetzes zur Anpassung des Hamburgischen Datenschutzgesetzes sowie weiterer Vorschriften an die Verordnung (EU) 2016/679

1. **Anlass des Gesetzesentwurfes**

Mit dem vorliegenden Gesetzentwurf ist beabsichtigt, das Hamburgische Datenschutzgesetz (HmbDSG) in einer Neufassung sowie weitere Vorschriften des Landesrechts an die am 25. Mai 2016 in Kraft getretene und ab dem 25. Mai 2018 geltende Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Verordnung (EU) 2016/679; im Folgenden: DS-GVO) anzupassen.

Ein wesentliches, durch die DS-GVO zu erreichendes Ziel ist es, in den EU-Mitgliedstaaten ein möglichst einheitliches und gleichwertiges Schutzniveau bei der Verarbeitung personenbezogener Daten herzustellen. Die im ausdrücklich als „Grundverordnung“ bezeichneten Rechtsakt enthaltenen Bestimmungen belassen den Mitgliedstaaten der EU indes Regelungsspielräume in Form von Rechtsetzungsaufträgen und Regelungsoptionen (Spezifizierungs-/Öffnungsklauseln). Mit der DS-GVO entsteht somit Anpassungsbedarf sowohl hinsichtlich des allgemeinen als auch des bereichsspezifischen Landesdatenschutzrechts, soweit sie nicht ein Festhalten an bestehenden gesetzlichen Bestimmungen zulässt.

2. **Inhalt des Gesetzesentwurfes**

Bei der Anpassung des HmbDSG sind angesichts des unionsrechtlichen Normwiederholungsverbotes Regelungen, die sich bereits inhaltlich auf Ebene der DS-GVO finden, aufzuheben. Der DS-GVO widersprechende Vorschriften sind auf Grund des Vorrangs des Unionsrechts vor nationalem Recht ebenfalls aufzuheben. Darüber hinaus sind die durch die DS-GVO erteilten Regelungsaufträge umzusetzen. Von den Regelungsoptionen wird in einer Weise Gebrauch gemacht, dass bestehende materielle Vorgaben des EU-Rechts beachtet und mit bereits bewährten Instrumenten des Bundes- und Landesrechts in Ausgleich gebracht werden. Die Neufassung orientiert sich dabei im Wesentlichen an den bis dato auf Ebene der Datenschutzreferentinnen und -referenten der Länder entwickelten und besprochenen Vorentwürfen.

Mit Blick auf die unmittelbare Geltung der DS-GVO in den Mitgliedstaaten (Artikel 288 des Vertrages über die Arbeitsweise der Europäischen Union) kommt es zu einer grundlegenden strukturellen Änderung hinsichtlich des anzuwendenden allgemeinen und bereichsspezifischen Datenschutzrechts. Eine bloße Änderung des HmbDSG ist aus diesem Grund nicht ausreichend. Der Gesetzentwurf fasst das Hamburgische Datenschutzgesetz neu mit folgenden Regelungsschwerpunkten:

– Festgelegt werden die Stellen und Einrichtungen, die dem HmbDSG unterfallen.

  Im Interesse eines bundesweit einheitlichen Datenschutzrechts und -niveaus in den Ländern wird der Anwendungsbereich der Verordnung (EU) 2016/679 auf einzelne Verarbeitungsvorgänge erstreckt, die nicht unmittelbar dem Unionsrecht unterfallen. Zur Vermeidung von Datenschutzlücken werden hier im Vierten Abschnitt öffentliche Auszeichnungen und Ehrungen sowie Begnadigungsverfahren erfasst.

– Es werden in den Grenzen der DS-GVO fachspezifische gesetzliche Voraussetzungen geschaffen, unter denen personenbezogene Daten zu anderen Zwecken verwendet werden dürfen als denjenigen, zu denen sie ursprünglich verarbeitet wurden. In den übrigen Fällen gilt eine strenge Zweckbindung.

– Es werden zwecks Ausführung der DS-GVO Regelungen zu besonderen Verarbeitungssituationen getroffen, u.a. die Verarbeitung personenbezogener Daten von Beschäftigten, zu Forschungs- und Statistikzwecken sowie zu künstlerischen Zwecken.

– Es erfolgt eine terminologische Anpassung des Landesrechts an die DS-GVO.

– Die Bestimmungen über die Datenschutzaufsichtsbehörde werden weiter an das Datenschutzrecht der EU angepasst.

– Es werden die gesetzlichen Voraussetzungen geschaffen, unter denen die in der DS-GVO vorgesehenen Betroffenenrechte nach Maßgabe unionsrechtlicher Vorgaben eingeschränkt werden dürfen.

– Anpassungen des Hamburgischen Transparenzgesetzes sowie des Hamburgischen Ausführungsgesetzes zum Bundesmeldegesetz.

Für die Bürgerinnen und Bürger sowie die Verwaltung der Freien und Hansestadt Hamburg entsteht durch dieses Gesetz kein neuer Erfüllungsaufwand. Soweit mit der Stärkung der Betroffenenrechte und der Erweiterung technischer Anforderungen an die Datensicherheit ein erhöhter Erfüllungsaufwand verbunden ist, resultiert dieser unmittelbar aus der DS-GVO und nicht aus diesem Gesetz.

3. **Kosten**

Die Anpassungen begründen weitere Informationspflichten seitens der Verwaltung, deren Kosten derzeit noch nicht beziffert werden können. Diese beruhen jedoch auf der DS-GVO und nicht auf diesem Gesetz.

4. **Petitum**

Der Senat beantragt, die Bürgerschaft wolle das anliegende Gesetz beschließen.

Gesetz
zur Anpassung des Hamburgischen Datenschutzgesetzes sowie weiterer Vorschriften an die Verordnung (EU) 2016/679

Vom . . . .

Artikel 1

Hamburgisches Datenschutzgesetz (HmbDSG)

Inhaltsübersicht

Erster Abschnitt

Allgemeine Vorschriften

§ 1

Zweck

Dieses Gesetz trifft die zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, 72) ergänzenden Regelungen. Darüber hinaus regelt dieses Gesetz für im Einzelnen bezeichnete Situationen die Verarbeitung personenbezogener Daten, die nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 fallen.

§ 2
Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch folgende Stellen und Einrichtungen der Freien und Hansestadt Hamburg (öffentliche Stellen):

1. Behörden,
2. den Rechnungshof,
3. die Bürgerschaft, die Gerichte und die Behörden der Staatsanwaltschaft, soweit sie Verwaltungsaufgaben wahrnehmen,
4. die der Aufsicht der Freien und Hansestadt Hamburg unterstehenden juristischen Personen des öffentlichen Rechts und deren öffentlich-rechtlich organisierte Einrichtungen,
5. Stellen, soweit sie als Beliehene hoheitliche Aufgaben wahrnehmen,
6. sonstige öffentlich-rechtlich organisierte Stellen oder Einrichtungen.

(2) Für juristische Personen, Gesellschaften und andere Vereinigungen von Personen des privaten Rechts, an denen die Freie und Hansestadt Hamburg oder eine ihrer Aufsicht unterstehende juristische Person des öffentlichen Rechts beteiligt ist, gelten die Vorschriften der Verordnung (EU) 2016/679 sowie des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) über nicht-öffentliche Stellen in ihrer jeweils geltenden Fassung.

(3) Soweit öffentliche Stellen im Sinne des Absatzes 1 als Unternehmen am Wettbewerb teilnehmen, sind auf diese unbeschadet anderer Rechtsgrundlagen die Vorschriften der Verordnung (EU) 2016/679 sowie des Bundesdatenschutzgesetzes über nicht-öffentliche Stellen in ihrer jeweils geltenden Fassung anzuwenden.

(4) Dieses Gesetz gilt nicht für öffentliche Stellen, soweit deren Tätigkeit der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 S. 89) unterfällt.

(5) Die Bürgerschaft, ihre Mitglieder, ihre Gremien, die Fraktionen und Gruppen sowie deren Verwaltungen unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie zur Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten und dabei die von der Bürgerschaft zu erlassende Datenschutzordnung anzuwenden haben.

(6) Fällt die Verarbeitung personenbezogener Daten durch die in Absatz 1 bezeichneten öffentlichen Stellen nicht in den Anwendungsbereich der Verordnung (EU) 2016/679, sind ihre Vorschriften entsprechend anzuwenden, es sei denn, dieses Gesetz oder andere spezielle Rechtsvorschriften enthalten abweichende Regelungen.

§ 3
Datengeheimnis

(1) Denjenigen Personen, die bei den in § 2 Absatz 1 genannten öffentlichen Stellen oder ihren auftragnehmenden Stellen dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, insbesondere bekannt zu geben oder zugänglich zu machen. Dieses Verbot besteht auch nach Beendigung der Tätigkeit fort.

(2) Die Datenschutzbeauftragten nach Artikel 37 bis 39 der Verordnung (EU) 2016/679 der in § 2 Absatz 1 genannten öffentlichen Stellen sind, auch nach Beendigung ihrer Tätigkeit, zur Verschwiegenheit über die Identität Betroffener und Beschäftigter, die sich an sie gewandt haben, sowie über Umstände, die Rückschlüsse auf diese Personen zulassen, verpflichtet.

Zweiter Abschnitt
Grundsätze der Verarbeitung personenbezogener Daten

§ 4
Zulässigkeit der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten durch eine der in § 2 Absatz 1 genannten öffentlichen Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

§ 5
Erhebung personenbezogener Daten

(1) Bei nicht-öffentlichen Dritten sollen personenbezogene Daten nur unter den in § 6 Absatz 2 genannten Voraussetzungen erhoben werden.

(2) Werden personenbezogene Daten bei Dritten erhoben, sind diese auf Verlangen über den Erhebungszweck zu unterrichten, soweit dadurch schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden. Werden die Daten auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, ist auf die Auskunftspflicht, sonst auf die Freiwilligkeit der Angaben hinzuweisen.

§ 6

Zweckbindung

(1) Vom Zweck einer Verarbeitung personenbezogener Daten einschließlich solcher im Sinne von Artikel 9 der Verordnung (EU) 2016/679 erfasst ist auch die Verarbeitung zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung, zur Durchführung von Organisationsuntersuchungen sowie zu Zwecken der Datensicherung, Datenschutzkontrolle oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage. Dies gilt auch für die Verarbeitung personenbezogener Daten zu Aus- und Fortbildungszwecken, soweit nicht berechtigte Interessen der betroffenen Person an der Geheimhaltung der Daten offensichtlich überwiegen.

(2) Eine Verarbeitung personenbezogener Daten zu anderen als den ursprünglichen Zwecken ist zulässig, wenn

1. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit erforderlich ist,
2. dies zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,
3. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Erledigung eines gerichtlichen Auskunftsersuchens erforderlich sind und gesetzliche Regelungen nicht entgegenstehen,
4. dies erforderlich ist, um Angaben der betroffenen Person zu überprüfen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. bei Teilnahme am Privatrechtsverkehr oder zur Durchsetzung öffentlich-rechtlicher Forderungen ein rechtliches Interesse an der Kenntnis der zu verarbeitenden Daten vorliegt und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Personen an der Geheimhaltung überwiegt,
6. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und diese in Kenntnis des anderen Zwecks ihre Einwilligung erteilen würde,
7. die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen werden durften oder entnommen werden dürfen oder die Daten verarbeitende Stelle sie veröffentlichen dürfte, es sei denn, dass schutzwürdige Interessen der betroffenen Personen offensichtlich entgegenstehen,
8. sie der Bearbeitung von Eingaben, parlamentarischen Anfragen oder Aktenvorlageersuchen der Bürgerschaft dient und überwiegende schutzwürdige Interessen der betroffenen Personen nicht entgegenstehen,
9. es zur Durchführung wissenschaftlicher oder historischer Forschung oder Statistik erforderlich ist, das Interesse an der Durchführung des Forschungs- oder Statistikvorhabens das Interesse der Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Forschungs- oder Statistikzweck auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Unterliegen die personenbezogenen Daten einem Berufsgeheimnis und sind sie der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufspflicht übermittelt worden, findet Absatz 2 keine Anwendung.

(4) Sind mit personenbezogenen Daten weitere Daten der betroffenen Person oder Dritter derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so sind auch die Kenntnisnahme, die Weitergabe innerhalb des Verantwortlichen und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, zulässig, soweit nicht schutzwürdige Belange der betroffenen Person oder Dritter überwiegen. Die nicht erforderlichen Daten unterliegen insoweit einem Verarbeitungsverbot.

§ 7

Automatisierte Verfahren und Gemeinsame Dateien

Die Einrichtung eines automatisierten Abrufverfahrens oder einer gemeinsamen automatisierten Datei, in oder aus der mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten, ist zulässig, soweit dies unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können.

§ 8

Verantwortung bei der Offenlegung personenbezogener Daten

(1) Die Verantwortung für die Rechtmäßigkeit einer Offenlegung personenbezogener Daten durch deren Übermittlung, Verbreitung oder eine sonstige Form der Bereitstellung trägt die offenlegende Stelle.

(2) Erfolgt eine Offenlegung personenbezogener Daten durch deren Übermittlung, Verbreitung oder eine sonstige Form der Bereitstellung auf Grund eines

Ersuchens einer öffentlichen Stelle, trägt diese die Verantwortung für die Einhaltung des Datenschutzes. Die offenlegende Stelle prüft nur, ob das Ersuchen im Rahmen der Aufgaben der Empfängerin oder des Empfängers liegt, es sei denn, dass im Einzelfall Anlass zur Prüfung der Rechtmäßigkeit der Datenverarbeitung besteht. Die ersuchende Stelle hat in dem Ersuchen die für diese Prüfung erforderlichen Angaben zu machen.

(3) Bei Nutzung eines automatisierten Abrufverfahrens trägt die abrufende Stelle die Verantwortung für die Rechtmäßigkeit des Abrufes.

Dritter Abschnitt

Besondere Verarbeitungssituationen

§ 9

Videoüberwachung

(1) Die Beobachtung öffentlich zugänglicher Bereiche mit optisch-elektronischen Einrichtungen (Videobeobachtung) ist nur zulässig, soweit und solange sie

1. zur Aufgabenerfüllung öffentlicher Stellen oder
2. zur Wahrnehmung des Hausrechts

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Beobachtung nicht-öffentlich zugänglicher Bereiche ist über die in Satz 1 genannten Voraussetzungen hinaus nur zulässig, soweit und solange dies zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte erforderlich ist.

(2) Die Speicherung (Videoaufzeichnung) oder Verwendung der nach Absatz 1 erhobenen Daten ist zulässig, soweit und solange sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Eine Verarbeitung zu einem anderen Zweck ist nur zulässig, wenn dies zur Verfolgung von Straftaten oder zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte erforderlich ist.

(3) Videobeobachtung und Videoaufzeichnung sowie die verantwortliche Stelle sind zum frühestmöglichen Zeitpunkt durch geeignete Maßnahmen erkennbar zu machen.

§ 10

Verarbeitung von Beschäftigtendaten

(1) Die in § 2 Absatz 1 genannten öffentlichen Stellen dürfen personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ihrer Bewerberinnen und Bewerber, Beschäftigten, früheren Beschäftigten und von deren Hinterbliebenen nur verarbeiten, soweit dies eine Rechtsvorschrift, ein Tarifvertrag, eine allgemeine Regelung der obersten Dienstbehörde, die mit den Spitzenorganisationen der zuständigen Gewerkschaften und Berufsverbände beziehungsweise mit den Berufsverbänden der Richterinnen und Richter verbindlich vereinbart worden ist, oder eine Dienstvereinbarung vorsieht. Soweit derartige Regelungen nicht bestehen, gelten ergänzend zur Verordnung (EU) 2016/679 die Absätze 2 bis 7.

(2) Die in § 2 Absatz 1 genannten öffentlichen Stellen dürfen, soweit die nachfolgenden Absätze keine besonderen Regelungen enthalten, personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 der in Absatz 1 genannten Personen nur verarbeiten, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung oder des Personaleinsatzes, erforderlich ist.

(3) §§ 85 bis 92 des Hamburgischen Beamtengesetzes (HmbBG) vom 15. Dezember 2009 (HmbGVBl. S. 405), zuletzt geändert am 4. April 2017 (HmbGVBl. S. 99), in der jeweils geltenden Fassung sind auf diejenigen in Absatz 1 genannten Personen entsprechend anzuwenden, die nicht in den Anwendungsbereich dieser Vorschriften fallen.

(4) Eine Übermittlung der Daten von Beschäftigten an Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, soweit

1. die Stelle, der die Daten übermittelt werden sollen, ein überwiegendes rechtliches Interesse darlegt,
2. Art oder Zielsetzung der Aufgaben, die der oder dem Beschäftigten übertragen sind, die Übermittlung erfordert

oder

3. offensichtlich ist, dass die Übermittlung im Interesse der betroffenen Person liegt, und keine Anhaltspunkte vorliegen, dass diese in Kenntnis des Übermittlungszweckes ihre Einwilligung nicht erteilen würde.

Die Übermittlung an eine künftige Dienstherrin oder Arbeitgeberin oder einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung der betroffenen Person zulässig, es sei denn, dass eine Abordnung oder Versetzung vorbereitet wird, die der Zustimmung der oder des Beschäftigten nicht bedarf. Absatz 3 in Verbindung mit § 89 HmbBG bleibt unberührt.

(5) Verlangt eine in § 2 Absatz 1 genannte öffentliche Stelle medizinische oder psychologische Untersuchungen oder Tests (Untersuchungen), so hat sie

Anlass und Zweck der Untersuchung anzugeben sowie erforderlichenfalls auf die der betroffenen Person obliegenden Aufgaben hinzuweisen. Sie darf von der untersuchenden Stelle nur die Mitteilung der Untersuchungsergebnisse sowie derjenigen festgestellten Risikofaktoren verlangen, deren Kenntnis für ihre Entscheidung in personellen Angelegenheiten der betroffenen Person erforderlich ist; darüber hinausgehende Daten darf sie nur verlangen, soweit auch deren Kenntnis für ihre Entscheidung erforderlich ist. Führt eine in §2 Absatz 1 genannte öffentliche Stelle die Untersuchungen durch, so gilt für die Weitergabe der erhobenen Daten Satz 2 entsprechend. Im Übrigen ist eine Weiterverarbeitung der bei den Untersuchungen erhobenen Daten ohne Einwilligung der betroffenen Person nur zu dem Zweck zulässig, zu dem sie erhoben worden sind.

(6) Personenbezogene Daten, die vor der Eingehung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Beschäftigungsverhältnis nicht zustande kommt. Dies gilt nicht, soweit überwiegende berechtigte Interessen der Daten verarbeitenden Stelle der Löschung entgegenstehen oder die betroffene Person in die weitere Speicherung einwilligt. Nach Beendigung eines Beschäftigungsverhältnisses sind personenbezogene Daten zu löschen, soweit diese Daten nicht mehr benötigt werden, es sei denn, dass Rechtsvorschriften entgegenstehen.

(7) Soweit Daten der Beschäftigten im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach Artikel 32 der Verordnung (EU) 2016/679 gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

(8) §11 bleibt unberührt.

§11

Datenverarbeitung zum Zwecke wissenschaftlicher und historischer Forschung sowie Statistik

(1) Die in §2 Absatz 1 genannten Stellen dürfen für bestimmte Vorhaben personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke verarbeiten, soweit schutzwürdige Interessen der betroffenen Personen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Einer Einwilligung bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der betroffenen Person erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann oder erheblich beeinträchtigt würde. Die an die in Satz 1 genannten Stellen übermittelten personenbezogenen Daten dürfen nur mit Einwilligung der betroffenen Personen weiter übermittelt oder für einen anderen als den ursprünglichen Zweck verarbeitet werden.

(2) Personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 sind, soweit und sobald der Forschungs- oder Statistikzweck dies zulässt, dergestalt zu verändern, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (Anonymisierung), es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Anderenfalls sind sie sobald möglich zu pseudonymisieren (Artikel 4 Nummer 5 der Verordnung (EU) 2016/679). Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck oder die berechtigten Interessen der betroffenen Person dies erfordern. §22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

(3) Die wissenschaftliche oder historische Forschung oder Statistik betreibenden öffentlichen Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. die betroffene Person eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(4) An Dritte oder Stellen, die den Vorschriften dieses Gesetzes nicht unterliegen, dürfen personenbezogene Daten nur übermittelt werden, wenn diese sich verpflichten, die Bestimmungen der Absätze 2 und 3 einzuhalten.

(5) Das Recht auf Auskunft nach Artikel 15 der Verordnung (EU) 2016/679, auf Berichtigung nach Artikel 16 der Verordnung (EU) 2016/679, auf Einschränkung der Verarbeitung nach Artikel 18 der Verordnung (EU) 2016/679 und auf Widerspruch nach Artikel 21 der Verordnung (EU) 2016/679 bestehen nicht, soweit die Wahrnehmung dieser Rechte die Verwirklichung des wissenschaftlichen oder historischen Forschungszwecks oder des Statistikzwecks voraussichtlich unmöglich machen oder ernsthaft beeinträchtigen würde.

§12

Datenverarbeitung zu künstlerischen Zwecken

(1) Soweit personenbezogene Daten zu künstlerischen Zwecken verarbeitet werden, gelten von den

Kapiteln II bis VII sowie IX der Verordnung (EU) 2016/679 nur Artikel 5 Absatz 1 Buchstaben b und f sowie die Artikel 24, 32 und 33.

(2) Führt die Verarbeitung personenbezogener Daten gemäß Absatz 1 zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Gerichtsentscheidungen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, so sind diese Gegendarstellungen, Verpflichtungserklärungen, Gerichtsentscheidungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren, wie die Daten selbst sowie bei einer Offenlegung der Daten gemeinsam offenzulegen.

(3) Die Absätze 1 und 2 gelten auch für nichtöffentliche Stellen.

Vierter Abschnitt

Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 fallenden Tätigkeiten

§ 13

Öffentliche Auszeichnungen und Ehrungen

(1) Zur Vorbereitung öffentlicher Auszeichnungen und Ehrungen dürfen die zuständigen Stellen die dazu erforderlichen Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Kenntnis der betroffenen Person verarbeiten. Auf Anforderung der in Satz 1 genannten Stellen dürfen andere öffentliche Stellen die zur Vorbereitung der Auszeichnung oder Ehrung erforderlichen Daten übermitteln.

(2) Eine Verarbeitung dieser personenbezogenen Daten für andere Zwecke ist nur mit Einwilligung der betroffenen Person zulässig.

(3) Die Absätze 1 und 2 finden keine Anwendung, wenn der Daten verarbeitenden Stelle bekannt ist, dass die betroffene Person ihrer öffentlichen Auszeichnung oder Ehrung oder der mit ihr verbundenen Datenverarbeitung widersprochen hat.

(4) Es besteht weder eine Informationspflicht noch eine Auskunftspflicht des Verantwortlichen.

§ 14

Begnadigungsverfahren

In Begnadigungsverfahren ist die Verarbeitung personenbezogener Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 und Artikel 10 der Verordnung (EU) 2016/679 zulässig, soweit sie zur Ausübung des Gnadenrechts durch die zuständigen Stellen erforderlich ist. Entsprechend anzuwenden sind nur Artikel 5 bis 7 sowie Kapitel IV mit Ausnahme von Artikel 33 der Verordnung (EU) 2016/679.

Fünfter Abschnitt

Rechte der Betroffenen

§ 15

Beschränkung der Informationspflicht

(1) Eine Information gemäß Artikel 13 oder 14 der Verordnung (EU) 2016/679 erfolgt nicht, soweit und solange

1. die Information die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten ist,
3. dies zur Verfolgung von Straftaten und Ordnungswidrigkeiten erforderlich ist,
4. dies die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder
5. eine Weiterverarbeitung analog gespeicherter Daten vorgenommen wird, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem ursprünglichen Erhebungszweck gemäß der Verordnung (EU) 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist.

(2) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten an Behörden und Stellen der Staatsanwaltschaft, der Polizei, der Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, der Behörden des Verfassungsschutzes, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes und, soweit die Sicherheit des Bundes berührt wird, anderen Behörden des Bundesministeriums der Verteidigung, ist mit diesen zuvor Einvernehmen herzustellen.

(3) Wird nach Absatz 1 Nummern 1 bis 3 und 5 oder Absatz 2 von einer Information der betroffenen Person abgesehen, hat der Verantwortliche die Gründe hierfür zu dokumentieren.

§ 16

Beschränkung des Auskunftsrechts

(1) Anträge auf Auskunftserteilung nach Artikel 15 der Verordnung (EU) 2016/679 können abgelehnt werden, soweit und solange

1. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die Auskunft dazu führen würde, dass Sachverhalte, die nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind, aufgedeckt werden, oder
3. dies zur Verfolgung von Straftaten und Ordnungswidrigkeiten erforderlich ist.

(2) Die Ablehnung einer Auskunft bedarf keiner Begründung, soweit durch die Begründung der Zweck der Ablehnung gefährdet würde. In diesem Fall sind die wesentlichen Gründe für die Entscheidung zu dokumentieren. Wird der betroffenen Person keine Auskunft erteilt, so ist sie darauf hinzuweisen, dass sie sich an die Hamburgische Beauftragte bzw. den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit wenden kann. Auf ihr Verlangen ist der oder dem Beauftragten für Datenschutz und Informationsfreiheit die Auskunft zu erteilen, soweit nicht die jeweils zuständige Behörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde.

(3) Bezieht sich die Auskunft auf die Herkunft personenbezogener Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, von Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, sowie vom Bundesnachrichtendienst, Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, von anderen Behörden des Bundesministeriums der Verteidigung, ist mit diesen zuvor Einvernehmen herzustellen. Gleiches gilt, soweit sich die Auskunft auf die Übermittlung personenbezogener Daten an diese Behörden bezieht.

§ 17

Beschränkung der Löschungspflicht

Ergänzend zu Artikel 18 Absatz 1 Buchstaben b und c der Verordnung (EU) 2016/679 gilt Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 nicht, soweit und solange der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung personenbezogener Daten schutzwürdige Interessen der betroffenen Person beeinträchtigt werden. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Der Verantwortliche benachrichtigt die betroffene Person über die Einschränkung der Verarbeitung.

§ 18

Beschränkung der Benachrichtigungspflicht

(1) Der Verantwortliche kann von der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person gemäß Artikel 34 der Verordnung (EU) 2016/679 absehen, soweit und solange die Benachrichtigung

1. die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, oder
2. zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist, oder
3. dazu führen würde, dass Sachverhalte, personenbezogenen Daten oder die Tatsache ihrer Verarbeitung, die nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind, aufgedeckt würden, oder
4. die Funktionsfähigkeit von Datenverarbeitungssystemen einer öffentlichen Stelle gefährden würde.

(2) Wenn nach Absatz 1 von einer Benachrichtigung abgesehen wird, ist die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zu informieren.

Sechster Abschnitt

Die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

§ 19

Zuständigkeit

(1) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist Aufsichtsbehörde im Sinne des Artikels 51 Absatz 1 der Verordnung (EU) 2016/679.

(2) Die oder der Beauftragte für Datenschutz und Informationsfreiheit überwacht bei den in § 2 Absatz 1 genannten öffentlichen Stellen und bei anderen Stellen, soweit sie sich auf Grund gesetzlicher Vorschriften ihrer bzw. seiner Überwachung unterworfen haben, die Einhaltung der Vorschriften über den Datenschutz. Sie oder er ist zudem zuständige Aufsichtsbehörde nach § 40 des Bundesdatenschutzgesetzes für die Datenverarbeitung nicht-öffentlicher Stellen.

(3) Die Bürgerschaft und der Rechnungshof unterliegen der Überwachung durch die Hamburgische Beauftragte bzw. den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit nur, soweit sie

in Verwaltungsangelegenheiten tätig werden. Beim Rechnungshof überwacht die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit darüber hinaus, ob die erforderlichen technischen und organisatorischen Maßnahmen nach Artikel 32 der Verordnung (EU) 2016/679 getroffen und eingehalten werden.

(4) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist im Rahmen der ihr oder ihm durch Artikel 57 der Verordnung (EU) 2016/679 sowie dieses Gesetzes zugewiesenen Aufgaben zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten.

(5) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist zuständig für die Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Verordnung (EU) 2016/679.

(6) Für die Aufsicht über die Verarbeitung personenbezogener Daten im Rahmen der Verwaltung landesrechtlich geregelter Steuern ist die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig, soweit die Datenverarbeitung auf bundesgesetzlich geregelten Besteuerungsgrundlagen oder auf bundeseinheitlichen Festlegungen beruht.

§ 20

Ernennungsvoraussetzungen

Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit muss die Befähigung zum Richteramt oder für die Laufbahn Allgemeine Dienste in der Laufbahngruppe 2 mit Zugang zum zweiten Einstiegsamt haben und die zur Erfüllung ihrer bzw. seiner Aufgaben erforderliche Fachkunde besitzen.

§ 21

Rechtsstellung

(1) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit steht in einem öffentlich-rechtlichen Amtsverhältnis zur Freien und Hansestadt Hamburg, in das sie bzw. er gemäß Artikel 60a Absatz 3 der Verfassung der Freien und Hansestadt Hamburg berufen wird.

(2) Das Amtsverhältnis beginnt mit der Aushändigung der Ernennungsurkunde durch die Präsidentin oder den Präsidenten der Bürgerschaft. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit leistet vor der Präsidentin oder dem Präsidenten der Bürgerschaft folgenden Eid: „Ich schwöre, das Grundgesetz für die Bundesrepublik Deutschland, die Verfassung der Freien und Hansestadt Hamburg und alle in der Bundesrepublik Deutschland geltenden Gesetze zu wahren und meine Amtspflichten gewissenhaft zu erfüllen, so wahr mir Gott helfe.“ Der Eid kann auch ohne religiöse Beteuerungsformel geleistet werden.

(3) Das Amtsverhältnis endet mit Ablauf der Amtszeit oder durch Entlassung. Die Entlassung wird mit der Zustellung der Entlassungsurkunde wirksam.

(4) Für den Fall ihrer oder seiner Verhinderung bestimmt die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit eine Beamtin oder einen Beamten ihrer bzw. seiner Behörde zur Vertreterin oder zum Vertreter. Die Vertretungsbefugnis besteht nach dem Ende der Amtszeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit bis zur Ernennung einer Amtsnachfolgerin oder eines Amtsnachfolgers fort.

(5) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit erhält Fürsorge und Schutz wie eine Beamtin oder ein Beamter der Besoldungsgruppe B 4 des Hamburgischen Besoldungsgesetzes vom 26. Januar 2010 (HmbGVBl. S. 23), zuletzt geändert am 18. Juli 2017 (HmbGVBl. S. 214), in der jeweils geltenden Fassung, im Beamtenverhältnis auf Zeit, insbesondere Besoldung, Versorgung, Erholungsurlaub und Beihilfe im Krankheitsfall. Die Inanspruchnahme von Urlaub hat sie oder er ihrer oder seiner Vertretung anzuzeigen.

(6) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit unterliegt der Rechnungsprüfung durch den Rechnungshof nur, soweit ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

§ 22

Besondere Pflichten

(1) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit darf neben ihrem bzw. seinem Amt kein anderes besoldetes Amt ausüben. Sie oder er darf keine entgeltlichen oder unentgeltlichen Tätigkeiten ausüben, die mit ihrem bzw. seinem Amt nicht vereinbar sind. § 10 Absätze 1 bis 3 und § 11 Absatz 1 des Senatsgesetzes vom 18. Februar 1971 (HmbGVBl. S. 23), zuletzt geändert am 12. November 2014 (HmbGVBl. S. 484), in der jeweils geltenden Fassung gelten entsprechend. Sie oder er darf kein Gewerbe und keinen Beruf ausüben, gegen Entgelt keine außergerichtlichen Gutachten abgeben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft eines Landes oder des Bundes angehören. Sie oder er hat der Präsidentin oder dem Präsidenten der Bürgerschaft Mitteilung über Geschenke zu machen, die sie bzw. er in Bezug auf das Amt erhält; diese oder dieser entscheidet dann über die Verwendung der Geschenke.

(2) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr bzw. ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Sie oder er entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie bzw. er über solche Angelegenheiten vor Gericht oder außergerichtlich aussagt oder Erklärungen abgibt; wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit erforderlich. Sagt sie oder er als Zeugin oder Zeuge aus und betrifft die Aussage Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung des Senats zuzurechnen sind oder sein könnten, darf sie bzw. er nur im Benehmen mit dem Senat aussagen.

§ 23

Tätigkeit nach Beendigung des Amtsverhältnisses

(1) Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit sieht für die Dauer von zwei Jahren nach Beendigung der Amtszeit von allen mit den Aufgaben des früheren Amtes nicht zu vereinbarenden Handlungen und entgeltlichen Tätigkeiten ab.

(2) Ehemalige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit haben der Präsidentin oder dem Präsidenten der Bürgerschaft die Aufnahme einer Erwerbstätigkeit oder sonstigen ständigen Beschäftigung außerhalb des öffentlichen Dienstes, öffentlicher Unternehmen, öffentlich-rechtlicher Körperschaften, Anstalten und Stiftungen schriftlich anzuzeigen. Die Anzeigepflicht besteht für einen Zeitraum von zwei Jahren nach Beendigung des Amtsverhältnisses.

(3) Die Präsidentin oder der Präsident der Bürgerschaft soll die Erwerbstätigkeit oder sonstige ständige Beschäftigung untersagen, soweit sie mit dem Amt der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit nicht zu vereinbaren ist. Die Untersagung ist innerhalb von vierzehn Tagen nach Eingang der Anzeige nach Absatz 1 und für einen bestimmten Zeitraum auszusprechen. Das Verbot endet spätestens mit Ablauf von zwei Jahren nach Beendigung des Amtsverhältnisses.

(4) Bei freiberuflichen Tätigkeiten sind die entsprechenden Regelungen in den Berufsordnungen zur Vermeidung von Interessenkollisionen zu beachten; sie gehen dieser Regelung vor.

§ 24

Befugnisse und Rechte

(1) Zusätzlich zu den Befugnissen aus Artikel 58 der Verordnung (EU) 2016/679 ist die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zur Erfüllung ihrer oder seiner Aufgaben befugt, jederzeit Zugang zu Diensträumen zu erhalten. Diese Befugnis kann die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit auf ihre oder seine Mitarbeiterinnen und Mitarbeiter übertragen.

(2) Ergänzend zu Artikel 59 der Verordnung (EU) 2016/679 hat die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit die Befugnis, die Öffentlichkeit im Rahmen ihrer oder seiner Zuständigkeit zu informieren.

(3) Die Befugnis Geldbußen zu verhängen, steht der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gegenüber Behörden und öffentlichen Stellen mit Ausnahme der in § 2 Absatz 3 genannten Stellen nicht zu.

§ 25

Verwaltungsgebühren

(1) Für Amtshandlungen, die der Kontrolle nichtöffentlicher Stellen durch die Aufsichtsbehörde nach § 40 des Bundesdatenschutzgesetzes dienen, werden Gebühren, Zinsen und Auslagen erhoben. Der Senat wird ermächtigt, die gebührenpflichtigen Tatbestände und die Gebührensätze im Einvernehmen mit der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit durch Rechtsverordnung festzulegen.

(2) Zur Zahlung der Gebühren, Zinsen und Auslagen ist die kontrollierte Stelle verpflichtet. Wird die Kontrolle weder von der Aufsichtsbehörde noch von der oder dem Datenschutzbeauftragten der kontrollierten Stelle veranlasst, gilt dies jedoch nur, wenn Mängel festgestellt werden.

(3) In den Fällen des Artikels 57 Absatz 4 der Verordnung (EU) 2016/679 kann die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Anfragenden eine Gebühr von bis zu 1000 Euro auferlegen.

Siebenter Abschnitt

Strafvorschriften, Ordnungswidrigkeiten

§ 26

Strafvorschrift

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer gegen Entgelt oder in der Absicht, sich oder eine andere bzw. einen anderen zu

bereichern oder eine andere bzw. einen anderen zu schädigen, personenbezogene Daten, die nicht offenkundig sind, unbefugt nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 verarbeitet oder durch Vortäuschung falscher Tatsachen an sich oder eine andere bzw. einen anderen übermitteln lässt.

(2) Der Versuch ist strafbar.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche und die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit.

(4) Die Absätze 1 bis 3 finden nur Anwendung, soweit die Tat nicht nach anderen Vorschriften mit Strafe bedroht ist.

§27

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer personenbezogene Daten, die nicht offenkundig sind,

1. unbefugt verarbeitet, oder
2. durch Vortäuschung falscher Tatsachen an sich oder eine andere Person übermitteln lässt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfundzwanzigtausend Euro geahndet werden.

Artikel 2

Änderung des Hamburgischen Hochschulgesetzes

§111 des Hamburgischen Hochschulgesetzes vom 18. Juli 2001 (HmbGVBl. S. 171), zuletzt geändert am 28. November 2017 (HmbGVBl. S. 365), wird wie folgt geändert:

1. Absatz 1 Satz 1 erhält folgende Fassung: „Die Hochschulen dürfen diejenigen personenbezogenen Daten von Studienbewerberinnen und Studienbewerbern, Studierenden, Prüfungskandidatinnen und Prüfungskandidaten, Absolventinnen und Absolventen und anderen ehemaligen Studierenden sowie Nutzerinnen und Nutzern von Hochschuleinrichtungen verarbeiten, die für die Identifikation, die Zulassung, die Immatrikulation, die Erhebung von Beiträgen und Gebühren nach den §§6a und 6b, die Rückmeldung, die Beurlaubung, die Teilnahme an Lehrveranstaltungen, die Prüfungen, die Nutzung von Hochschuleinrichtungen, die Hochschulplanung, die Sicherung und Verbesserung der Qualität in Studium und Lehre sowie die Kontaktpflege mit ehemaligen Hochschulmitgliedern erforderlich sind.“
2. Absatz 2 wird wie folgt geändert:
   a) In Satz 4 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.
   b) In Satz 5 wird das Wort „Verwendung“ durch das Wort „Verarbeitung“ ersetzt.
3. Absatz 2a wird wie folgt geändert:
   a) Hinter Satz 2 wird folgender Satz eingefügt: „Für die weitere Verarbeitung bedarf es einer ausdrücklichen Einwilligung.“
   b) Im neuen Satz 5 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.
4. Absatz 3 erhält folgende Fassung: „(3) Die Hochschulen können diejenigen personenbezogenen Daten des wissenschaftlichen und künstlerischen Personals verarbeiten, die zur Beurteilung der Lehr- und Forschungstätigkeit, des Studienangebotes und des Ablaufs von Studium und Prüfungen, für Planungs- und Organisationsentscheidungen, zur Erfüllung des Gleichstellungsauftrags sowie zur Kontaktpflege mit ehemaligen Mitgliedern erforderlich sind.“
5. Absatz 4 wird wie folgt geändert:
   a) In Satz 1 wird das Wort „zusammenführen“ durch das Wort „verarbeiten“ ersetzt.
   b) In Satz 3 wird das Wort „Nutzung“ durch das Wort „Verarbeitung“ ersetzt.
6. Absatz 5 Satz 1 wird wie folgt geändert:
   a) In Nummer 1 werden die Wörter „erhoben und“ gestrichen.
   b) In Nummer 2 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.
   c) In Nummer 3 werden die Wörter „erhoben und“ gestrichen.
   d Die Nummern 4 und 5 erhalten folgende Fassung:

   „4. welche Daten nach den Absätzen 2a und 3 verarbeitet werden dürfen, sowie das Verfahren ihrer Verarbeitung,

5. welche Daten nach Absatz 4 Satz 1 verarbeitet werden dürfen und wie die gemeinsame Datei nach Absatz 4 Satz 2 auszugestalten ist; Betroffene können sich zur Wahrnehmung ihrer Rechte auf Auskunft, Berichtigung, Sperrung und Löschung an jede der beteiligten Stellen wenden.“
7. Absatz 7 erhält folgende Fassung:

   „(7) Soweit die Auskunftspflicht der Hochschulen nach dem Hochschulstatistikgesetz vom 2. November 1990 (BGBl. I S. 2414), zuletzt geändert am 7. Dezember 2016 (BGBl. I S. 2826, 2833), in der jeweils geltenden Fassung, auch Daten umfasst, die die Hochschulen nicht nach den Absätzen 1 bis 6 verarbeiten, so sind die Hochschulen unabhängig hiervon befugt, diese Daten der betreffenden Personen ausschließlich für Aufgaben nach dem Hochschulstatistikgesetz entsprechend den statistikrechtlichen Anforderungen zu verarbeiten."

Artikel 3

Änderung des Hamburgischen Transparenzgesetzes

§ 14 des Hamburgischen Transparenzgesetzes vom 19. Juni 2012 (HmbGVBl. S. 271) wird wie folgt geändert:

1. Absatz 1 Satz 2 wird gestrichen.
2. In Absatz 2 Satz 2 wird das Wort „Berufung" durch das Wort „Ernennung" und die Textstelle „§§ 21 und 22 des Hamburgischen Datenschutzgesetzes" durch die Textstelle „§§ 20 und 21 des Hamburgischen Datenschutzgesetzes vom… (einzusetzen sind die Daten des Neuerlasses des Hamburgischen Datenschutzgesetzes durch Artikel 1 des vorliegenden Gesetzes)… (HmbGVBl. S. …) in der jeweils geltenden Fassung" ersetzt.

Artikel 4

Änderung des Hamburgischen Ausführungsgesetzes zum Bundesmeldegesetz

Das Hamburgische Ausführungsgesetz zum Bundesmeldegesetz vom 15. Juli 2015 (HmbGVBl. S. 193) wird wie folgt geändert:

1. § 1 Absatz 3 wird wie folgt geändert:
   a) In Satz 1 wird die Textstelle „gemäß § 10 Satz 1 des Hamburgischen Datenschutzgesetzes (HmbDSG) vom 5. Juli 1990 (HmbGVBl. S. 133, 165, 226), zuletzt geändert am 5. April 2013 (HmbGVBl. S. 148, 155), in der jeweils geltenden Fassung" gestrichen.
   b) Satz 2 erhält folgende Fassung: „Die zentrale Meldebehörde ist für das Melderegister insgesamt verantwortlich."
2. § 4 Absatz 2 wird wie folgt geändert:
   a) In Satz 1 werden die Wörter „und genutzt" gestrichen.
   b) Satz 2 wird gestrichen.
3. § 6 Absatz 2 wird wie folgt geändert:
   a) In Satz 1 wird das Wort „verwendet" durch das Wort „verarbeitet" ersetzt.
   b) Satz 2 wird gestrichen.

Artikel 5

Aufhebung der Hochschuldatenverordnung

Die Hochschuldatenverordnung vom 24. November 1992 (HmbGVBl. S. 248) in der geltenden Fassung wird aufgehoben.

Artikel 6

Verordnungsermächtigung

Der Senat wird ermächtigt, Rechtsverordnungen auf Grund der §§ 11 und 11a des Hamburgischen Datenschutzgesetzes vom 5. Juli 1990 (HmbGVBl. S. 133, 165, 226) in der bis zum 24. Mai 2018 geltenden Fassung durch Rechtsverordnung aufzuheben.

Artikel 7

Schlussbestimmungen

(1) Dieses Gesetz tritt am 25. Mai 2018 in Kraft. Zum selben Zeitpunkt tritt das Hamburgische Datenschutzgesetz vom 5. Juli 1990 (HmbGVBl. S. 133, 165, 226) in der geltenden Fassung außer Kraft.

(2) Mit Inkrafttreten dieses Gesetzes ist die oder der amtierende Hamburgische Beauftragte für Datenschutz und Informationsfreiheit aus dem Beamtenverhältnis auf Zeit entlassen. Ab dem Zeitpunkt der Entlassung nimmt sie oder er bis zum Ende der nach Artikel 7 des Gesetzes zur weiteren Stärkung der Unabhängigkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vom 20. Dezember 2016 (HmbGVBl. S. 570) laufenden Amtszeit das Amt in einem öffentlich-rechtlichen Amtsverhältnis gemäß Artikel 1 § 21 dieses Gesetzes wahr.

Begründung zum Entwurf eines Gesetzes zur Anpassung des Hamburgischen Datenschutzgesetzes (HmbDSG) sowie weiterer Vorschriften an die Verordnung (EU) 2016/679

A.

Allgemeiner Teil

Am 25. Mai 2016 ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Verordnung (EU) 2016/679) in Kraft getreten. Gemäß ihrem Artikel 99 Absatz 2 gilt sie ab dem 25. Mai 2018. Abweichend von der bisherigen Rechtslage ist das Datenschutzrecht nun nicht mehr in einer ins nationale Recht umgesetzten Richtlinie (gegenwärtig 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) geregelt, sondern vorrangig durch eine EU-Verordnung, die gemäß Artikel 288 Absatz 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) grundsätzlich unmittelbar anwendbares Recht schafft.

Ein wesentliches, durch die Verordnung (EU) 2016/679 zu erreichendes Ziel ist es, in den EU-Mitgliedstaaten ein möglichst einheitliches und gleichwertiges Schutzniveau bei der Verarbeitung personenbezogener Daten herzustellen (vgl. Erwägungsgrund 10 und 13 zur Verordnung (EU) 2016/679). Die in der ausdrücklich als „Grundverordnung“ bezeichneten Verordnung getroffenen Bestimmungen belassen den Mitgliedstaaten der Europäischen Union indes Regelungsspielräume, denn sie enthalten zum einen konkrete Rechtsetzungsaufträge, zum anderen Regelungsoptionen (Spezifizierungs-/Öffnungsklauseln).

Mit der Verordnung (EU) 2016/679 entsteht somit Anpassungsbedarf sowohl hinsichtlich des allgemeinen als auch des bereichsspezifischen Landesdatenschutzrechts, soweit nicht in der Verordnung selbst enthaltene Spezifizierungs-/Öffnungsklauseln ein Festhalten an bestehenden gesetzlichen Bestimmungen zulassen. Dem dient der vorliegende Gesetzentwurf. Angesichts ihrer unmittelbaren Geltung (Artikel 288 AEUV) kommt es zu einer grundlegenden strukturellen Änderung hinsichtlich des anzuwendenden allgemeinen und bereichsspezifischen Datenschutzrechts. Eine bloße Änderung des HmbDSG ist aus diesem Grund nicht ausreichend.

Durch dieses Gesetz wird insbesondere das Hamburgische Datenschutzgesetz (HmbDSG) in einer Neufassung an die Vorgaben des EU-Rechts angepasst. Dabei sind Regelungen, die der Verordnung (EU) 2016/679 widersprechen, und solche, welche deren Regelungsinhalt lediglich wiederholen, aufzuheben. Darüber hinaus sind Regelungsaufträge umzusetzen. Von den Regelungsoptionen wird in einer Weise Gebrauch gemacht, dass bestehende unionsrechtliche Vorgaben vollständig beachtet und bereits bewährte Instrumente des Landesrechts damit in Ausgleich gebracht werden.

Dabei ist von folgenden unionsrechtlichen Vorgaben auszugehen:

Angesichts der unmittelbaren Geltung der Verordnung (EU) 2016/679 in allen Mitgliedstaaten der EU (vgl. Artikel 288 Absatz 2 AEUV) ist – bestätigt durch die Rechtsprechung des Europäischen Gerichtshofs (u.a. EuGH, Urt. v. 10. Oktober 1973 – Rs. 34/73, Slg. 1975, 981 – Variola; EuGH, Urt. v. 31. Januar 1978 – Rs. 94/77, Slg. 1978, 99 – Zerbone) – eine wiederholende Wiedergabe von Inhalten einer EU-Verordnung im nationalen Recht grundsätzlich ausgeschlossen, um nicht die Herkunft des Rechtsakts, dessen unmittelbare Geltung sowie die Jurisdiktion des Gerichtshofs zu verschleiern. Die Verordnung (EU) 2016/679 lässt hiervon lediglich in sehr engen Grenzen Ausnahmen zu (vgl. Erwägungsgrund 8 zur Verordnung (EU) 2016/679).

In der Verordnung (EU) 2016/679 sind allgemeine und besondere Öffnungs-/Spezifizierungsklauseln vorgesehen, die den mitgliedstaatlichen Gesetzgebern einräumen, spezifische Regelungen über die Verarbeitung personenbezogener Daten zu erlassen oder – sofern bereits vorhanden – beizubehalten. Die wesentliche allgemeine Norm findet sich in Artikel 6 der Verordnung (EU) 2016/679. Sie erlaubt den Mitgliedstaaten der EU unter den dort genannten Voraussetzungen den Erlass oder die Beibehaltung spezifischer Normen betreffend die Datenverarbeitung. Darüber hinaus enthält die Verordnung (EU) 2016/679 spezielle Öffnungsklauseln für mitgliedstaatliche Regelungen zur Ausgestaltung des Medienprivilegs (Artikel 85), der Beschäftigtendatenverarbeitung (Artikel 88) und zur Ausgestaltung der Datenverarbeitung zu im öffentlichen Interesse liegenden Archiv-, Forschungs- und Statistikzwecken (Artikel 89).

Der unionsweit möglichst einheitliche Schutz personenbezogener Daten verlangt u.a. eine präzise Festlegung von Rechten betroffener Personen. Diese sind in erster Linie in den Artikeln 12 ff., 34 der Verordnung (EU) 2016/679 niedergelegt. Das Unionsrecht lässt indes unter engen Voraussetzungen Beschränkungen dieser Rechte durch mitgliedstaatliche Normen zu. Zentrale Norm hierfür ist Artikel 23 der Verordnung (EU) 2016/679. Die Betroffenenrechte einschränkenden Vorschriften des mitgliedstaatlichen Rechts müssen gemäß dieser Norm den Wesensgehalt der Grundrechte und Grundfreiheiten achten und eine notwendige und verhältnismäßige Maßnahme darstellen. Darüber hinaus kommen Einschränkungen der Betroffenenrechte lediglich aus den dort abschließend aufgeführten Gründen in Betracht. Schließlich müssen die die Betroffenenrechte einschränkenden Gesetze die Vorgaben des Artikels 23 Absatz 2 der Verordnung (EU) 2016/679 beachten. Spezielle Bestimmungen betreffend die Einschränkung von Betroffenenrechten enthalten auch Artikel 14 Absatz 5, Artikel 17 Absatz 1 Buchstabe e, Absatz 3, Artikel 85 Absatz 2 und Artikel 89 Absatz 2 und 3 der Verordnung (EU) 2016/679.

Die mitgliedstaatlichen Gesetzgeber sind durch Artikel 54 der Verordnung (EU) 2016/679 verpflichtet, Vorschriften über eine unabhängige Aufsichtsbehörde zu schaffen bzw. bestehende Regelungen anzupassen. Des Weiteren sind die Normen, die auch nach Geltungsbeginn der Verordnung (EU) 2016/679 bestehen bleiben können, inhaltlich und terminologisch an das neue Datenschutzrecht der EU anzupassen. Schließlich sind Vorschriften zu erlassen, um die Regelungsaufträge und -optionen gemäß der Verordnung (EU) 2016/679 wahrzunehmen. Dabei ist auch den bereits erfolgten Änderungen des Datenschutzrechts auf Bundesebene – in erster Linie dem Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I 2017, 2097) –, insbesondere bei der Gestaltung von Normverweisen, Rechnung zu tragen.

Der Gesetzentwurf fasst das Hamburgische Datenschutzgesetz neu mit folgenden Regelungsschwerpunkten:

- Festgelegt werden die Stellen und Einrichtungen, die dem HmbDSG unterfallen. Im Interesse eines einheitlichen Datenschutzniveaus wird der Anwendungsbereich der Verordnung (EU) 2016/679 auch auf solche Stellen und Verarbeitungsvorgänge erstreckt, die nicht dem Unionsrecht unterfallen.
- Es werden fachspezifische gesetzliche Voraussetzungen geschaffen, unter denen personenbezogene Daten zu anderen Zwecken verwendet werden dürfen als denjenigen, zu denen sie ursprünglich erhoben bzw. verarbeitet wurden. Zudem wird festgelegt, welche Verarbeitungszwecke miteinander kompatibel sind. In den übrigen Fällen gilt eine strenge Zweckbindung.
- Es werden zwecks Ausführung der Verordnung (EU) 2016/679 Regelungen zu besonderen Verarbeitungssituationen getroffen, u.a. die Verarbeitung personenbezogener Daten von Beschäftigten sowie zu Forschungs- und Statistikzwecken.
- Die Bestimmungen über die Datenschutzaufsichtsbehörde werden weiter an die Vorschriften des EU-Rechts angepasst.
- Es werden die gesetzlichen Voraussetzungen geschaffen, unter denen die in der Verordnung (EU) 2016/679 vorgesehenen Betroffenenrechte nach Maßgabe der unionsrechtlichen Vorgaben eingeschränkt werden dürfen.

Die Gesetzgebungskompetenz für das allgemeine Datenschutzrecht des HmbDSG ergibt sich aus Artikel 30, 70 Absatz 1 Grundgesetz in Verbindung mit Artikel 73, 74 Grundgesetz. Den Ländern steht das Recht der Gesetzgebung danach dann zu, soweit das Grundgesetz nicht dem Bund Gesetzgebungskompetenzen verleiht. Der Bereich öffentlicher Landesverwaltung der Freien und Hansestadt Hamburg ist nicht durch Bundesrecht geregelt; die Regelungskompetenz steht hinsichtlich des Datenschutzrechts uneingeschränkt der Freien und Hansestadt Hamburg zu.

Des Weiteren an die Verordnung (EU) 2016/679 angepasst wird das Hamburgische Hochschulgesetz. Neben terminologischen und redaktionellen Anpassungen bedarf es einer Änderung mit Blick auf spezifische Anforderungen des EU-Datenschutzrechts an Einwilligungen. Die Verordnung über die Angabe personenbezogener Daten gegenüber Hochschulen ist zwischenzeitlich gegenstandslos geworden, sodass sie im Wege der Rechtsbereinigung aufzuheben ist.

Terminologischen und redaktionellen Anpassungen bedürfen darüber hinaus sowohl das Hamburgische Transparenzgesetz (HmbTG) als auch das Hamburgische Gesetz zur Ausführung des Bundesmeldegesetzes.

Für die Bürgerinnen und Bürger der Freien und Hansestadt Hamburg entsteht durch dieses Gesetz kein neuer Erfüllungsaufwand. Mit der Stärkung der Betroffenenrechte durch die Verordnung (EU) 2016/679, etwa im Bereich der Informationspflichten (Artikel 13, 14 der Verordnung (EU) 2016/679), ist ein erhöhter Erfüllungsaufwand zulasten der Verwaltung verbunden. Dieser resultiert indes aus dem Unionsrecht selbst, nicht hingegen aus diesem Gesetz. Vielmehr führt die Wahrnehmung der Regelungsoptionen insbesondere gemäß Artikel 23 der Verordnung (EU) 2016/679 zu einem geringeren Erfüllungsaufwand als unionsrechtlich ohne Wahrnehmung von Modifikationsbefugnissen vorgesehen.

Für die Hamburgische Beauftragte bzw. den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit führt das Gesetz zu keinem Aufgabenzuwachs. Auch insoweit resultieren die zusätzlichen Aufgaben und Befugnisse aus dem Unionsrecht. Die wesentlichen Anpassungen an die Verordnung (EU) 2016/679 mit Blick auf die Aufsichtsbehörden sind bereits mit Gesetz vom 20. Dezember 2016 (HmbGVBl. S. 570) erfolgt.

Soweit landesrechtliche Regelungen auf das HmbDSG verweisen bzw. Bezug nehmen, sind Anpassungen durch die Ressorts im Rahmen ihrer eigenen Zuständigkeiten vorzunehmen.

B.

Besonderer Teil

Zu Artikel 1 § 1 (Zweck)

Den einzelnen Vorschriften des Gesetzes wird eine allgemeine Zweckbestimmung vorangestellt. Das Gesetz verfolgt nach Satz 1 zum einen den Zweck, die zur Anpassung an die Verordnung (EU) 2016/679 (ABl. EU (2016) Nr. L 119 vom 4. Mai 2016, S. 1; berichtigt ABl. EU (2016) Nr. L 314 v. 22. November 2016, S. 72) ergänzenden Regelungen zu treffen und gleichzeitig spezifische Anforderungen an die Verarbeitung personenbezogener Daten zu bestimmen. In Bezug genommen werden damit die in der Verordnung (EU) 2016/679 enthaltenen Regelungsaufträge einschließlich der durch sie eingeräumten Regelungsoptionen. Möglich ist, sofern durch die Verordnung zugelassen, die Normierung spezifischer, konkretisierender Bestimmungen, Ergänzungen und Modifikationen. § 1 des Gesetzes hebt die Wahrnehmung dieser Aufträge und Optionen hervor, um sowohl den Gesetzesanwendern als auch den betroffenen Personen zu verdeutlichen, dass angesichts des Vorrangs des Unionsrechts vor nationalem Recht in erster Linie die Verordnung (EU) 2016/679 anzuwenden ist und dieses Gesetz insoweit lediglich Ergänzungen und Modifikationen an solchen Stellen vornimmt, die die Verordnung (EU) 2016/679 den Mitgliedstaaten einräumt.

Über den so umschriebenen Gesetzeszweck hinaus verfolgt das Gesetz gemäß Satz 2 das Ziel, einzelne Verarbeitungssituationen zu regeln, die nicht in den unionsrechtlichen Anwendungsbereich nach Artikel 2 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 fallen. Diese werden – neben der in § 2 Absatz 5 des Gesetzes geregelten besonderen Situation der parlamentarischen Arbeit der Bürgerschaft – im Vierten Abschnitt geregelt. Vor Inkrafttreten dieses Gesetzes bestehende bereichsspezifische Regelungen in dort nicht aufgeführten Verarbeitungssituationen werden nicht berührt.

Zu Artikel 1 § 2 (Anwendungsbereich)

Mit § 2 des Gesetzes wird dessen persönlicher und sachlicher Anwendungsbereich beschrieben. Aufgeführt werden zunächst die Stellen und Einrichtungen, für die das HmbDSG gilt (Absatz 1). Abgrenzungen erfolgen zum Geltungsbereich des Bundesdatenschutzgesetzes (Absatz 2 und 3) sowie für Tätigkeitsbereiche, die der Richtlinie (EU) 2016/680 unterfallen (Absatz 4). Für die Bürgerschaft erfolgt eine gesonderte Regelung (Absatz 5). Absatz 6 schließlich erstreckt den Geltungsbereich der Verordnung (EU) 2016/679 und dieses Gesetzes auf im Einzelnen bestimmte Verarbeitungssituationen, die nicht dem Anwendungsbereich des Unionsrechts unterliegen. Einer Abgrenzung zum VwVfG bedarf es nicht, da sich in § 3 b VwVfG eine entsprechende Regelung findet.

Zu Absatz 1:

Die Vorschrift zählt positiv auf, welches die Normadressaten des Gesetzes sind. Wie bereits nach bisheriger Rechtslage regelt das Gesetz lediglich die Verarbeitung personenbezogener Daten im öffentlichen Bereich des Landes. Die Begriffe „Verarbeitung“ und „personenbezogene Daten“ sind dabei unter ausschließlicher Anwendung von Artikel 4 Nummer 1 und Nummer 2 der Verordnung (EU) 2016/679 auszulegen. Mangels einer entsprechenden Definitionsnorm auf Ebene der Verordnung (EU) 2016/679 definiert das Gesetz für diese Zwecke den Begriff „öffentliche Stelle“. Vom Anwendungsbereich des Gesetzes erfasst sein sollen grundsätzlich alle öffentlichen Stellen, soweit sie personenbezogene Daten verarbeiten. Das Gesetz stellt dabei im Grundsatz auf die Institution im organisationsrechtlichen Sinn ab, soweit nichts Abweichendes geregelt ist.

Adressat des Gesetzes sind nach Nummer 1 Behörden. Für den Begriff der Behörde ist auf die Bestimmung des § 1 Absatz 2 HmbVwVfG zu rekurrieren. Behörde ist danach jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

Dem Anwendungsbereich des Gesetzes unterfällt auch der Rechnungshof (Nummer 2).

Erfasst werden des Weiteren die Bürgerschaft, die Gerichte und die Behörden der Staatsanwaltschaft (Nummer 3). Rücksicht ist insoweit jedoch zum einen zu nehmen auf die unterschiedlichen Funktionen, die diese Institutionen und Einrichtungen wahrnehmen. Die Bürgerschaft hat vorwiegend legislative Aufgaben, die Gerichte und Behörden der Staatsanwaltschaft vorwiegend solche im Bereich der Justiz. Sie alle verfügen somit über eine besondere Stellung im gewaltengeteilten System. Daher sollen sie lediglich insoweit erfasst sein, als sie allgemeine Verwaltungsaufgaben wahrnehmen und als Behörde agieren. Verwaltungsaufgaben in diesem Sinn sind die Funktionen, die darauf gerichtet sind, die finanziellen, organisatorischen und personellen Voraussetzungen für ihre Tätigkeit zu schaffen und zu unterhalten. Zum anderen ist zu berücksichtigen, dass auf ihre Tätigkeit außerhalb von Verwaltungsaufgaben besondere Rechtsgrundlagen anwendbar sind. Für die Gerichte gilt in erster Linie die Verordnung (EU) 2016/679 und im Übrigen das BDSG (vgl. § 1 Absatz 1 BDSG) sowie – dem BDSG vorgehend – das Prozessrecht. Für die Behörden der Staatsanwaltschaft gilt die StPO, ergänzend das BDSG. Hinsichtlich der parlamentarischen Tätigkeit der Bürgerschaft sieht Absatz 5 eine Sonderregelung vor.

Vom Anwendungsbereich umfasst sein sollen darüber hinaus die der Aufsicht der Freien und Hansestadt Hamburg unterstehenden juristischen Personen des öffentlichen Rechts und deren öffentlich-rechtlich organisierte Einrichtungen (Nummer 4). Die der Freien und Hansestadt zustehenden Kontroll- und Weisungsrechte gegenüber diesen Stellen und Einrichtungen rechtfertigen deren Einbeziehung in den Anwendungsbereich des Landesdatenschutzrechts. Zugleich wird damit von der durch § 1 Absatz 1 BDSG eingeräumten Möglichkeit einer landesrechtlichen Regelung Gebrauch gemacht.

Beliehene sollen ebenfalls den Regelungen des Landesdatenschutzrechts unterstellt werden, da sie in ihrer Funktion als Beliehene Teil der öffentlichen Gewalt sind (Nummer 5).

Als Auffangtatbestand werden sonstige öffentlich-rechtlich organisierte Stellen und Einrichtungen erfasst (Nummer 6). Die Erfassung sonstiger Stellen und Einrichtungen beugt Gesetzeslücken mit Blick auf den umfassenden Anwendungsbereich der Verordnung (EU) 2016/679 vor und erfasst solche Stellen und Einrichtungen, die nicht als Behörde im Sinne von Nummer 1 oder als sonst zuvor genannte Stelle oder Einrichtung anzusehen sind.

Zu Absatz 2:

Entsprechend der bisherigen Rechtslage sollen juristische Personen, Gesellschaften und andere Vereinigungen privaten Rechts, auch wenn an ihnen eine Mehrheitsbeteiligung der Freien und Hansestadt Hamburg besteht, nicht den Regeln dieses Gesetzes, sondern den für den nicht-öffentlichen Bereich geltenden Rechtsvorschriften unterstellt werden. Dies sind vorrangig die Verordnung (EU) 2016/679 und ergänzend das Bundesdatenschutzgesetz. Spezialgesetzliche Regelungen gehen zudem nach allgemeiner juristischer Methodik den allgemeinen Bestimmungen vor.

Zu Absatz 3:

Die Anwendbarkeit des Gesetzes wird in Absatz 3 ausgeschlossen für am Wettbewerb teilnehmende öffentliche Stellen und Einrichtungen im Sinne von Absatz 1. Auch sie unterfallen stattdessen den für nicht-öffentliche Stellen geltenden Regelungen der Verordnung (EU) 2016/679 und ergänzend denen des Bundesdatenschutzgesetzes. Verarbeiten die von Absatz 3 erfassten Stellen Daten für andere als für wettbewerbliche Zwecke, gilt ergänzend dieses Gesetz. Dies betrifft etwa den Bereich der Personaldatenverarbeitung.

Zu Absatz 4:

Mit Absatz 4 wird der Anwendungsbereich weiter negativ abgegrenzt. Neben den bereits in den vorstehenden Absätzen genannten Stellen und Einrichtungen sollen die Behörden der Staatsanwaltschaft zusätzlich zu der in Absatz 1 Nummer 2 bezeichneten Einschränkung auch dann nicht von den Vorschriften dieses Gesetzes erfasst sein, sofern und soweit sich ihre Tätigkeit im Anwendungsbereich der Richtlinie (EU) 2016/680 bewegt. Das Gesetz vollzieht damit die durch Artikel 2 der Verordnung (EU) 2016/679 vorgegebene Trennlinie nach. Die Umsetzung der für den Justiz- und Polizeibereich geltenden Richtlinie erfolgt in den fachspezifischen Gesetzen, nicht hingegen im allgemeinen Landesdatenschutzrecht.

Zu Absatz 5:

Die Bürgerschaft einschließlich der aus dem Gesetzeswortlaut ersichtlichen Unterteilungen ist im Rahmen der Erfüllung ihrer parlamentarischen Aufgaben vom Anwendungsbereich sowohl des Unionsrechts als auch dieses Gesetzes ausgenommen. Wie bereits nach gegenwärtiger Rechtslage gibt sich die Bürgerschaft eine eigene Datenschutzordnung. Hinsichtlich der Wahrnehmung von Verwaltungsaufgaben ist der Anwendungsbereich des Gesetzes indes auch für die Bürgerschaft uneingeschränkt eröffnet.

Zu Absatz 6:

Zwecks Vermeidung einer parallelen Anwendung unterschiedlicher Datenschutzrechtsregime im Bereich des allgemeinen Datenschutzrechts wird der Anwendungsbereich der Verordnung (EU) 2016/679 auf solche Verarbeitungssituationen erstreckt, die nicht in den sachlichen Anwendungsbereich des EU-Rechts fallen, wie er in Artikel 2 der Verordnung (EU) 2016/679 umschrieben ist. Diese werden – neben der Sonderregelung in Absatz 5 – im Vierten Abschnitt dieses Gesetzes behandelt. Hervorzuheben und einer Regelung bedürfen insbesondere die Datenverarbeitung bei Verleihung öffentlicher Ehrungen und Auszeichnungen sowie in Begnadigungsverfahren.

Zu Artikel 1 §3 (Datengeheimnis)

Zu Absatz 1:

Mit der Vorschrift führt das Gesetz die nach bisheriger Rechtslage bestehende allgemeine gesetzliche Verpflichtung zur Wahrung des Datengeheimnisses in §7 HmbDSG a.F. fort. Hierdurch wird eine gesonderte Verpflichtung der Mitarbeiterinnen und Mitarbeiter der in §2 Absatz 1 genannten Stellen zur Wahrung des Datengeheimnisses entbehrlich.

Erfasst werden sämtliche Personen bei den in §2 Absatz 1 genannten Stellen und Einrichtungen, die im Rahmen ihrer Tätigkeit Kenntnis von personenbezogenen Daten nehmen können. Eine faktische Zugangsmöglichkeit ist ausreichend. Darüber hinaus werden auch alle diejenigen Personen erfasst, die im Rahmen einer Auftragsdatenverarbeitung (Artikel 28 der Verordnung (EU) 2016/679) Kenntnis von personenbezogenen Daten erhalten können.

Zu Absatz 2:

Das Gesetz enthält auf Grund der weitgehend abschließenden Regelung behördlicher Datenschutzbeauftragter in Artikel 37–39 der Verordnung (EU) 2016/679 keine eigenen Bestimmungen über die Pflicht zur Benennung behördlicher Datenschutzbeauftragte, deren Stellung oder Aufgaben, auch, da von der Möglichkeit zur Erweiterung der Aufgaben nach mitgliedstaatlichem Recht kein Gebrauch gemacht wird. Unionsrechtlich geregelt sind darüber hinaus ein Abberufungs- und Benachteiligungsverbot. Hinsichtlich des Abberufungsverbots trifft Artikel 38 der Verordnung (EU) 2016/679 indes nur eine Teilregelung. Einer besonderen Vorschrift über die Abberufung aus anderen Gründen als der Amtsführung (etwa aus betriebsbedingten Gründen) bedarf es im Landesrecht indes nicht, da insoweit bundesrechtliche Vorschriften entsprechend anzuwenden sind, z.B. §626 Bürgerliches Gesetzbuch. Eine Vorschrift betreffend den Kündigungsschutz ist im Landesrecht ebenfalls nicht zu treffen, da hierfür keine Gesetzgebungskompetenz besteht (vgl. Artikel 74 Absatz 1 Nummer 12 Grundgesetz) und das BDSG eine entsprechende Vorschrift enthält.

Behördliche Datenschutzbeauftragte bei den in §2 Absatz 1 genannten Stellen sind – in Wahrnehmung der Regelungsoption in Artikel 38 Absatz 5 der Verordnung (EU) 2016/679 – über Absatz 1 hinaus gesetzlich darauf zu verpflichten, die ihnen während ihrer Tätigkeit als Datenschutzbeauftragte zur Kenntnis gelangten Informationen geheim und vertraulich zu halten. Dies betrifft über die in Absatz 1 bestehende Geheimhaltungspflicht hinaus diejenigen Daten, die einen Rückschluss auf konkrete Personen zulassen. Dabei kann es sich nicht nur um betroffene Personen handeln, sondern auch um in den Behörden beschäftigte Mitarbeiterinnen und Mitarbeiter, die sich an behördliche Datenschutzbeauftragte gewandt haben. Die Verschwiegenheitspflicht behördlicher Datenschutzbeauftragter erstreckt sich in zeitlicher Hinsicht über das Ende ihrer Tätigkeit hinaus. Sie besteht lediglich dann nicht, wenn die jeweils betroffene Person den behördlichen Datenschutzbeauftragten von der Pflicht zur Verschwiegenheit befreit hat oder eine Äußerung behördlicher Datenschutzbeauftragter über geheim zu haltende Umstände gesetzlich zugelassen ist. In keiner Konstellation darf einer betroffenen Person aus der Anrufung des Datenschutzbeauftragten ein Nachteil erwachsen. Dies folgt bereits aus Artikel 38 Absatz 4 der Verordnung (EU) 2016/679, der betroffenen Personen ausdrücklich das Recht zugesteht sich an den Datenschutzbeauftragten zu wenden.

Zu Artikel 1 §4 (Zulässigkeit der Verarbeitung personenbezogener Daten)

Die Norm schafft eine allgemeine Rechtsgrundlage für die Datenverarbeitung auf der Grundlage von Artikel 6 Absatz 1 Buchstabe e in Verbindung mit Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679. Der Schaffung einer solchen Vorschrift im nationalen Recht bedarf es, weil Artikel 6 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 selbst keine Rechtsgrundlage für die Verarbeitung von Daten darstellt, sondern einen Regelungsauftrag erteilt, wie sich aus der Formulierung in Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 ergibt. Dem wird mit §4 nachgekommen.

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen gemäß der Generalklausel des §4 ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Beides kann sowohl aus nationalen Rechtsvorschriften als auch aus EU-Vorgaben folgen. Die Verarbeitung personenbezogener Daten ist allerdings nicht nur auf dieser Rechtsgrundlage zulässig, sondern auch auf Grundlage der weiteren in Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Erlaubnistatbestände einschließlich der auf der Grundlage der Verordnung (EU) 2016/679 erlassenen bereichsspezifischen Regelungen. Dass zudem eine Einwilligung als Rechtsgrundlage zur Verarbeitung personenbezogener Daten infrage kommt, ergibt sich unmittelbar aus Artikel 6 Absatz 1 Satz 1 Buchstabe a der Verordnung (EU) 2016/679.

Terminologisch erfolgt eine Anpassung des Landesrechts an den umfassenden Begriff der „Verarbeitung“ personenbezogener Daten, wie er in Artikel 4

Nummer 2 der Verordnung (EU) 2016/679 definiert wird. Dieser Begriff umfasst „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Zu Artikel 1 §5 (Erhebung personenbezogener Daten)

Die Verordnung (EU) 2016/679 verlangt – anders als das bisher geltende Datenschutzrecht – nicht die vorrangige Erhebung personenbezogener Daten beim Betroffenen (sog. Grundsatz der Direkterhebung), sondern stellt die Erhebung beim Betroffenen und die Erhebung bei Dritten gleichrangig nebeneinander. Kompensiert wird dies durch die Verordnung (EU) 2016/679 dadurch, dass sie weitreichende Informationspflichten (Artikel 13, 14) einführt, die die betroffenen Personen in die Lage versetzen, ihre Rechte in Bezug auf personenbezogene Daten wirksam wahrzunehmen. Auf diese Weise wird der auch durch den Grundsatz der Direkterhebung verfolgte Transparenzgedanke auf strukturell andere Weise verwirklicht als bisher. Es ist bislang ungeklärt, ob das Unionsrecht deshalb einer Normierung eines entsprechenden Grundsatzes im nationalen Recht unter Geltung der Verordnung (EU) 2016/679 entgegensteht. Für dessen Zulässigkeit spricht die Aufnahme des Transparenzgebots in Artikel 5 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679.

Zu Absatz 1:

Abweichend vom bisherigen Recht wird am Grundsatz der Direkterhebung nicht vollen Umfangs festgehalten. Vielmehr wird die vorrangige Beschaffung personenbezogener Daten bei der betroffenen Person dahingehend eingeschränkt, dass Daten bei nicht-öffentlichen Dritten nur unter den in §6 Absatz 2 genannten Voraussetzungen erhoben werden dürfen. Der Nachweis für das Vorliegen dieser Voraussetzungen ist von dem für die Datenverarbeitung Verantwortlichen zu erbringen (vgl. Artikel 5 Absatz 2 der Verordnung (EU) 2016/679). Gerade die Beschaffung personenbezogener Daten bei privaten Dritten ist besonders risikobehaftet, was die Aufrechterhaltung des Vorranges der Direkterhebung für diese Fälle rechtfertigt. Insoweit wird an der bisherigen Regelungstechnik (Zulässigkeit der Dritterhebung für Fälle einer zulässigen Zweckänderung) festgehalten.

Zu Absatz 2:

Die Verordnung (EU) 2016/679 regelt nicht die Pflicht zur Information Dritter, bei denen Daten erhoben wurden. Zu Gunsten privater Dritter folgte eine solche bisher aus §12a Absatz 4 HmbDSG a.F. Die Fortführung dieser Regelung erscheint angezeigt. Sie wird zudem erweitert auf Dritte, die dem öffentlichen Bereich zuzuordnen sind. Die Regelungsbefugnis hierzu ergibt sich aus Artikel 6 Absatz 2 und Absatz 3 der Verordnung (EU) 2016/679.

Die Unterrichtung über den Erhebungszweck soll „auf Verlangen“ erfolgen. Eine Unterrichtung von Amts wegen ist daher nicht erforderlich. Notwendig ist vielmehr, dass der Dritte ausdrücklich eine Unterrichtung begehrt. Ein solches Begehren kann formlos angebracht werden.

Zu Artikel 1 §6 (Zweckbindung)

Die Zweckbindung – unionsrechtlich normiert in Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 – zählt zu den wesentlichen Grundsätzen des Datenschutzrechts. Daten dürfen demzufolge grundsätzlich nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiter verarbeitet werden. §6 setzt die Geltung dieses Grundsatzes voraus. Von einer erneuten Normierung ist vor dem Hintergrund des unionsrechtlichen Normwiederholungsverbots (vgl. Erwägung 8 zur Verordnung (EU) 2016/679) abzusehen.

Zu Absatz 1:

In Absatz 1 wird beschrieben, welche Verarbeitungszwecke als vom ursprünglichen Zweck der Verarbeitung mitumfasst anzusehen sind. Hinsichtlich der Verarbeitung personenbezogener Daten zu Aus- und Fortbildungszwecken knüpft das Gesetz deren Verarbeitung an eine Abwägung mit berechtigten Interessen der Betroffenen an der Geheimhaltung. Deren Überwiegen, welches einer Verarbeitung entgegensteht, muss jedoch offensichtlich im Sinne einer für jedermann gegebenen Erkennbarkeit sein. Bei der Verarbeitung „zur Sicherstellung eines ordnungsgemäßen Betriebes eines Datenverarbeitungssystems“ ist eine Datenverarbeitung nur zulässig, wenn dies für den ordnungsgemäßen Betrieb der Datenverarbeitungsanlage erforderlich ist – „zur Sicherstellung“ ist insoweit enger zu verstehen als beispielsweise „Prüfung und Wartung“ und impliziert bereits terminologisch das Erfordernis einer Verhältnismäßigkeitsprüfung. Dieses Erfordernis wird derzeit in angemessener Weise durch die Freigaberichtlinie vom 4. April 2005 (MittVw S. 46) konkretisiert.

Zu Absatz 2:

Absatz 2 schafft für öffentliche Stellen im Rahmen ihrer jeweiligen Aufgabenerfüllung eine landesweite Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu einem anderen Zweck als demjenigen, für den sie ursprünglich erhoben wurden. Auf eine Vereinbarkeit der Zwecke der weiteren Verarbeitung mit den Zwecken, für die die Daten ursprünglich erhoben wurden, kommt es nicht an. Unberührt bleibt eine Datenverarbeitung zu anderen Zwecken, soweit die betroffene Person eine Einwilligung hierzu gemäß Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a der Verordnung (EU) 2016/679 gegeben hat.

Mit Absatz 2 wird von der in Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 eingeräumten Regelungsoption Gebrauch gemacht. Die Mitgliedstaaten der EU haben die Kompetenz, nationale Regelungen für Fälle vorzusehen, in denen der Zweck der weiteren Verarbeitung nicht mit dem ursprünglichen Datenverarbeitungszweck vereinbar ist, soweit die mitgliedstaatliche Regelung eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 der Verordnung (EU) 2016/679 genannten Ziele darstellt.

Unter geringfügiger Modifikation der bisherigen Regelung in §13 HmbDSG a.F. werden in Absatz 2 die Fälle normiert, in denen personenbezogene Daten zu anderen Zwecken verarbeitet werden dürfen als zu den Zwecken, zu denen sie ursprünglich erhoben wurden. Über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus ist von einer Rechtsetzungskompetenz nicht nur für Konstellationen auszugehen, in denen eine Unvereinbarkeit zwischen den Weiterverarbeitungszwecken und den ursprünglichen Zwecken besteht, sondern auch für solche, in denen Zwecke miteinander grundsätzlich zu vereinbaren sind (siehe Erwägungsgrund 50 zur Verordnung (EU) 2016/679).

In den Nummern 1 bis 9 sind zulässige Ausnahmen vom Gebot der Zweckbindung geregelt. Zulässig ist eine Zweckänderung demnach – außer in den Fällen, in denen der oder die Betroffene eine rechtswirksame Einwilligung erteilt hat – gemäß Nummer 1, wenn dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die normierten Rechtsgüter erforderlich ist.

Nummer 2 erlaubt eine Verarbeitung zu anderen Zwecken wenn dies zur Abwehr einer schwerwiegenden Beeinträchtigung von Rechten einer anderen Person erforderlich ist. Die Nummern 1 und 2 entsprechen weitestgehend der bisherigen Regelung in §13 Absatz 2 Nummer 4 HmbDSG a.F.

Nummer 3 entspricht der bisherigen Regelung in §13 Absatz 2 Nummer 5 HmbDSG a.F. und erlaubt Durchbrechungen der Zweckbindung, um die Verfolgung von Straftaten oder Ordnungswidrigkeiten, die Strafvollstreckung oder den Strafvollzug und weitere gerichtliche Maßnahmen zu ermöglichen.

Nummer 4 entspricht §13 Absatz 2 Nummer 3 HmbDSG a.F. und betont den Grundsatz rechtmäßiger und inhaltlich zutreffender Aufgabenerfüllung. Danach wird eine anderweitige Nutzung personenbezogener Daten ermöglicht, wenn tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen. Dies ist auch im Interesse der Betroffenen, die sich sonst zu einem späteren Zeitpunkt unter Umständen Erstattungsansprüchen der öffentlichen Verwaltung ausgesetzt sähen.

Nummer 5 entspricht §13 Absatz 2 Nummer 2 HmbDSG a.F. und erlaubt eine zweckändernde Datenverarbeitung, wenn die öffentliche Stelle wie ein privater Gläubiger ein Interesse an der Durchsetzung von Rechtsansprüchen hat und dazu nach einer Abwägung mit den Betroffeneninteressen die für andere Zwecke erhobenen Daten nutzt. Die öffentliche Stelle soll in diesem Fall nicht schlechter gestellt werden als ein privater Gläubiger, dem bei Vorliegen der gleichen Voraussetzungen personenbezogene Daten übermittelt würden. Vom Begriff der in Nummer 5 genannten öffentlich-rechtlichen Forderungen sind etwa solche erfasst, die dem Steuer- und Zollwesen zuzuordnen sind. Auch vollstreckbare Bußgeldforderungen fallen hierunter.

Nummer 6 (nach bisheriger Rechtslage normiert in §13 Absatz 2 Nummer 6) normiert den Fall einer mutmaßlichen Einwilligung (beispielsweise bei Bewusstlosen) und erlaubt eine zweckändernde Verarbeitung, wenn offensichtlich ist, dass die zweckändernde Verarbeitung im Interesse der betroffenen Person liegt und sie die Einwilligung erteilen würde.

Im Fall von Nummer 7 bestehen keine Bedenken gegen eine zweckändernde Verarbeitung, wenn die verwendeten Daten ohnehin schon von der öffentlichen Stelle aus allgemein zugänglichen Quellen rechtmäßig entnommen werden durften oder dürften oder die verarbeitende Stelle sie rechtmäßig veröffentlichen dürfte. Eine identische Regelung findet sich auch im bisherigen §13 Absatz 2 Nummer 7 HmbDSG a.F.

Nummer 8 entspricht mit leichten Modifikationen §13 Absatz 2 Nummer 8 HmbDSG a.F. und regelt eine Ausnahme für Eingaben, Aktenvorlageersuchen oder parlamentarische Anfragen der Bürgerschaft. Für Datenverarbeitungsvorgänge innerhalb der Bürgerschaft ist nach wie vor die Datenschutzordnung der Bürgerschaft maßgeblich. Die Bestimmung dient der Regelung der Datenverarbeitung anderer Stellen, die lediglich auf Anregung der Bürgerschaft (beispielsweise durch ein Aktenvorlageersuchen) geschieht. Spezielle Regelungen über den Datenschutz, wie z.B. den Sozialdatenschutz (vgl. §35 SGB I, §§67 ff. SGB X) gehen den Bestimmungen dieses Gesetzes vor.

Nummer 9 privilegiert Forschung, Wissenschaft und Statistik bei der Datenverarbeitung und ermöglicht, sofern diese erforderlich ist, eine zweckändernde Datennutzung nach strenger Abwägung mit den Interessen der Betroffenen.

Die Vorschrift erfasst sowohl Datenübermittlungen an Stellen außerhalb des Verantwortlichen (Artikel 4 Nummer 7 der Verordnung (EU) 2016/679) als auch Datenübermittlungen innerhalb der verantwortlichen Stelle. Beide sind gemäß der Datenschutz-Grundverordnung als Zweckänderung anzusehen.

Zu Absatz 3:

Artikel 6 Absätze 2 und 3 der Verordnung (EU) 2016/679 ausführend wird entsprechend der bisherigen Rechtslage eine weitere Datenverarbeitung zu anderen als den ursprünglichen Zwecken dann für nicht zulässig erklärt, wenn die zu verarbeitenden personenbezogenen Daten einem Berufsgeheimnis unterliegen. Die Regelung entspricht im Wesentlichen der bisherigen nach §13 Absatz 2 Satz 2 HmbDSG a.F.

Zu Absatz 4:

Mit Absatz 4 wird das bisher in §14 Absatz 2 HmbDSG a.F. normierte „Aktenprivileg“ fortgesetzt. Bei einer aktenmäßigen Verarbeitung personenbezogener Daten ist nicht stets gewährleistet, dass eine Trennung nach erforderlichen und nicht erforderlichen Daten mit verhältnismäßigem Aufwand erfolgen kann. Dieser faktischen Unmöglichkeit wird mit Absatz 4 Rechnung getragen, zugleich wird sie aber auch begrenzt, denn eine Trennung darf nur bei unverhältnismäßigem Aufwand unterbleiben. In diesen Fällen ist eine Offenlegung auch der nicht für den konkreten Zweck erforderlichen Daten zulässig. Notwendig ist jedoch eine Abwägung mit schutzwürdigen Belangen des Betroffenen oder Dritter. Sofern Ergebnis einer solchen Abwägung ist, dass die schutzwürdigen Belange der betroffenen Person bzw. Dritter überwiegen, hat gegebenenfalls auch eine Offenlegung der erforderlichen Daten zu unterbleiben. Um die Rechte betroffener Personen oder Dritter zu schützen, unterliegen die nicht erforderlichen Daten beim Empfänger einem Verarbeitungsverbot.

Zu Artikel 1 §7 (Automatisierte Verfahren und Gemeinsame Dateien)

Mit §7 werden materielle Anforderungen bei automatisierten Abrufverfahren und solchen Dateien normiert, die mehreren öffentlichen Stellen die Verarbeitung personenbezogener Daten in einem Datenbestand ermöglichen oder bei denen die beteiligten Stellen sich wechselseitig Zugriffe auf die gespeicherten personenbezogenen Daten gestatten sollen (gemeinsame Dateien). Die Regelung setzt damit u.a. die unionsrechtliche Vorgabe in Artikel 26 der Verordnung (EU) 2016/679 um. Zugleich führt sie den materiellrechtlichen Gehalt der bisherigen Regelungen in §§11, 11a HmbDSG a.F. fort. Der Bedarf für eine Fortführung dieser Bestimmungen ergibt sich v.a. aus dem Dataport-Verbund, dem die Freie und Hansestadt Hamburg angehört.

Die Norm regelt besondere Zulässigkeitsvoraussetzungen für den Betrieb automatisierter Abrufverfahren sowie gemeinsamer Dateien, d.h. solche Verfahren, bei denen mehrere öffentliche Stellen im Sinne von §2 Absatz 1 dieses Gesetzes die Verarbeitung personenbezogener Daten in einem gemeinsamen Datenbestand durchführen oder sich gegenseitig gestatten, auf die gespeicherten Daten zuzugreifen.

Das bisherige generelle formale Erfordernis aus §§11, 11a HmbDSG a.F., dass automatisierte Abrufverfahren sowie gemeinsame Dateien stets einer Rechtsvorschrift bedürfen, wird unter der Geltung der Verordnung (EU) 2016/679 aufgehoben. Auf Grund der Sicherungsmechanismen, die sich bereits unmittelbar aus der Verordnung ergeben, wie insbesondere die Datenschutz-Folgeabschätzung (Artikel 35), bedarf es dieser formalen Vorgabe, die sich in der Praxis häufig als hinderlich erwiesen hat, nicht länger. Auch mit Blick auf die anstehenden Digitalisierungsherausforderungen ist daran nicht mehr festzuhalten.

Zu Artikel 1 §8 (Verantwortung bei der Offenlegung personenbezogener Daten)

§8 legt als spezifische Bestimmung im Sinne von Artikel 6 Absätze 2 und 3 der Verordnung (EU) 2016/679 fest, wer im Falle einer Offenlegung, d.h. Übermittlung, Verbreitung oder sonstigen Form der Bereitstellung – legaldefiniert in Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 – die Verantwortung für die Datenverarbeitung bei den im Tatbestand bezeichneten Handlungen trägt.

Zu Absatz 1:

In Absatz 1 wird der Grundsatz festgelegt, dass die Verantwortung bei der datenoffenlegenden Stelle liegt. Diese hat vor einer Datenoffenlegung zu prüfen, ob die von ihr selbst vorgenommene Übermittlung, Weitergabe oder sonstige Verbreitung als Fallgruppen einer Datenverarbeitung mit Recht und Gesetz in Einklang steht.

Zu Absatz 2:

Im Falle eines Ersuchens einer anderen öffentlichen Stelle um Datenoffenlegung ist die Verantwortung hingegen eine geteilte: Auf das Ersuchen führt die ersuchte Stelle lediglich eine eingeschränkte Prüfung im Hinblick auf die Zugehörigkeit des Ersuchens zu den Aufgaben der ersuchenden Stelle durch. Wie bisher ist zudem eine Offenlegungsbefugnis erforderlich, deren Vorliegen von der offenlegenden Stelle vor Datenoffenlegung geprüft werden muss. Im Hinblick auf die inhaltliche Rechtmäßigkeit des Ersuchens liegt die Verantwortung hingegen im Wesentlichen bei der Behörde, die um die Bereitstellung der personenbezogenen Daten ersucht und sie weiter verarbeiten möchte. Die bereitstellende Behörde wird diesbezüglich weitgehend von einer Verantwortlichkeit freigestellt. Sie hat selbst lediglich dann eine Prüfung vorzunehmen, wenn sich Anhaltspunkte dafür ergeben, dass das Ersuchen nicht rechtmäßig ist bzw. eine Bereitstellung der Daten gegen Rechtsvorschriften verstößt. Um der offenlegenden Stelle die in Satz 2 beschriebene Prüfung des Ersuchens zu ermöglichen, hat die ersuchende Stelle nach Satz 3 die dafür erforderlichen Angaben zu machen.

Zu Absatz 3:

Absatz 3 behandelt den Sonderfall einer Datenoffenlegung durch automatisierten Abruf. In diesen Fällen verlagert sich die Verantwortlichkeit auf die abrufende Stelle, weil sie die Kontrolle über den konkreten Datenverarbeitungsvorgang (Abruf) hat.

Zu Artikel 1 § 9 (Videoüberwachung)

§ 9 passt die Anforderungen an die bisher in § 30 HmbDSG a.F. normierte Videoüberwachung an europarechtliche Vorgaben an. Einige nach bisheriger Rechtslage im Landesrecht geregelte Aspekte werden durch die Datenschutz-Grundverordnung bereits unmittelbar auf Unionsebene festgelegt und bedürfen keiner gesonderten Normierung im Recht der Mitgliedstaaten. Dies betrifft unter anderem das Recht auf Löschung (bisher: § 30 Absatz 5 HmbDSG), das in Artikel 17 der Verordnung (EU) 2016/679 geregelt ist. Die nach bisherigem Recht geltende Sieben-Tages-Frist kann der Praxis weiterhin als Orientierung dienen.

Zu Absatz 1:

Die nach bisheriger Rechtslage geltende Beschränkung auf eine Wahrnehmung des Hausrechts soll aufgegeben werden, die zulässigen Zwecke einer Videoüberwachung werden durch die Erstreckung auf Fälle der Aufgabenwahrnehmung erweitert. Absatz 1 Satz 1 regelt die Beobachtung öffentlich zugänglicher Räume. Zu verstehen sind darunter Bereiche – innerhalb oder außerhalb von Gebäuden –, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und ihrem Zweck nach auch dazu bestimmt sind. Die Zweckbestimmung kann sich dabei aus einer Widmung für den öffentlichen Verkehr oder aus einem sonstigen erkennbaren Willen des Berechtigten ergeben.

Nummer 1 umfasst grundsätzlich jedes Tätigwerden einer öffentlichen Stelle zur Erfüllung von Aufgaben innerhalb ihres Zuständigkeitsbereiches. Diese Spezifizierung für die Datenverarbeitung durch Videoüberwachung wird durch Artikel 6 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 erlaubt.

Im Rahmen der einzelnen Zulässigkeitstatbestände bezeichnet die „Aufgabenerfüllung einer öffentlichen Stelle“ alle solche Aufgaben, die sich innerhalb der Zuständigkeit der jeweiligen verantwortlichen Stelle befinden. Die Aufgabe muss dabei nicht unmittelbar durch den Einsatz der Videotechnik erfüllt werden, es genügt, wenn die Videoüberwachung die Aufgabenerfüllung unterstützt. Dabei kann es sich z.B. in Museen um den Schutz von Kulturgütern und Sammlungen handeln.

Der Begriff des Hausrechts (Absatz 1 Satz 1 Nummer 2) ist in einem umfassenden Sinne zu verstehen und beinhaltet die Befugnis, darüber zu entscheiden, wer ein befriedetes Besitztum oder Gebäude betreten und darin verweilen darf. Das Hausrecht umfasst auch die Berechtigung einer Kontrolle der Zugangserlaubnis, sodass von einer gesonderten Normierung dieses Zulässigkeitstatbestandes abgesehen wird. Da die Hausrechtswahrnehmung öffentlicher Stellung der Aufrechterhaltung eines ordnungsgemäßen Dienstbetriebes dient, ist die Spezifizierung ebenfalls durch Artikel 6 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 gerechtfertigt.

Der Begriff der „Beobachtung“ bezeichnet die Sichtbarmachung von Geschehnissen und Personen mit Hilfe dazu geeigneter technischer Einrichtungen. Neben der optischen Erfassung setzt „beobachten“ eine gewisse Dauer voraus. Daraus folgt, dass weder eine (bei entsprechender Ausstattung technisch mögliche) zusätzliche akustische Überwachung, noch eine einmalige Bilderfassung vom Regelungsbereich umfasst sind.

Die Videoüberwachung ist einzustellen, sobald die gesetzlichen Voraussetzungen nicht mehr erfüllt sind. Der Verantwortliche sollte aus eigenem Interesse (Artikel 5 Absatz 2 der Verordnung (EU) 2016/679) die Erforderlichkeit in regelmäßigen Abständen, mindestens jedoch wie nach bisheriger Rechtslage alle zwei Jahre überprüfen.

Zu Absatz 2:

Unterfälle der Videoüberwachung sind die bloße Beobachtung sowie die Aufzeichnung. Die Videoaufzeichnung bezeichnet die über die bloße Beobachtung hinausgehende Speicherung der Überwachungsbilder und greift stärker in die informationelle Selbstbestimmung der betroffenen Person ein. Videoüberwachung und Videoaufzeichnung zeichnen sich damit durch unterschiedliche Eingriffsniveaus aus. Bei der vorzunehmenden Angemessenheitsprüfung ist dieses Stufenverhältnis zu berücksichtigen, das heißt eine Speicherung kann nur dann gerechtfertigt sein, wenn das angestrebte Ziel nicht mit einer bloßen (flüchtigen) Überwachung als milderes Mittel erreicht werden kann. Die Bewertung der Erforderlichkeit muss objektiv im Rahmen einer Einzelfallprüfung erfolgen.

Zu Absatz 3:

Über Videoüberwachung – ist zum frühestmöglichen Zeitpunkt durch geeignete Maßnahmen zu informieren (Hinweisschilder). Insoweit sind die weitreichenden Informationspflichten zu beachten, die den Verantwortlichen nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 treffen.

Zu Artikel 1 § 10 (Verarbeitung von Beschäftigtendaten)

Die Vorschrift erfüllt den Regelungsauftrag in Artikel 88 der Verordnung (EU) 2016/679. Sie entspricht im Wesentlichen dem bisherigen § 28 HmbDSG a.F. Die Terminologie wurde der der Datenschutz-Grundverordnung angepasst.

Zu Artikel 1 § 11 (Datenverarbeitung zum Zwecke wissenschaftlicher und historischer Forschung sowie Statistik)

Die Vorschrift baut auf § 27 HmbDSG a.F. auf und enthält Elemente des § 40 BDSG a.F. sowie des § 27 BDSG in der ab dem 25. Mai 2018 gültigen Fassung. Sie regelt spezifische Anforderungen und Befugnisse bei der Verarbeitung personenbezogener Daten für Forschungs- und Statistikzwecke und macht von der Ermächtigung aus Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) 2016/679 Gebrauch. § 11 erfüllt gleichzeitig den Regelungsauftrag aus Artikel 6 Absatz 2 und 3 in Verbindung mit Artikel 89 der Verordnung (EU) 2016/679. Die Neuregelung dient in Einklang mit der Zielsetzung der Verordnung (EU) 2016/679 der Privilegierung wissenschaftlicher Forschung bei der Datenverarbeitung und somit einer wissenschaftsfreundlichen Gestaltung des Datenschutzrechts. Mit dieser Zielrichtung ermöglicht § 11 eine Verarbeitung und Weiterleitung personenbezogener Daten zu wissenschaftlichen Forschungs- und Statistikzwecken, sofern dabei angemessene Bedingungen und Garantien zum Schutz der Betroffenenrechte eingehalten werden. Die ebenfalls von Artikel 89 der Verordnung (EU) 2016/679 umfasste Datenverarbeitung für Archivzwecke wird in bereichsspezifischen Datenschutzgesetzen (Archivgesetz) geregelt und daher nicht in § 11 aufgenommen. Für Statistikzwecke sieht § 11 dieses Gesetzes keine gesonderte Erhebungsgrundlage vor. Hierfür gelten die Vorschriften über das Recht der Statistik, insbesondere das Hamburgische Statistikgesetz vom 19. März 1991 (HmbGVBl. S. 79, 474). Vor diesem Hintergrund gelten lediglich die Absätze 2 bis 5 für die Datenverarbeitung für statistische Zwecke.

Zu Absatz 1:

Absatz 1 normiert entsprechend der bisherigen Regelung in § 27 Absatz 1 HmbDSG a.F. die Voraussetzungen, unter denen eine Verarbeitung personenbezogener Daten zulässig ist. Der Absatz definiert entsprechend der Vorgaben der Verordnung den zulässigen Zweck und bringt damit die Regelung in Einklang mit EU-Recht. Erforderlich ist weiterhin, dass die Daten für bereits bestimmte Vorhaben, d.h. konkrete Forschungsprojekte, deren Umfang und Auswirkungen bereits klar konturiert sind, verarbeitet werden. Eine „Vorratssammlung“ ist grundsätzlich unzulässig, es sei denn, sie dient einem im vorgenannten Sinn konkreten Forschungsprojekt. Satz 1 normiert die Zulässigkeit einer Datenverarbeitung in Konstellationen, in denen schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden. Im Fall einer Beeinträchtigung schutzwürdiger Interessen ermöglicht Satz 2 eine Abwägung mit dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens. Anders als in der vormaligen Fassung des § 27 HmbDSG kann ein „unverhältnismäßiger Aufwand“ bei der Durchführung des Forschungsvorhabens nicht mehr per se die Verarbeitung personenbezogener Daten ohne Einwilligung rechtfertigen, da dies nicht im Einklang mit den Anforderungen der Verordnung (EU) 2016/679 steht. Die nun verwendete Terminologie orientiert sich an den Kriterien der Verordnung (EU) 2016/679 und verhindert eine Verdrängung des Schutzes personenbezogener Daten bei der Ausgestaltung wissenschaftlicher Privilegien. Erforderlich ist nunmehr, dass der Zweck der Forschung nicht erreicht werden kann oder erheblich beeinträchtigt würde (wenn der Aufwand ohne die in Frage stehende Datenverarbeitung so hoch würde, dass es das Forschungsvorhaben faktisch unmöglich werden ließe, würde dies von der Alternative der „ernsthaften Beeinträchtigung“ abgedeckt). Die personenbezogenen Daten unterliegen nach wie vor (vgl. § 27 Absatz 4 HmbDSG a.F.) einer strengen Zweckbindung. Eine zweckändernde Verarbeitung ist daher gemäß Satz 3 nur mit Einwilligung des Betroffenen möglich.

Zu Absatz 2:

Absatz 2 normiert die Vorschriften zum Schutz der Rechte der betroffenen Personen und setzt die Forderung des Artikels 89 der Verordnung (EU) 2016/679 nach geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen um. Der Absatz fordert eine vorrangige Anonymisierung der Daten, die durch eine Pseudonymisierung ersetzt werden kann, falls anderenfalls der Forschungs- oder Statistikzweck beeinträchtigt würde. Abgebildet wird so das in Artikel 89 der Verordnung (EU) 2016/679 zum Ausdruck gebrachte Stufenverhältnis zwischen Anonymisierung und Pseudonymisierung, mit dem insbesondere der Grundsatz der Datenminimierung gewährleistet wird. Satz 1 enthält eine Legaldefinition für den in der Verordnung nicht näher erläuterten Begriff der Anonymisierung. Der Begriff der Pseudonymisierung wird bereits in Artikel 4 Nummer 5 der Verordnung (EU) 2016/679) definiert. Über den Verweis auf § 22 Absatz 2 BDSG trägt Absatz 2 zudem den Anforderungen des Artikels 9 Absatz 2 Buchstabe j der Verordnung (EU) 2016/679 Rechnung, der fordert, dass eine Forschungsklausel angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

Zu Absatz 3:

Absatz 3 spezifiziert die Anforderungen an dem Umgang mit personenbezogenen Daten im Hinblick auf deren Veröffentlichung. Wie bisher soll zum Schutz der Rechte der betroffenen Personen eine personenbezogene Darstellung von Forschungs- oder Statistikergebnissen nur im besonderen Ausnahmefall (Darstellung von Ereignissen der Zeitgeschichte) zulässig sein und dies auch nur nach einer strengen Abwägung (für die Darstellung „unerlässlich"). In allen anderen Fällen ist eine Veröffentlichung nur mit Einwilligung der betroffenen Personen zulässig.

Zu Absatz 4:

Durch Absatz 4 wird sichergestellt, dass die in den vorherigen Absätzen normierten Garantien zum Schutz der Rechte der betroffenen Personen auch dann Anwendung finden, wenn der Datenempfänger selbst nicht den Vorschriften des HmbDSG unterliegt.

Zu Absatz 5:

Mit Absatz 5 wird von der durch Artikel 89 der Verordnung (EU) 2016/679 eingeräumten Option Gebrauch gemacht, die Betroffenenrechte einzuschränken.

Zu Artikel 1 § 12 (Datenverarbeitung zu künstlerischen Zwecken)

Gemäß der in Artikel 85 der Verordnung (EU) 2016/679 enthaltenen Öffnungsklausel fällt es in die Zuständigkeit der Mitgliedstaaten, das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung einschließlich der Verarbeitung zu journalistischen, künstlerischen und literarischen Zwecken in Einklang zu bringen. § 12 dient der partiellen Wahrnehmung dieses Regelungsauftrags.

Die Vorschrift verlangt Geltung nicht nur für den öffentlichen Bereich, sondern auch für nicht-öffentliche Stellen. Die Einordnung in das Hamburgische Datenschutzgesetz trägt dem Umstand Rechnung, dass nur so Meinungsäußerungen in Form von Kunstwerken erfasst werden können, die hinsichtlich ihrer Behandlung keinem der besonderen Fachgesetze und -verträge, wie z.B. dem NDR-Staatsvertrag, dem Medienstaatsvertrag oder dem Hamburgischen Pressegesetz, zuzuordnen sind.

Artikel 85 der Verordnung (EU) 2016/679 erlaubt Abweichungen und Ausnahmen vom Regelungsprogramm der Datenschutz-Grundverordnung. Der dem nationalen Gesetzgeber zukommende Spielraum ist dabei als weit einzustufen. Angesichts der hohen Bedeutung, die dem Recht auf freie Meinungsäußerung und Kunst in der Rechtsordnung und Gesellschaft zukommt, erscheint es angezeigt, diesen unionsrechtlich gewährten Spielraum im Sinne des Schutzes der Grundrechte in weitreichendem Umfang zu nutzen, ohne dabei datenschutzrelevante Aspekte außer Acht zu lassen.

Zu Absatz 1:

Die Vorschrift konzentriert sich angesichts der spezialgesetzlichen Regelungen zum Ausgleich der Meinungsfreiheit mit dem Datenschutz auf den Bereich der Datenverarbeitung zur Ausübung der Kunstfreiheit. Sie enthält im Kontext der unionsrechtlichen Vorgaben für diesen Bereich im Wesentlichen dem bereits zuvor bestehende Medienprivileg (vgl. § 41 BDSG a.F.) entsprechende Regelungen. Zwecks Gewährleistung dieses Privilegs bedarf es des Ausschlusses einer Vielzahl von Bestimmungen der Verordnung (EU) 2016/679, da sich deren Vorgaben häufig nicht mit Datenverarbeitungen zu künstlerischen Zwecken vereinbaren lassen. Daher werden aus den in Artikel 85 Absatz 2 der Verordnung (EU) 2016/679 genannten Kapiteln II bis VII und IX lediglich Artikel 5 Absatz 1 Buchstabe b und f sowie die Artikel 24, 32, 33 der Verordnung (EU) 2016/679 für anwendbar erklärt. Gegenüber dem bisherigen Recht ist der Datenschutz insoweit verstärkt, als der Grundsatz der Zweckbindung auch bei Verarbeitungsvorgängen für künstlerische Zwecke vorgesehen wird.

Eine Abweichungsbefugnis hinsichtlich Kapitel VIII der Datenschutz-Grundverordnung für den Bereich journalistischer, künstlerischer oder literarischer Zwecke sieht Artikel 85 Absatz 2 Verordnung (EU) 2016/679 nicht vor; die Vorschriften des Kapitels VIII stehen damit nicht zur Disposition der mitgliedstaatlichen Gesetzgeber. Daraus ergibt sich, dass weder die Sanktionsregelungen der Datenschutz-Grundverordnung, insbesondere die in Artikel 82 Verordnung (EU) 2016/679 enthaltene Schadensersatzregelung, noch die Rechte auf einen wirksamen Rechtsbehelf in Landesgesetzen modifiziert werden dürfen. Dies beruht nicht unwesentlich auf dem in der Verordnung (EU) 2016/679 u.a. angelegten Ziel, Verstöße gegen ihre Bestimmungen wirksam, verhältnismäßig und abschreckend zu sanktionieren (vgl. Artikel 84 Absatz 1 der Verordnung (EU) 2016/679 a.E.). Bei unmittelbarer Anwendung z.B. des Artikels 82 der Verordnung (EU) 2016/679 durch die Gerichte darf aber nicht übersehen werden, dass die Vorschrift gerade im Anwendungsbereich der Meinungs- und Kunstfreiheit primärrechtlich überformt ist (vgl. Artikel 11, 13 Grundrechte-Charta). Der Umstand, dass sich die sekundärrechtliche Bestimmung des Artikels 82 Verordnung (EU) 2016/679 an Artikel 11, 13 Grundrechte-Charta bzw. den Grundsätzen des EU-Rechts (vgl. Artikel 6 EUV) messen lassen muss, ist jedoch im Wege einer primärrechtskonformen Auslegung bei Anwendung des Artikels 82 der Verordnung (EU) 2016/679 zu gewinnen und nicht durch eine diese vorwegnehmende „interpretatorische Gesetzgebung“ auf nationaler Ebene. Abweichendes ergibt sich auch nicht aus Artikel 85 Absatz 1 der Verordnung (EU) 2016/679.

Zu Absatz 2:

Das Recht auf freie Meinungsäußerung sowie die Kunstfreiheit würden zu weitgehenden Einschränkungen unterworfen, falls Berichtigungs- und Löschungsansprüche betroffener Personen uneingeschränkt durchgesetzt werden könnten. Nach der Verordnung (EU) 2016/679 dürfte etwa eine uneingeschränkte Pflicht zur Berichtigung oder Löschung bereits veröffentlichter oder zur Veröffentlichung vorgesehener Werke kaum zu rechtfertigen sein. Aus dem Grundrecht auf Datenschutz (Artikel 8 Grundrechte-Charta) wie auch aus dem Recht auf informationelle Selbstbestimmung (Artikel 2 Absatz 1 Grundgesetz in Verbindung mit Artikel 1 Absatz 1 Grundgesetz) folgt jedoch ein Anspruch auf Verwendung vollständiger und zutreffender personenbezogener Daten. Die gegenläufigen Interessen werden im Wege einer Verpflichtung zur gemeinsamen Aufbewahrung und gegebenenfalls Übermittlung miteinander in Ausgleich gebracht.

Zu Absatz 3:

Zwecks Schaffung einer Norm, die – von Spezialregelungen abgesehen – den Bereich des Rechts auf freie Ausübung von Kunst sowie den auf freie Meinungsäußerung erfasst und auf diese Weise den Regelungsauftrag aus Artikel 85 der Verordnung (EU) 2016/679 erfüllt, wird ihr Geltungsbereich über öffentliche Stellen im Sinne von § 2 Absatz 1 dieses Gesetzes hinaus auf nicht-öffentliche Stellen erstreckt.

Zu Artikel 1 § 13 (Öffentliche Auszeichnungen und Ehrungen)

Öffentliche Auszeichnungen und Ehrungen unterfallen gemäß Artikel 2 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 nicht dem Anwendungsbereich des Unionsrechts. Zwecks einheitlicher Anwendung des Datenschutzrechts in Bezug auf solche Verarbeitungssituationen, die nicht in den Anwendungsbereich der Datenschutz-Grundverordnung fallen, erstreckt § 2 Absatz 6 die Geltung der Verordnung (EU) 2016/679 auch auf diese. Eine Ausprägung hiervon regelt § 13 dieses Gesetzes. Die Vorschrift bestimmt die Voraussetzungen für die Zulässigkeit der Verarbeitung personenbezogener Daten zur Vorbereitung öffentlicher Auszeichnungen und Ehrungen.

Zu Absatz 1:

In Absatz 1 wird die Erlaubnis zur Datenverarbeitung der eine öffentliche Auszeichnung oder Ehrung vorbereitenden Stelle festgelegt. Die Befugnis ist durch das Tatbestandsmerkmal der Erforderlichkeit begrenzt. Zur Vorbereitung der Entscheidung erforderlich sind sämtliche Daten, die zur Beurteilung der Würdigkeit der betroffenen Person benötigt werden. Welche Daten dies im Einzelfall sind, kann nicht abstrakt im Vorhinein bestimmt werden. Erfasst sein dürften indes solche Daten, die eine Würdigung in Bezug auf die Aspekte des der Auszeichnung zugrundliegenden Sachzusammenhangs ermöglichen. Zum anderen kann die persönliche Integrität der auszuzeichnenden Person von Bedeutung für den Umfang benötigter Daten sein.

Absatz 1 Satz 2 enthält – korrespondierend zur Erhebungs- und Verarbeitungsbefugnis gemäß Absatz 1 Satz 1 – eine Erlaubnisnorm für andere Stellen als die die Entscheidung vorbereitenden Stelle, Informationen zum Zwecke der Entscheidungsvorbereitung an die die öffentliche Auszeichnung oder Ehrung vorbereitende Stelle zu übermitteln. Übermittlungen nach Absatz 1 Satz 2 sind jedoch davon abhängig, dass Informationen von der über die öffentliche Auszeichnung oder Ehrung entscheidenden Stelle angefordert werden. Ausgeschlossen ist damit eine anlasslose Datenübermittlung.

Zu Absatz 2:

Absatz 2 bestätigt zum Schutz der Rechte betroffener Personen die Geltung einer strengen Zweckbindung. In Ergänzung zur allgemeinen Bestimmung in § 6 Absatz 2 dieses Gesetzes regelt Absatz 2 eine (weitere) zulässige Zweckänderung. Für die Einwilligung gelten die Artikel 7 und 8 der Verordnung (EU) 2016/679.

Zu Absatz 3:

Absatz 3 dient der Klarstellung, dass die in den Absätzen 1 und 2 geregelten Erlaubnisse zur Datenverarbeitung in solchen Fällen nicht bestehen, in denen der zuständigen Stelle bekannt ist, dass die für eine öffentliche Auszeichnung oder Ehrung vorgesehene Person einer solchen widersprochen hat. Es kommt nicht darauf an, ob ein solcher Widerspruch bereits im Vorfeld eines Ehrungs- oder Auszeichnungsverfahrens artikuliert worden ist oder erst während des Verfahrens.

Zu Absatz 4:

Eine Information der betroffenen Person durch die übermittelnde Stelle darf gemäß Absatz 4 unterbleiben, da sie zum einen angesichts des Verarbeitungszwecks häufig untunlich sein dürfte und die Datenübermittlung zum anderen auf der Grundlage einer Rechtsvorschrift im Sinne von Artikel 14 Absatz 5 Buchstabe c der Verordnung (EU) 2016/679 erfolgt. In den letztgenannten Fällen findet Artikel 14 der Verordnung (EU) 2016/679 keine Anwendung. Absatz 4 regelt darüber hinaus, dass eine Auskunftspflicht des Verantwortlichen im Zusammenhang mit einer öffentlichen Auszeichnung oder Ehrung gegenüber der betroffenen Person nicht besteht. Vielmehr wird die Entscheidung über die Auskunftserteilung in das pflichtgemäß auszuübende Ermessen des Verantwortlichen gestellt. Eine Auskunftserteilung dürfte insbesondere dann in Betracht kommen, wenn die Entscheidung über die öffentliche Auszeichnung oder Ehrung bereits getroffen wurde.

Zu Artikel 1 § 14 (Begnadigungsverfahren)

Die Durchführung von Begnadigungsverfahren fällt nicht in den Anwendungsbereich des Unionsrechts und damit auch nicht in den der Verordnung (EU) 2016/679, wie aus deren Artikel 2 Absatz 2 Buchstabe a ersichtlich wird. Gemäß § 2 Absatz 6 sollen einzelne nicht in den Anwendungsbereich des Unionsrechts fallende Bereiche dennoch generell der Verordnung (EU) 2016/679 unterstellt und eventuelle Besonderheiten in diesem Gesetz (Vierter Abschnitt) geregelt werden. Hierzu gehören auch Verfahren betreffend Begnadigungsersuchen, über die von der zuständigen Behörde – Justizbehörde – entschieden wird.

Satz 1 erlaubt die Verarbeitung personenbezogener Daten in Gnadensachen und stellt damit die hierfür notwendige Erlaubnisnorm dar. Die gesetzliche Erlaubnis umfasst die Verarbeitung besonders sensitiver Daten im Sinne von Artikel 9 Absatz 1 und Artikel 10 der Verordnung (EU) 2016/679. Die Datenverarbeitung ist indes daran geknüpft, dass sie für die Bearbeitung von Gnadengesuchen erforderlich sein muss.

Satz 2 benennt – als gegenüber § 2 Absatz 6 speziellere Norm und diese Bestimmung einschränkend – die Normen der Verordnung (EU) 2016/679, die in Begnadigungsverfahren zur Anwendung kommen sollen. Dies betrifft die Grundsätze der Verarbeitung personenbezogener Daten sowie den Bereich des technischen und organisatorischen Datenschutzes.

Zu Artikel 1 § 15 (Beschränkung der Informationspflicht)

In Artikel 13 und 14 der Verordnung (EU) 2016/679 werden den Verantwortlichen (Artikel 4 Nummer 7 der Verordnung (EU) 2016/679) weitgehende Informationspflichten auferlegt, die bei Erhebung personenbezogener Daten bei den betroffenen Personen selbst oder bei Dritten entstehen. Diese Informationspflichten gehen deutlich über die bisher nach BDSG oder HmbDSG bestehenden hinaus. Mittels dieser Informationen sollen zum einen ein größtmögliches Maß an Transparenz hergestellt und zum anderen die betroffenen Personen in die Lage versetzt werden, ihre Rechte umfassend wahrzunehmen. Unabhängig von den bereits unionsrechtlich nach Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 vorgesehenen Ausnahmen erlaubt es Artikel 23 der Verordnung (EU) 2016/679, diese Informationspflichten nach Maßgabe des mitgliedstaatlichen Rechts einzuschränken, sofern dabei die engen unionsrechtlichen Vorgaben zur Beschränkung des Rechts auf Auskunftserteilung beachtet und eingehalten werden.

Zu Absatz 1:

Die Beschränkungen in § 15 Absatz 1 Nummer 1 stützen sich auf Artikel 23 Absatz 1 Buchstabe a bis c und e der Verordnung (EU) 2016/679.

§ 15 Absatz 1 Nummer 2 stützt sich auf Artikel 23 Absatz 1 Buchstabe e und i der Verordnung (EU) 2016/679.

Die in § 15 Absatz 1 Nummer 3 vorgesehene Beschränkung findet ihre unionsrechtliche Grundlage in

Artikel 23 Absatz 1 Buchstabe d und e der Verordnung (EU) 2016/679.

§ 15 Absatz 1 Nummer 4 entspricht § 32 Absatz 1 Nummer 4 BDSG und stützt sich auf Artikel 23 Absatz 1 Buchstabe j der Verordnung (EU) 2016/679.

§ 15 Absatz 1 Nummer 5 entspricht § 32 Absatz 1 Nummer 1 BDSG. Geregelt wird eine Abweichung von Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 (vgl. Erwägungsgrund 62).

Zu Absatz 2:

Absatz 2 greift die besonders gelagerte Fallkonstellation einer Datenübermittlung an die dort genannten Behörden und Einrichtungen auf, welche eine Informationspflicht nach Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 auslösen würde. Die Beschränkung dient dem wichtigen öffentlichen Ziel der Gewährleistung der öffentlichen und nationalen Sicherheit. Insbesondere soll eine von einer Datenübermittlung betroffene Person grundsätzlich nicht im Wege einer Informationserteilung nach Artikel 13 oder 14 der Verordnung (EU) 2016/679 Informationen erhalten, die ihr die in Absatz 2 genannten Behörden bzw. Einrichtungen nicht von sich aus erteilen würden. Die Verantwortung für die Übermittlung der Daten liegt nach den unionsrechtlichen Vorgaben jedoch weiterhin bei der übermittelnden Behörde. Auf Grundlage von Artikel 23 Absatz 1 Buchstabe a bis d der Verordnung (EU) 2016/679 erfolgt daher eine Einschränkung des Rechts auf Informationserteilung lediglich insoweit, als mit den betroffenen Behörden ein Einvernehmen herzustellen ist, um der übermittelnden Behörde eine bessere Entscheidungsgrundlage zu geben, ob die Informationen herausgegeben werden können oder ob ein Fall von Absatz 1 Nummer 1 bis 4 vorliegt. Das in diesem Gesetz gewählte Einvernehmens-Modell ist gegenüber einem Zustimmungs-Modell vorzugswürdig, da es der durch Artikel 5 Absatz 2 der Verordnung (EU) 2016/679 und letztlich auch § 8 Absatz 1 dieses Gesetzes geregelten Verantwortlichkeit für eine Informationserteilung Rechnung trägt. Eines Einvernehmens bedarf es lediglich dann, falls der Verantwortliche die Informationserteilung nicht bereits nach eigener Prüfung ablehnt.

Zu Absatz 3:

Die Norm enthält für den Fall einer nach Absatz 1 Nummern 1 bis 3 und 5 oder Absatz 2 nicht erteilten Auskunft eine Dokumentationspflicht. Eine Dokumentationspflicht besteht nicht in den Fällen des Absatzes 1 Nummer 4, da dies zu einer zu einer Vereitelung oder wenigstens ernsthaften Beeinträchtigung des Verarbeitungszwecks führen könnte (vgl. BundestagsDrucksache 18/11325 S. 103).

Zu Artikel 1 § 16 (Beschränkung des Auskunftsrechts)

Artikel 15 der Verordnung (EU) 2016/679 regelt den Auskunftsanspruch betroffener Personen umfassend und mit unmittelbarer Wirkung für die Mitgliedstaaten. Die bisherige Regelung in § 18 HmbDSG kann daher nicht aufrechterhalten werden. An ihre Stelle treten die unionsrechtlichen Vorgaben. Diese dürfen zwar im mitgliedstaatlichen Recht Einschränkungen erfahren. Dabei sind jedoch die Maßgaben von Artikel 23 der Verordnung (EU) 2016/679 zu beachten. Mit § 16 wird von dieser Beschränkungsoption Gebrauch gemacht.

Zu Absatz 1:

Absatz 1 zählt die Gründe auf, aus denen Auskunftsersuchen nach Artikel 15 der Verordnung (EU) 2016/679 abgelehnt werden können.

Die Beschränkung der Auskunftserteilung gemäß § 16 Absatz 1 Nummer 1 fußt auf Artikel 23 Absatz 1 Buchstaben a bis c und e der Verordnung (EU) 2016/679.

§ 16 Absatz 1 Nummer 2 findet seine unionsrechtliche Grundlage in Artikel 23 Absatz 1 Buchstaben c und i der Verordnung (EU) 2016/679.

§ 16 Absatz 1 Nummer 3 fußt auf Artikel 23 Absatz 1 Buchstabe d DSGVO.

Es besteht nach dem Wortlaut der Bestimmung keine Verpflichtung des Verantwortlichen, Anträge auf Erteilung von Auskünften abzulehnen, wenn einer der in Absatz 1 aufgezählten Gründe vorliegt. Die Vorschrift räumt dem Verantwortlichen vielmehr ein pflichtgemäß auszuübendes Ermessen sowohl hinsichtlich des „Ob“ einer Auskunftserteilung als auch deren „Wie“ ein.

Weitere Ablehnungsgründe betreffend Auskunftsersuchen ergeben sich aus § 11 Absatz 5 hinsichtlich wissenschaftlicher oder historischer Forschungsvorhaben sowie für Statistiken, und weiter nach § 13 Absatz 4 Satz 2 dieses Gesetzes mit Blick auf öffentliche Auszeichnungen und Ehrungen.

Zu Absatz 2:

Mit Absatz 2 Satz 1 wird gewährleistet, dass durch die Erteilung einer Begründung für die Ablehnung eines Antrags auf Auskunft nicht die der Ablehnung zugrunde liegenden Zwecke oder Ziele offenbart werden müssen. Gefährdet die Erteilung einer Begründung diese Ziele, muss sie in dem Umfang unterbleiben, soweit eine solche Gefährdung besteht. Der Verantwortliche hat zu prüfen, in welchem Umfang und in welchem Zeitraum eine Gefährdung im Sinne der in Satz 1 geregelten Tatbestände besteht.

Zum Schutz der Rechte der betroffenen Person regelt Absatz 2 für den Fall einer nicht erteilten Auskunft, dass diese auf das Verlangen der betroffenen Person der Aufsichtsbehörde zu erteilen ist, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Auf die Möglichkeit, sich an den Hamburgischen Beauftragten bzw. die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zu wenden, ist seitens des Verantwortlichen hinzuweisen. Als Maßnahme im Sinne von Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 ist gewährleistet, dass die Rechte der betroffenen Person angemessen gewahrt bleiben. Die gegenüber der Aufsichtsbehörde mögliche Beschränkung der Information verfolgt die nach Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 genannten Zwecke und Ziele. In der Praxis dürfte es sich indes um selten auftretende Einzelfälle handeln, weil gegenüber der Aufsichtsbehörde lediglich in besonders gelagerten Situationen Sicherheitsbedenken geltend gemacht werden können. Die Gründe der Ablehnung müssen aktenkundig gemacht werden.

Zu Absatz 3:

Falls personenbezogene Daten an die in Absatz 3 genannten Behörden in den genannten Tätigkeitsbereichen übermittelt wurden, ist mit den betroffenen Behörden und Stellen vor Erteilung der Auskunft gemäß Absatz 3 Satz 1 Einvernehmen herzustellen. Satz 2 regelt den umgekehrten Fall einer Auskunft über eine Übermittlung von diesen Behörden. Dies geschieht vor dem Hintergrund, dass betroffene Personen grundsätzlich nicht im Wege von Anträgen auf Auskunftserteilung bei anderen als den in Absatz 3 genannten Informationen erhalten, die ihr insbesondere die Sicherheitsbehörden oder Nachrichtendienste nicht direkt mitteilen dürften oder könnten. Allerdings verbleibt die Verantwortlichkeit für die Übermittlung der Daten an die auskunftsbegehrende Person bei der übermittelnden Behörde. An dieser unionsrechtlichen Vorgabe sollen keine Änderungen vorgenommen werden. Die hier gewählte Beschränkung des Auskunftsrechts stützt sich auf Artikel 23 Absatz 1 Buchstaben a bis e der Verordnung (EU) 2016/679.

Zu Artikel 1 § 17 (Beschränkung der Löschungspflicht)

Unter den in Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 genannten Voraussetzungen hat der Verantwortliche personenbezogene Daten zu löschen. Diese Vorschrift ist nicht lediglich als Betroffenenrecht ausgestaltet, sondern enthält auch eine objektivrechtliche Pflicht der Verwaltung, Daten unverzüglich zu löschen. Diese Pflicht kann grundsätzlich nur aus den explizit in Artikel 23 der Verordnung (EU) 2016/679 aufgeführten Gründen eingeschränkt werden. § 17 dieses Gesetzes dient der Umsetzung einer solchen Einschränkung.

Zwecks Wahrung schutzwürdiger Interessen einer betroffenen Person im Sinne von Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679 sieht § 17 eine Eingrenzung der Löschungspflichten vor. Sie dient der Ergänzung der Regelung des Artikel 18 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 in Konstellationen, in denen der Verantwortliche Daten der betroffenen Person gemäß Artikel 17 Absatz 1 Buchstabe a und d der Verordnung (EU) 2016/679 löschen müsste, aber schutzwürdige Interessen der betroffenen Person am Erhalt der Daten bestehen. Diesfalls soll statt einer Löschung generell und von Amts wegen lediglich eine Einschränkung der Verarbeitung erfolgen, ohne dass es eines vorhergehenden Antrags der betroffenen Person bedürfte. Erforderlich ist aber, dass der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden.

Da die Einschränkung der Verarbeitung (statt einer nach Artikel 17 der Verordnung (EU) 2016/679 gebotenen Löschung) den tatsächlichen Interessen der betroffenen Person zuwiderlaufen und sie sich auch für eine Löschung entscheiden kann, ist sie über die erfolgte Einschränkung der Verarbeitung im Sinne des Artikels 18 der Verordnung (EU) 2016/679 zu informieren. Dies stellt zugleich eine Maßnahme im Sinne von Artikel 23 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 dar. Regelhaft wird lediglich eine vorübergehende Beschränkung der Löschungspflicht vorliegen (vgl. Artikel 23 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679.

Zu Artikel 1 § 18 (Beschränkung der Benachrichtigungspflicht)

Hat eine Verletzung des Schutzes personenbezogener Daten – legaldefiniert in Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 – voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so besteht nach Artikel 34 der Verordnung (EU) 2016/679 eine Pflicht des Verantwortlichen, die betroffene Person unverzüglich von der Verletzung zu benachrichtigen. Dieses Recht der betroffenen Person bzw. die damit korrespondierende Pflicht des Verantwortlichen darf lediglich unter den engen Voraussetzungen von Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 beschränkt werden.

Zu Absatz 1:

Die Beschränkung der Benachrichtigungspflicht in § 18 Absatz 1 Nummer 1 beruht auf Artikel 23 Absatz 1 Buchstabe a bis c und e der Verordnung (EU) 2016/679, denn die Verhinderung von Gefährdungen für die nationale und öffentliche Sicherheit sowie die Landesverteidigung sind dort ausdrücklich aufgeführte Belange. Zugleich stellen sich diese Belange als wichtige Ziele des allgemeinen öffentlichen Interesses dar.

Auf Grundlage des Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 schränkt § 18 Absatz 1 Nummer 2 die Löschungspflicht in unionsrechtskonformer Art und Weise ein.

§ 18 Absatz 1 Nummer 3 findet seine Rechtsgrundlage in den Öffnungsklauseln in Artikel 23 Absatz 1 Buchstabe e und i der Verordnung (EU) 2016/679.

Die Erhaltung der Funktionsfähigkeit von Datenverarbeitungssystemen einer öffentlichen Stelle gehört zu den wichtigen Zielen des allgemeinen öffentlichen Interesses im Sinne von Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 und rechtfertigt daher die Beschränkung der Benachrichtigungspflicht in § 18 Absatz 1 Nummer 4. Unter Datenverarbeitungssystemen sind dabei sowohl Hardwarekomponenten als auch Software in jeglicher Hinsicht zu verstehen. Diese Vorschrift soll vor allem verhindern, dass Sicherheitslücken offenbart werden müssen, bevor sie geschlossen werden.

Gefährdet die Benachrichtigung diese Ziele, muss sie unterbleiben, soweit und solange eine solche Gefährdung besteht. Der Verantwortliche hat zu prüfen, in welchen Umfang und in welchem Zeitraum eine entsprechende Gefährdung besteht. Liegt eine Gefährdung nicht mehr vor, hat die entsprechende Benachrichtigung zu erfolgen.

Es besteht nach dem Wortlaut der Bestimmung keine Verpflichtung des Verantwortlichen, von einer Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 abzusehen, wenn einer der in Nummern 1 bis 3 aufgezählten Gründe vorliegt. Die Vorschrift räumt dem Verantwortlichen vielmehr ein pflichtgemäß auszuübendes Ermessen ein. Dieses bezieht sich auf das „Ob" einer Benachrichtigung. Hinsichtlich der Dauer des Vorliegens einer Gefährdung der Ziele besteht kein – gerichtlich nur eingeschränkt überprüfbarer – Beurteilungsspielraum des Verantwortlichen.

Zu Absatz 2:

Zur Sicherstellung des Schutzes der Betroffenenrechte legt § 18 Absatz 2 fest, dass bei einem Absehen von der Benachrichtigung gemäß Absatz 1 die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zu informieren ist.

Zu Artikel 1 § 19 (Zuständigkeit)

Die Vorschrift des § 19 regelt die Zuständigkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

Zu Absatz 1:

Nach Absatz 1 wird dem oder der Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit die Aufgabe der Aufsichtsbehörde für den Datenschutz und Informationsfreiheit gemäß Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 übertragen.

Zu Absätzen 2 bis 4:

Die Absätze 2 bis 4 der Vorschrift sind weitestgehend unverändert aus der bisherigen Fassung des § 23 HmbDSG a.F. entnommen. Die vorgenommenen Kürzungen korrelieren mit entsprechenden Normierungen auf Unionsebene, die einer Wiederholung auf Landesebene entgegenstehen. Dies gilt insbesondere für die in § 23 HmbDSG a.F. normierten Aufgaben, die nun ausführlich in Artikel 57 der Verordnung (EU) 2016/679 ausgeführt sind.

Die darüber hinaus gegebene Zuständigkeit nach § 40 BDSG ergab sich nach bisheriger Rechtslage aus § 24 HmbDSG a.F. In inhaltlich entsprechender Weise ist die Aufsichtsbefugnis über Gerichte bereits durch die Vorgabe des Artikels 55 Absatz 3 der Verordnung (EU) 2016/679 europarechtlich beschränkt worden, sodass eine Regelung im nationalen Recht insoweit ausscheidet.

Gemäß Absatz 4 ist die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit im Rahmen der zugewiesenen Aufgabenbereiche zuständig für die Verfolgung von Ordnungswidrigkeiten. Diese Festsetzung erfolgte bisher in § 23 Absatz 7 HmbDSG a.F. und trat bereits mit der letzten Änderung des HmbDSG durch das „Gesetz zur weiteren Stärkung der Unabhängigkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit" zum 1. Januar 2017 in Kraft. Die Regelung ersetzte die bisherige Anordnung der Zuständigkeit durch den Senat und ergibt sich aus der Sachnähe und besonderen Fachkunde der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, die eine sachgerechte Ausführung der getroffenen Bestimmungen sicherstellt.

Zu Absatz 5:

In die Zuständigkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit fällt gemäß Absatz 5 nunmehr auch die Akkreditierung von Zertifizierungsstellen im Sinne von Artikel 43 der Verordnung (EU) 2016/679. Dass die Aufsichtsbehörden zudem auch selbst Zertifizierungen vornehmen dürfen, ergibt sich bereits unmittelbar aus Artikel 42 Absatz 5 der Verordnung (EU) 2016/679.

Zu Absatz 6:

Nach des §32h Absatz 1 der Abgabenordnung (AO; in der Fassung ab dem 25. Mai 2018) werden die datenschutzrechtlichen Anforderungen durch Aufnahme in der AO vereinheitlicht. Für die Wahrnehmung der datenschutzrechtlichen Aufsichtsbefugnisse soll ab dem 25. Mai 2018 allein der BfDI zuständig sein, soweit es die Aufsicht über die Datenverarbeitung bei der Verwaltung bundesgesetzlich geregelter Steuern betrifft. Grund hierfür ist, dass nach den gesetzlichen Vorgaben weitgehend identische technische Abläufe und eine immer homogener werdende IT-Architektur zu etablieren sind. Daher ist es sinnvoll, auch die datenschutzrechtliche Aufsicht zu zentralisieren und damit auch den Dokumentationsaufwand vor Freigabe des Verfahrens zu reduzieren.

Bezüglich der weiterhin vom Landesdatenschutzbeauftragten zu beaufsichtigenden landesgesetzlich geregelten Steuern (Kirchensteuer, Spielbankabgabe, Spielvergnügungssteuer, Kultur- und Tourismustaxe, Zweitwohnungsteuer, Hundesteuer) besteht das Risiko, dass die dort ebenfalls eingesetzten bundeseinheitlichen Verfahren in datenschutzrechtlicher Hinsicht anders beurteilt werden, als durch den BfDI, unverändert fort. Wenn auch in geringerem Umfang werden für die Verwaltung dieser Steuerarten ebenfalls zahlreiche, in Teilen dieselben Verfahren aus dem bundeseinheitlichen Programmierverbund verwendet. Dies gilt zum Beispiel für die Adressdatenverwaltung (Verfahren GRINFO, bzw. GINSTER), die Buchung und Erhebung der Steuerfestsetzungen und die kassentechnische Abwicklung. Das Ziel, den Aufwand für die datenschutzrechtliche Dokumentation deutlich zu reduzieren, ließe sich nicht erreichen, solange dieser weiterhin für einen Teil der zu verwaltenden Steuern (landes-) gesetzlich vorgeschrieben ist. Es könnte in Bezug auf einzelne KONSENS- Verfahren zu konfligierenden Auflagen kommen, die den Einsatz von IT-Programmen verzögern und gar verhinderten.

Nach Inkrafttreten der Übertragung ist die von §32h Absatz 3 AO vorgesehene Vereinbarung zur Verwaltungskostenerstattung abzuschließen.

Zu Artikel 1 §20 (Ernennungsvoraussetzungen)

Die Vorschrift entspricht der bisherigen Regelung in §21 HmbDSG a.F. und statuiert die persönlichen Voraussetzungen für eine Ernennung zum Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Unter Berücksichtigung der Vorgaben der Verordnung (EU) 2016/679 fordert §20, dass sie/er die Befähigung zum Richteramt oder für die Laufbahn Allgemeine Dienste in der Laufbahngruppe 2 mit Zugang zum zweiten Einstiegsamt haben und die zur Erfüllung ihrer oder seiner Aufgabe erforderliche Fachkunde besitzen muss. Die Laufbahnbefähigung wäre mangels eines besonderen Weisungs- oder Eingriffsrechts gegenüber den zu kontrollierenden Stellen im öffentlichen Bereich zwar nicht unmittelbar gefordert, ist aber nicht zuletzt wegen der verliehenen aufsichtsbehördlichen Kompetenzen (unter anderem Erlass von Verwaltungsakten oder Verhängung von Bußgeldern) gegenüber privaten Stellen bedeutsam. Das vormals geltende Mindestalter von 35 Jahren wurde mit Blick auf das beamtenrechtliche Leistungsprinzip aufgehoben.

Zu Artikel 1 §21 (Rechtsstellung)

§21 greift in weiten Teilen die Regelung des vormaligen §22 HmbDSG a.F. auf und regelt die Rechtsstellung des Beauftragten für Datenschutz und Informationsfreiheit. Zwecks besserer Handhabbarkeit wurde der ehemalige §22 HmbDSG a.F. (Aufgaben) in zwei Paragraphen aufgeteilt, von denen §21 die Rechtsstellung und §22 die Pflichten ausgestaltet. Die Absätze 1 bis 3 entsprechen den bisherigen Regelungen in §22 Absätze 1 bis 3 a.F., §21 Absatz 4 entspricht dem bisherigen §22 Absatz 6 HmbDSG a.F. und Absatz 5 entspricht §22 Absatz 7 HmbDSG a.F. Der Regelungsinhalt des bisherigen §22 Absatz 8 HmbDSG a.F. wird auf Unionsebene in Artikel 52 Absatz 4, Absatz 5 der Verordnung (EU) 2016/679 abschließend geregelt, sodass eine gesonderte Normierung auf Landesebene nicht mehr zulässig ist.

Zu Absatz 1:

Mit Absatz 1 wird ein öffentlich-rechtliches Amtsverhältnis eigener Art geschaffen, das auf der einen Seite in der konkreten Ausgestaltung die Unabhängigkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit sichert und auf der anderen Seite die entsprechende Anwendung erprobter Regelwerke des Beamtenrechts zulässt, wenn dadurch die unions- und verfassungsrechtlich vorgegebene Unabhängigkeit nicht beeinträchtigt wird.

Zu Absatz 2:

Dieser Absatz entspricht ebenfalls der bisherigen Regelung und lehnt sich an die Formvorschriften des Beamtenrechts an. Die Bestimmung dient der Rechtssicherheit. Beginn und Ende des Amtsverhältnisses sollen eindeutig feststellbar sein. Die Leistung eines Amtseides ist für öffentlich-rechtliche Amtsverhältnisse (Beamtinnen/Beamte, Regierungsmitglieder, Bundesbeauftragte für Datenschutz u.a.) üblich und wird auch hier vorgesehen.

Zu Absatz 3:

Absatz 3 regelt wie bisher § 22 Absatz 3 HmbDSG a.F. die Beendigung des Amtsverhältnisses. Die materiellen Beendigungsgründe gibt Artikel 60a Absatz 5 der Verfassung der Freien und Hansestadt Hamburg abschließend und zwingend vor. Auch hier wird aus Gründen der Rechtssicherheit zum Verfahren wieder auf die Urkundenform zurückgegriffen. Neben der Aushändigung wird die Entlassung aber auch mit jeder anderen Zustellungsform wirksam. Ohne dass es eines besonderen Verweises bedarf, gelten ergänzend die allgemeinen Regelungen des Verwaltungsverfahrensrechts.

Zu Absatz 4:

Entsprechend der bisherigen Regelung in § 22 Absatz 6 trifft Absatz 4 eine Vertreterregelung. Die Regelung bezweckt, dass der Schutz des Rechts auf informationelle Selbstbestimmung auch bei der Verhinderung der Amtsinhaberin bzw. des Amtsinhabers durch einen Stellvertreter sichergestellt werden kann.

Zu Absatz 5:

Die Vorschrift regelt die Besoldung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

Zu Absatz 6:

Absatz 6 klärt wie die Parallelregelung in § 10 Absatz 2 BDSG n.F. im Hinblick auf den Regelungsauftrag des Artikel 52 Absatz 6 der Verordnung (EU) 2016/679 das Verhältnis zwischen unabhängiger Datenschutzkontrolle durch die Aufsichtsbehörde und unabhängiger Finanzkontrolle durch den Rechnungshof.

Zu Artikel 1 § 22 (Besondere Pflichten)

Die in § 22 geregelten besonderen Pflichten der oder des Hamburgischen beauftragten für Datenschutz und Informationsfreiheit sollen die Integrität der Amtsausübung absichern.

Zu Absatz 1:

Absatz 1 setzt Artikel 54 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 um und dient der Vermeidung von potentiellen Interessenkonflikten. Die Sätze 1 und 2 enthalten ein umfassendes Verbot sämtlicher nicht mit dem Amt zu vereinbarender Handlungen und Tätigkeiten, gleich ob entgeltlich oder unentgeltlich. Diese allgemeine Regelung wird durch die Verbote einiger mit dem Amt nicht zu vereinbarenden Tätigkeitsbereiche in Satz 4 konkretisiert.

Zu Absatz 2:

Die in Absatz 2 normierte Verschwiegenheitspflicht entspricht der vorherigen Regelung in § 22 Absatz 4 HmbDSG a.F. und setzt Artikel 54 Absatz 2 der Verordnung (EU) 2016/679 um.

Zu Artikel 1 § 23 (Tätigkeit nach Beendigung des Amtsverhältnisses)

§ 23 ist neu eingefügt und dient ebenfalls der Umsetzung des Artikels 54 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679, der einen Regelungsauftrag nicht nur für Bedingungen während, sondern auch für solche nach der Amtszeit enthält. Durch ein Verbot sämtlicher mit dem Amt nicht zu vereinbarenden Tätigkeiten auch für die Dauer von zwei Jahren nach Beendigung des Amtes soll das Risiko von Interessenkonflikten minimiert werden. Die Vorschrift ist § 9a des Senatsgesetzes nachempfunden mit dem Unterschied, dass die Anzeigepflicht (Absatz 2) gegenüber der Präsidentin oder dem Präsidenten der Bürgschaft und nicht gegenüber dem Senat besteht. Entsprechend ist auch die Präsidentin oder der Präsident der Bürgschaft befugt, eine nicht mit dem Amt des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zu vereinbarende Tätigkeit zu untersagen. Gegen diese Untersagungsverfügung steht der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit der Verwaltungsrechtsweg offen.

Zu Artikel 1 § 24 (Befugnisse und Rechte)

Zu Absatz 1:

§ 24 macht von der Ermächtigung in Artikel 58 Absatz 6 der Verordnung (EU) 2016/679 Gebrauch und ergänzt die Befugnisse aus Artikel 58 Absatz 1. Über die in Artikel 58 geregelten Befugnisse hinaus erlaubt § 24 auch die Begehung von Diensträumen. Die Regelung stellt sicher, dass die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ihre bzw. seine Kontrollbefugnisse effektiv wahrnehmen kann. Der ihr bzw. ihm durch Artikel 57 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 auferlegten Beratungsaufgabe kann sie bzw. er lediglich nachkommen, wenn sie bzw. er ausreichend informiert wird. Dies wird gegenwärtig durch die Richtlinie zur Beteiligung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit in der Fassung vom 14. Februar 2011 (MittVw S. 58) sichergestellt.

Zu Absatz 2:

Der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit soll es neben der ihm zukommenden Befugnis zur Veröffentlichung eines Tätigkeitsberichts gemäß Artikel 59 der Verordnung (EU) 2016/679 weiterhin erlaubt sein, u.a. in Form von Pressemitteilungen an die Öffentlichkeit heranzutreten.

Zu Absatz 3:

Absatz 2 stellt klar, dass eine Verhängung von Bußgeldern gegenüber öffentlichen Stellen oder Behörden nur in Betracht kommt, soweit diese als Unternehmen am Wettbewerb teilnehmen.

Zu Artikel 1 § 25 (Verwaltungsgebühren)

Wie nach bisherigem Recht trägt grundsätzlich die kontrollierte Stelle die Kosten des Überprüfungsverfahrens. Eine Ausnahme findet sich in § 25 Absatz 2 Satz 2 für den Fall dass die Überprüfung weder von der Aufsichtsbehörde noch vom Datenschutzbeauftragten der kontrollierten Stelle veranlasst wurde und keine Mängel gefunden wurden. Nach Artikel 57 Absatz 3 DSGVO ist die Prüfung der Aufsichtsbehörde kostenfrei, soweit die betroffene Person der Antragsteller ist. Eine Ausnahme sieht insoweit nur Artikel 57 Absatz 4 DSGVO vor, der bei offenkundigen Missbrauchsfällen die Erhebung einer angemessenen Gebühr erlaubt. Von dieser Regelungsermächtigung macht § 25 Absatz 3 Gebrauch und legt in Anlehnung an Artikel 6 EGStGB eine Obergrenze von Euro 1.000 fest.

Zu Artikel 1 § 26 (Strafvorschrift)

Die Vorschrift bildet im Wesentlichen die vorherige Rechtslage nach § 32 HmbDSG a.F. ab. Es erfolgte eine terminologische Anpassung an die Datenschutz-Grundverordnung hinsichtlich des unionsrechtlich definierten Begriffs der Verarbeitung (Artikel 4 Nummer 2 der Verordnung (EU) 2016/679). Erweitert wurde die Bestimmung dahingehend, dass Absatz 3 die Antragsberechtigten nunmehr ausdrücklich nennt. Dabei wird der Bestimmung des Artikels 58 Absatz 5 der Verordnung (EU) 2016/679 Rechnung getragen.

Zu Artikel 1 § 27 Ordnungswidrigkeiten

Die Vorschrift entspricht inhaltlich dem bisherigen § 33 HmbDSG a.F. wobei die in Absatz 1 Nummer 1 aufgeführten Tathandlungen mit der Zusammenfassung unter dem Begriff „Verarbeitung“ an die europarechtliche Terminologie angepasst wurden.

Zu Artikel 2 (Änderung des Hochschulgesetzes)

Die Verordnung (EU) 2016/679 verwendet nicht die im deutschen Recht bisher bekannte Verarbeitungstrias von Erheben, Verarbeiten und Nutzen (vgl. § 3 BDSG a.F.), „Verarbeitung“ im Sinne der Verordnung (EU) 2016/679 umfasst vielmehr alle Formen des Umgangs mit personenbezogenen Daten. Die vom vorstehenden Gesetzesentwurf bezweckten Änderungen des § 111 HmbHG dienen, bis auf die Änderung des Absatzes 2a durch einen neuen Satz 3, der Anpassung des § 111 HmbHG an diese Terminologie der Verordnung (EU) 2016/679.

Aus Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 ergibt sich ferner, dass die Verarbeitung von Gesundheitsdaten nur zulässig ist, wenn die betroffene Person in die Verarbeitung ausdrücklich eingewilligt hat. Die Änderung des Absatzes 2a durch einen neuen Satz 3 passt die Vorschrift an dieses von der Verordnung(EU) 2016/679 aufgestellte Erfordernis der ausdrücklichen Einwilligung in die Verarbeitung von Gesundheitsdaten an.

Der Verweis in Absatz 5 Nummer 5 auf § 11a Absatz 1 Sätze 3 und 4 HmbDSG wird gestrichen, da die Vorschrift durch die Regelungen der Verordnung (EU) 2016/679 überlagert wird.

Zu Artikel 3 (Änderung des Hamburgischen Transparenzgesetzes)

Zu Nummer 1:

Die Möglichkeit, sich wegen einer Rechtsverletzung durch die Verarbeitung personenbezogener Daten nach dem Hamburgischen Transparenzgesetz an die oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zu wenden, ergibt sich mit der Neufassung des Hamburgischen Datenschutzgesetzes nicht mehr aus diesem, sondern unmittelbar aus Artikel 57 der Verordnung (EU) 2016/679. Der bisherige deklaratorische Hinweis in Satz 2 kann daher gestrichen werden.

Zu Nummer 2:

Es handelt sich um eine Folgeänderung der Neufassung des Hamburgischen Datenschutzgesetzes; Berufung und Rechtsstellung der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ergeben sich nunmehr aus §§ 20 und 21 des Hamburgischen Datenschutzgesetzes.

Zu Artikel 4 (Änderung des Hamburgischen Ausführungsgesetzes zum Bundesmeldegesetz)

Zu den Nummern 1, 2, 3b und 4b:

Die Verweise in § 1 Absatz 3 Satz 1 und 2 auf § 10 Absatz 1 und § 8 HmbDSG a.F. können entfallen, da ihr Regelungsgehalt zur Durchführung des Datenschutzes bzw. zu den technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes in Artikel 24 der Verordnung (EU) 2016/679 enthalten sind.

Zu den Nummern 3a und 4a:

Der Begriff „Verarbeitung“ im Sinne der Verordnung (EU) 2016/679 umfasst alle Formen des Umgangs mit personenbezogenen Daten. Die Änderungen dienen der Anpassung an diese Terminologie.

Zu Artikel 5 (Aufhebung der Verordnung über die Angabe personenbezogener Daten gegenüber den Hochschulen)

Gemäß § 131 Absatz 6 HmbHG tritt mit dem Zeitpunkt, an dem eine datenschutzrechtliche Satzung in Kraft tritt, für die betreffende Hochschule die Hochschuldatenverordnung außer Kraft. Für alle Hochschulen ist inzwischen eine solche Satzung in Kraft getreten, zuletzt für die Hochschule für bildende Künste Hamburg am 15. Dezember 2016. Der Hochschuldatenverordnung kommt daher keine eigene Bedeutung mehr zu, sodass sie im Sinne der Rechtsbereinigung aufzuheben ist.

Artikel 6 (Verordnungsermächtigung)

Mit dem Gesetz zur Anpassung des Hamburgischen Datenschutzgesetzes entfallen die Verordnungsermächtigungen in §§ 11, 11a HmbDSG a.F. zwecks Konkretisierung der gesetzlichen Vorgaben zum einen für automatisierte Abrufverfahren und zum anderen für gemeinsame und verbundene Dateien. Auf diesen Grundlagen erlassene Rechtsverordnungen gelten nach Wegfall der gesetzlichen Vorschrift, auf die sich ihr Erlass stützte, eigenständig fort. Um diese Rechtsverordnungen aber zu einem späteren Zeitpunkt aufheben zu können, bedarf es einer förmlichen gesetzlichen Grundlage. Diese stellt das Gesetz mit Artikel 6 bereit. Dem Senat wird hierdurch ermöglicht, auf Grund der §§ 11 und 11a HmbDSG a.F. erlassene Rechtsverordnungen im Wege des Erlasses einer Rechtsverordnung aufheben zu können, ohne dass es zum Zeitpunkt der beabsichtigten Aufhebung des Erlasses eines förmlichen Gesetzes bedürfte.

Artikel 7 (Schlussbestimmungen)

Absatz 1 regelt das Inkrafttreten des Artikelgesetzes. Absatz 2 betrifft die dienstrechtliche Einordnung des amtierenden Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit anlässlich der Neuregelungen des Artikels 1 dieses Gesetzes.

Gestaltung und Layout: Lütcke & Wulff, Rondenbarg 8, 22525 Hamburg, Tel. (040) 23 51 29-0