



# Hamburg

## Hamburgisches Datenschutzgesetz (HmbDSG)

Vom 5. Juli 1990 (HmbGVBl. S. 133, ber. 165, 226), zuletzt geändert durch Art. 2 des Gesetzes vom 18. November 2003 (HmbGVBl. S. 537, 539).

---

### Inhaltsübersicht

<b>Hamburgisches Datenschutzgesetz (HmbDSG)</b> .....	<b>1</b>
<b>ERSTER ABSCHNITT</b>	
<b>Allgemeine Vorschriften</b> .....	<b>4</b>
§ 1 Aufgabe des Datenschutzes.....	4
§ 2 Anwendungsbereich .....	4
§ 3 Datenverarbeitung im Auftrag.....	6
§ 4 Begriffsbestimmungen .....	8
§ 4 a (aufgehoben) .....	10
§ 5 Zulässigkeit der Datenverarbeitung.....	10
§ 5 a Automatisierte Einzelentscheidungen .....	13
§ 5 b Mobile Datenverarbeitungsmedien.....	13
§ 6 Rechte der Betroffenen.....	14

§ 7 Datengeheimnis ..... 15

§ 8 Technische und organisatorische Maßnahmen; Vorabkontrolle ..... 16

§ 9 Verfahrensbeschreibung..... 17

§ 10 Durchführung des Datenschutzes ..... 19

§ 10 a Behördliche Datenschutzbeauftragte bzw. behördlicher Datenschutz-  
beauftragter ..... 19

§ 11 Automatisiertes Abrufverfahren ..... 21

§ 11a Gemeinsame und verbundene automatisierte Dateien ..... 23

**ZWEITER ABSCHNITT**

**Rechtsgrundlagen der Datenverarbeitung..... 24**

§ 12 Datenerhebung ..... 24

§ 12 a Unterrichtung bei der Erhebung ..... 24

§ 13 Zulässigkeit der weiteren Datenverarbeitung; Zweckbindung..... 27

§ 14 Übermittlung innerhalb des öffentlichen Bereichs ..... 29

§ 15 Übermittlung an öffentlich-rechtliche Religionsgesellschaften ..... 30

§ 16 Übermittlung an Stellen außerhalb des öffentlichen Bereichs..... 30

§ 17 Übermittlung an Stellen außerhalb der Bundesrepublik Deutschland  
..... 31

**DRITTER ABSCHNITT**

**Rechte der Betroffenen ..... 34**

§ 18 Auskunft ..... 34

§ 19 Berichtigung, Sperrung und Löschung ..... 36

§ 20 Schadensersatz ..... 38

**VIERTER ABSCHNITT**

**Die bzw. der Hamburgische Datenschutzbeauftragte..... 39**

§ 21 Berufung ..... 39

§ 22 Rechtsstellung ..... 39

§ 23 Aufgaben..... 41

§ 24 (aufgehoben) ..... 43

§ 25 Beanstandungen..... 43

§ 26 Anrufung ..... 44

**FÜNFTER ABSCHNITT**

**Besondere Vorschriften über den Datenschutz ..... 46**

§ 27 Datenverarbeitung zum Zwecke wissenschaftlicher Forschung ... 46

§ 28 Datenverarbeitung bei Beschäftigungsverhältnissen ..... 47

§ 29 Fernmessen und Fernwirken ..... 50

§ 30 Datenverarbeitung für Planungszwecke..... 51

**SECHSTER ABSCHNITT**

**Straf- und Bußgeldvorschriften; Gebührevorschrift; Inkrafttreten ... 52**

§ 32 Straftaten ..... 52

§ 33 Ordnungswidrigkeiten ..... 52

§ 34 Verwaltungsgebühren ..... 53

§ 35 Inkrafttreten (nicht aufgenommen) ..... 53

# ERSTER ABSCHNITT

## Allgemeine Vorschriften

### § 1

#### **Aufgabe des Datenschutzes**

Dieses Gesetz regelt die Verarbeitung personenbezogener Daten durch öffentliche Stellen, um das Recht einer jeden Person zu schützen, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind.

### § 2

#### **Anwendungsbereich**

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch folgende öffentliche Stellen:

1. die Bürgerschaft, die Behörden, die Organe der Rechtspflege, den Rechnungshof und die sonstigen öffentlich-rechtlich organisierten Einrichtungen der Freien und Hansestadt Hamburg,
2. die der Aufsicht der Freien und Hansestadt Hamburg unterstehenden juristischen Personen des öffentlichen Rechts und deren öffentlich-rechtlich organisierte Einrichtungen,
3. Stellen, soweit sie als Beliehene hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen.

Für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, an denen die Freie und Hansestadt Hamburg oder eine ihrer Aufsicht unterstehende juristische Person des öf-

fentlichen Rechts beteiligt ist, gelten nur die auf nicht-öffentliche Stellen anzuwendenden Vorschriften des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung, wenn sie keine öffentlichen Stellen des Bundes gemäß § 2 Absatz 3 des Bundesdatenschutzgesetzes sind.

(2) Soweit die in Absatz 1 Satz 1 genannten Stellen als Unternehmen am Wettbewerb teilnehmen, gelten von den Vorschriften dieses Gesetzes nur die [§§ 10, 28](#), 29 und der Vierte Abschnitt. Im Übrigen sind die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme des § 38 in der jeweils geltenden Fassung anzuwenden.

(3) Für öffentlich-rechtliche Kreditinstitute gelten abweichend von Absatz 2 nur die Vorschriften des Bundesdatenschutzgesetzes, die auf nicht-öffentliche Stellen anzuwenden sind. Für die Hamburgische Wohnungsbaukreditanstalt gilt Satz 1 jedoch nicht, soweit sie Verwaltungsaufgaben wahrnimmt, die ihr gemäß § 3 Absatz 4 des Gesetzes über die Hamburgische Wohnungsbaukreditanstalt in der Fassung vom 6. März 1973 (HmbGVBl. S. 41), zuletzt geändert am 25. Juni 1997 (HmbGVBl. S. 280), in der jeweils geltenden Fassung übertragen sind.

(4) Für die Ausübung des Gnadenrechts findet dieses Gesetz keine Anwendung.

(5) Auf die nicht-automatisierte Verarbeitung personenbezogener Daten außerhalb von Dateien

1. durch die Gerichte im Rahmen der Rechtspflege,
2. durch die Staatsanwaltschaften und ihre Hilfsbeamtinnen und Hilfsbeamten bei der Verfolgung von Straftaten und bei der Strafvollstreckung sowie
3. durch die in Absatz 1 Satz 1 genannten Stellen bei der Verfolgung und Ahndung von Ordnungswidrigkeiten

finden [§ 5](#), § 6 Absatz 1 Nummern 1 bis 9 sowie die [§§ 12](#) bis 19 keine Anwendung. Satz 1 Nummer 1 gilt nicht für die Tätigkeit der Gerichtsvollzieherinnen und Gerichtsvollzieher.

(6) Dieses Gesetz gilt nicht für personenbezogene Daten, solange sie in all-gemein zugänglichen Quellen gespeichert sind, sowie für Daten von Betroffenen, die diese zur Veröffentlichung bestimmt haben.

(7) Soweit besondere Rechtsvorschriften auf die Verarbeitung personenbezogener Daten anzuwenden sind (Rechtsvorschriften über den Datenschutz), gehen sie den Vorschriften dieses Gesetzes vor.

### **§ 3**

#### **Datenverarbeitung im Auftrag**

(1) Die Vorschriften dieses Gesetzes gelten für die in [§ 2](#) Absatz 1 Satz 1 genannten Stellen auch insoweit, als personenbezogene Daten in deren Auftrag durch andere Stellen verarbeitet werden. In diesen Fällen ist die auftragnehmende Stelle unter besonderer Berücksichtigung der Eignung der von ihr getroffenen technischen und organisatorischen Maßnahmen ([§ 8](#)) sorgfältig auszuwählen. Bei Erteilung des Auftrags sind, falls erforderlich, ergänzende technische und organisatorische Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen. Die auftragnehmenden Stellen sind zu verpflichten, die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihnen überlassen worden sind, sowie nach Erledigung des Auftrags die überlassenen Datenträger zurückzugeben, zu löschen oder zu vernichten und bei ihnen gespeicherte personenbezogene Daten zu löschen, soweit nicht besondere Rechtsvorschriften entgegenstehen.

(2) Die Vorschriften der [§§ 12](#) bis 20 gelten nicht für die in § 2 Absatz 1

Satz 1 genannten Stellen, soweit sie personenbezogene Daten im Auftrag verarbeiten. In diesen Fällen ist die Datenverarbeitung nur im Rahmen der Weisungen der auftraggebenden Stelle zulässig. Ist die auftragnehmende Stelle der Ansicht, dass eine solche Weisung gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, so hat sie die auftraggebende Stelle unverzüglich darauf hinzuweisen.

(3) Sofern die [§§ 7](#) und 8 auf die auftragnehmende Stelle keine Anwendung finden, ist die auftraggebende Stelle verpflichtet, vertraglich sicherzustellen, dass die auftragnehmende Stelle die in diesen Bestimmungen für auftragnehmende Stellen enthaltenen Regelungen befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Überwachung der bzw. des Hamburgischen Datenschutzbeauftragten unterwirft. Bei einer Auftragsdurchführung außerhalb des Geltungsbereichs dieses Gesetzes ist die zuständige Datenschutzaufsichtsbehörde zu unterrichten.

(4) Die Absätze 1 bis 3 gelten entsprechend, soweit Stellen im Auftrag

1. beratende, begutachtende oder vergleichbare unterstützende Tätigkeiten ausführen,
2. Wartungsarbeiten oder Hilfstätigkeiten bei der Datenverarbeitung erledigen

und hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

## § 4 Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene, betroffene Personen).

(2) Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen personenbezogener Daten.

Im Einzelnen ist

1. Erheben das Beschaffen von Daten über Betroffene,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Verändern das inhaltliche Umgestalten von Daten,
4. Übermitteln das Bekanntgeben von Daten an Dritte in der Weise, dass die Daten weitergegeben, zur Einsicht bereitgehalten oder veröffentlicht werden oder dass Dritte in einem automatisierten Verfahren bereitgehaltene Daten abrufen,
5. Sperren das Verhindern weiterer Verarbeitung von Daten,
6. Löschen das Unkenntlichmachen von Daten oder das Vernichten des Datenträgers,
7. Nutzen jede sonstige Verwendung von Daten

ungeachtet der dabei angewendeten Verfahren.

(3) Daten verarbeitende Stelle ist jede der in [§ 2](#) Absatz 1 Satz 1 genannten Stellen, die allein oder gemeinsam mit anderen Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.



(4) Dritte sind alle Stellen außerhalb der Daten verarbeitenden Stelle, ausgenommen die Betroffenen und diejenigen Stellen, die in einem Mitgliedstaat der Europäischen Union personenbezogene Daten im Auftrag verarbeiten.

(5) Empfängerinnen und Empfänger sind alle Personen oder Stellen, die Daten erhalten.

(6) Eine Datei ist eine Sammlung personenbezogener Daten, die

1. durch automatisierte Verfahren verarbeitet werden kann (automatisierte Datei) oder
2. gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann (nicht-automatisierte Datei).

(7) Stellen sind natürliche Personen, juristische Personen und ihre Handlungseinheiten, Gesellschaften und andere Personenvereinigungen des privaten Rechts.

(8) Ein Datenträger ist jedes Material, auf dem Einzelangaben wahrnehmbar festgehalten werden.

(9) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.

(10) Pseudonymisieren ist das Verändern personenbezogener Daten mittels einer Zuordnungsregel derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis dieser Regel nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.

§ 4 a  
(aufgehoben)

**§ 5**  
**Zulässigkeit der Datenverarbeitung**

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, soweit

1. dieses Gesetz oder eine besondere Rechtsvorschrift über den Datenschutz sie erlaubt oder
2. die Betroffenen eingewilligt haben.

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben ist nur zulässig, soweit

1. die [§§ 15](#), 27 bis 30 oder eine besondere Rechtsvorschrift über den Datenschutz sie erlaubt,
2. die Betroffenen ausdrücklich eingewilligt haben,
3. es sich um Daten handelt, die die Betroffenen offensichtlich öffentlich gemacht haben,
4. sie zum Schutz lebenswichtiger Interessen der Betroffenen oder Dritter erforderlich ist und die Betroffenen aus rechtlichen oder tatsächlichen Gründen außer Stande sind, ihre Einwilligung zu geben,
5. sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,

6. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl zwingend erforderlich ist oder
7. sie zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und durch ärztliches Personal oder sonstige Personen erfolgt, die einem entsprechenden Berufs- oder besonderen Amtsgeheimnis unterliegen.

Satz 2 gilt nicht für

1. die Verarbeitung personenbezogener Daten zur Wahrnehmung von Aufgaben der Gefahrenabwehr und der Verfolgung von Straftaten sowie
2. die nicht-automatisierte Verarbeitung personenbezogener Daten außerhalb von Dateien.

Vor der Entscheidung, personenbezogene Daten nach Satz 2 Nummer 6 zu verarbeiten, ist die bzw. der behördliche Datenschutzbeauftragte oder, falls keine behördliche Datenschutzbeauftragte bzw. kein behördlicher Datenschutzbeauftragter bestellt wurde, die bzw. der Hamburgische Datenschutzbeauftragte zu hören.

(2) Die Einwilligung in die Verarbeitung personenbezogener Daten bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Gegenstand, Inhalt und Umfang der erlaubten Verarbeitung, insbesondere die Art der Daten, die Adressaten der Übermittlung, der Verwendungszweck und die Dauer der Aufbewahrung, sind in der Einwilligungserklärung klar und verständlich zu bezeichnen; die Betroffenen sind unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen können. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Die Einwilligung ist unwirksam, wenn sie durch unangemessene An-

drohung von Nachteilen, durch fehlende Aufklärung oder in sonstiger gegen die Gebote von Treu und Glauben verstoßender Weise erlangt wurde.

(3) Machen Betroffene schriftlich den Einwand geltend, dass einer Verarbeitung ihrer personenbezogenen Daten schutzwürdige, sich aus ihrer besonderen persönlichen Lage ergebende Gründe entgegenstehen, so ist die weitere Verarbeitung nur zulässig, nachdem eine Abwägung im Einzelfall ergeben hat, dass die geltend gemachten Gründe hinter dem öffentlichen Interesse an der Verarbeitung zurückstehen müssen. Satz 1 gilt nicht, soweit die Verarbeitung personenbezogener Daten

1. auf einer Einwilligung der Betroffenen beruht oder
2. zur Erfüllung einer rechtlichen Verpflichtung der Daten verarbeitenden Stelle erforderlich ist.

3 Wird dem Einwand entsprochen, so sind unverzüglich die Stellen zu verständigen, denen die Daten übermittelt worden sind; die Verständigung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Wird dem Einwand nicht entsprochen, so sind die Betroffenen darauf hinzuweisen, dass sie sich an die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten wenden können.

(4) Die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung technischer Einrichtungen haben sich auch an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiter zu verarbeiten. Dabei ist jeweils zu prüfen, inwieweit es möglich ist, personenbezogene Daten anonym oder pseudonym zu verarbeiten. Erforderlich sind Maßnahmen zur anonymen oder pseudonymen Datenverarbeitung nur, wenn ihr Aufwand in einem angemess-

senen Verhältnis zur Schutzwürdigkeit der Daten steht.

### **§ 5 a**

#### **Automatisierte Einzelentscheidungen**

(1) Entscheidungen, die für die Betroffenen rechtliche Folgen nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient.

(2) Absatz 1 gilt nicht, soweit

1. ein Gesetz, das die Wahrung der berechtigten Interessen der Betroffenen sicherstellt, solche Entscheidungen zulässt,
2. mit der Entscheidung einem Begehren der Betroffenen stattgegeben wird oder
3. den Betroffenen das Vorliegen einer Entscheidung im Sinne von Absatz 1 mitgeteilt und die Wahrung ihrer berechtigten Interessen durch geeignete Maßnahmen sichergestellt wird; als geeignete Maßnahme gilt insbesondere die Möglichkeit der Betroffenen, ihren Standpunkt geltend zu machen; die Daten verarbeitende Stelle ist verpflichtet, ihre Entscheidung unter Berücksichtigung der Stellungnahme der bzw. des Betroffenen erneut zu prüfen.

### **§ 5 b**

#### **Mobile Datenverarbeitungsmedien**

Gibt eine in [§ 2](#) Absatz 1 Satz 1 genannte Stelle mobile Datenverar-

beitungsmedien, insbesondere Chipkarten heraus, die mit von ihr oder Dritten bereitgestellten technischen Einrichtungen personenbezogene Daten mit oder ohne Mitwirkung der Betroffenen automatisiert austauschen können, so hat sie sicherzustellen, dass die Betroffenen den Datenaustausch jeweils erkennen und die ihnen nach diesem Gesetz zustehenden Rechte ohne unverhältnismäßigen Aufwand geltend machen können. Spätestens bei der Ausgabe sind die Betroffenen über die ihnen nach [§ 6](#) zustehenden Rechte sowie darüber aufzuklären, welche Maßnahmen bei Verlust oder beim Verdacht nicht ordnungsgemäßer Verarbeitung zu ergreifen sind.

## **§ 6 Rechte der Betroffenen**

(1) Die Betroffenen haben nach Maßgabe dieses Gesetzes ein Recht auf

1. Geltendmachung von Einwänden gegen die Verarbeitung ihrer Daten ([§ 5](#) Absatz 3),
2. Aufklärung bei der Herausgabe mobiler Datenverarbeitungsmedien ([§ 5b](#)),
3. Anrufung der bzw. des behördlichen Datenschutzbeauftragten ([§ 10a](#) Absatz 6),
4. Unterrichtung bei der Erhebung ([§ 12a](#)),
5. Sperrung der Übermittlung an Stellen außerhalb des öffentlichen Bereichs ([§ 16](#) Absatz 3),
6. Auskunft ([§ 18](#)),

7. Berichtigung ([§ 19](#) Absatz I),
  8. Sperrung (§ 19 Absatz 2),
  9. Löschung (§ 19 Absatz 3),
  10. Schadensersatz ([§ 20](#)),
  11. Anrufung der bzw. des Hamburgischen Datenschutzbeauftragten ([§ 26](#)).
- (2) Auf diese Rechte kann nicht im Vorwege verzichtet werden.

## **§ 7** **Datengeheimnis**

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

## § 8

### **Technische und organisatorische Maßnahmen; Vorabkontrolle**

(1) Die Daten verarbeitenden Stellen und ihre auftragnehmenden Stellen haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Erforderlich sind technische und organisatorische Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht.

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. die personenbezogenen Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben (Integrität),
3. die personenbezogenen Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. die personenbezogenen Daten ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit).

(3) Werden personenbezogene Daten nicht-automatisiert verarbeitet, sind technische und organisatorische Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

(4) Vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezoge-



ne Daten verarbeitet werden sollen, haben die Daten verarbeitenden Stellen zu untersuchen, ob und in welchem Umfang mit der Nutzung dieses Verfahrens Gefahren für die Rechte der Betroffenen verbunden sind. Die Einführung und die wesentliche Änderung eines automatisierten Verfahrens sind nur zulässig, soweit derartige Gefahren durch technische und organisatorische Maßnahmen wirksam beherrscht werden können, es sei denn, dass solche Maßnahmen gemäß Absatz 1 Satz 2 nicht erforderlich sind. Ergibt die Untersuchung, dass von einem Verfahren eine besondere Gefährdung für die Rechte der Betroffenen ausgeht, so ist das Ergebnis der Untersuchung vor der Einführung oder wesentlichen Änderung des Verfahrens der bzw. dem behördlichen Datenschutzbeauftragten oder, falls keine behördliche Datenschutzbeauftragte bzw. kein behördlicher Datenschutzbeauftragter bestellt wurde, der bzw. dem Hamburgischen Datenschutzbeauftragten zur Stellungnahme zuzuleiten.

## **§ 9**

### **Verfahrensbeschreibung**

(1) Die Daten verarbeitende Stelle legt in einer laufend auf dem neuesten Stand zu haltenden Verfahrensbeschreibung für jedes automatisierte Verfahren, mit dem personenbezogene Daten verarbeitet werden sollen, fest

1. den Namen und die Anschrift der Daten verarbeitenden Stelle,
2. die Bezeichnung des Verfahrens und seine Zweckbestimmungen,
3. die Art der verarbeiteten Daten sowie die Rechtsgrundlage ihrer Verarbeitung oder die Ziele, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,

4. den Kreis der Betroffenen,
5. die Empfängerinnen oder Empfänger oder den Kreis der Empfängerinnen und Empfänger, die Daten erhalten können,
6. eine beabsichtigte Datenübermittlung nach [§ 17](#) Absätze 2 und 3,
7. Fristen für die Sperrung und Löschung der Daten,
8. die technischen und organisatorischen Maßnahmen nach [§ 8](#),
9. die Art der Geräte, die Stellen, bei denen sie aufgestellt sind sowie das Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung.

Die Daten verarbeitende Stelle kann die Angaben nach Satz 1 für mehrere gleichartige Verfahren in einer Verfahrensbeschreibung zusammenfassen.

(2) Absatz 1 gilt nicht für Verfahren,

1. deren einziger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht,
2. die der Unterstützung der allgemeinen Bürotätigkeit dienen, insbesondere Verfahren der Textverarbeitung, Vorgangsverwaltung, Terminüberwachung und der Führung von Adress-, Telefon- und vergleichbaren Verzeichnissen, soweit sie keine Beeinträchtigung der Rechte Betroffener erwarten lassen.

(3) Daten verarbeitende Stellen, die keine behördlichen Datenschutzbeauftragten bestellt haben, übersenden ihre Verfahrensbeschreibungen und deren Änderungen unverzüglich, jedenfalls aber vor der Einführung oder wesentlichen Änderung eines Verfahrens an die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten. Die Verfahrensbeschreibungen können bei der

Daten verarbeitenden Stelle von jeder Person eingesehen werden; für die Angaben nach Absatz 1 Satz 1 Nummern 8 und 9 gilt dies nur, soweit dadurch die Sicherheit des Verfahrens nicht beeinträchtigt wird. Satz 2 gilt nicht für die Verfahrensbeschreibungen der in [§ 23](#) Absatz 6 genannten Stellen.

## **§ 10**

### **Durchführung des Datenschutzes**

Die in [§ 2](#) Absatz 1 Satz 1 genannten Stellen haben die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz jeweils für ihren Geschäftsbereich sicherzustellen. Sie haben insbesondere dafür zu sorgen, dass die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird. Der Senat kann die Überwachung nach Satz 2 für die Stellen der Freien und Hansestadt Hamburg einer anderen Stelle zuweisen, wenn die Überwachung besondere Fachkenntnisse hinsichtlich der verwendeten Datenverarbeitungssysteme erfordert.

## **§ 10 a**

### **Behördliche Datenschutzbeauftragte bzw. behördlicher Datenschutzbeauftragter**

(1) Die in [§ 2](#) Absatz 1 Satz 1 genannten Stellen können eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen. Die Bestellung einer oder eines Beschäftigten einer anderen in § 2 Absatz 1 Satz 1 genannten Stelle ist zulässig.

(2) Zu behördlichen Datenschutzbeauftragten dürfen nur Personen bestellt werden, die die zur Aufgabenerfüllung erforderliche Fachkunde und Zuverlässigkeit besitzen.

(3) Die Bestellung kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs widerrufen werden. Vor der Entscheidung über den Widerruf sind die bzw. der behördliche Datenschutzbeauftragte sowie die bzw. der Hamburgische Datenschutzbeauftragte zu hören.

(4) Die behördlichen Datenschutzbeauftragten können sich unmittelbar an die Leitung der Daten verarbeitenden Stelle wenden. Sie sind bei ihrer Tätigkeit weisungsfrei und dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. Sie sind in erforderlichem Umfang von der Erfüllung anderer Aufgaben freizustellen und bei der Erfüllung ihrer Aufgaben zu unterstützen.

(5) Die behördlichen Datenschutzbeauftragten haben die Aufgabe, die Daten verarbeitenden Stellen und deren Personalvertretungen in der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen. Sie können sich zu diesem Zweck jederzeit unmittelbar an die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten wenden. Zu ihren Aufgaben gehört es insbesondere,

1. auf die Umsetzung und Einhaltung von Vorschriften über den Datenschutz hinzuwirken,
2. die nach [§ 9](#) Absatz 1 zu erstellenden Verfahrensbeschreibungen zu führen und zur Einsicht nach § 9 Absatz 3 bereitzuhalten,
3. das Ergebnis der Untersuchung nach [§ 8](#) Absatz 4 zu prüfen und im Zweifelsfall die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten zu hören.

Soweit Rechtsvorschriften nicht entgegenstehen, können sie die zur Erfüllung ihrer Aufgaben erforderliche Einsicht in alle Unterlagen und Akten und die automatisierte Datenverarbeitung nehmen.

(6) Betroffene und Beschäftigte der Daten verarbeitenden Stellen können sich in allen Angelegenheiten des Datenschutzes jederzeit unmittelbar an die behördlichen Datenschutzbeauftragten wenden; niemand darf deswegen gemäßregelt oder benachteiligt werden.

(7) Die behördlichen Datenschutzbeauftragten 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. Dies gilt nicht, soweit die Betroffenen oder Beschäftigten sie von der Pflicht zur Verschwiegenheit entbunden haben oder eine Übermittlung der Daten nach Absatz 5 Satz 2 erforderlich ist.

(8) Die in [§ 2](#) Absatz 1 Satz 1 genannten Stellen melden die Bestellung und den Widerruf der Bestellung oder die sonstige Beendigung des Amtes behördlicher Datenschutzbeauftragter unverzüglich der bzw. dem Hamburgischen Datenschutzbeauftragten.

## **§ 11**

### **Automatisiertes Abrufverfahren**

(1) Ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte darf nur eingerichtet werden, wenn eine Rechtsvorschrift dies ausdrücklich zulässt.

(2) Der Senat wird ermächtigt, die Einrichtung automatisierter Abrufverfahren durch Rechtsverordnung zuzulassen. Die bzw. der Hamburgische Datenschutzbeauftragte ist vorher zu hören. Ein solches Verfahren ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Verordnung hat die abrufende Stelle, die Datenart und den Zweck des Abrufs festzulegen. Sie hat technische und organisatorische Maßnahmen und Maßnahmen und zur Datenschutzkontrolle vorzusehen, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(3) Die Einrichtung eines automatisierten Abrufverfahrens innerhalb einer Daten verarbeitenden Stelle bedarf der Zulassung durch die Leiterin bzw. den Leiter der Stelle, wenn die Einheit, die die Daten zum Abruf bereithält, und die abrufende Einheit unterschiedliche Aufgaben wahrnehmen. Für die Zulassung findet Absatz 2 Sätze 2 bis 6 entsprechende Anwendung.

(4) Personenbezogene Daten dürfen für Stellen außerhalb des öffentlichen Bereichs zum automatisierten Abruf nicht bereitgehalten werden; dies gilt nicht für Betroffene.

(5) Die Absätze 1 bis 4 gelten nicht für Datenbestände, die jeder oder jedem ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

## § 11a

### **Gemeinsame und verbundene automatisierte Dateien**

(1). Die Einrichtung gemeinsamer oder verbundener automatisierter Dateien, in oder aus denen mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten sollen, bedarf der ausdrücklichen Zulassung durch eine Rechtsvorschrift. Der Senat wird ermächtigt, die Einrichtung automatisierter Dateien im Sinne des Satzes 1 durch Rechtsverordnung zuzulassen. [§ 11](#) Absatz 2 Sätze 2, 3 und 5 und Absatz 5 gilt entsprechend. Die Verordnung hat die Art der zu verarbeitenden Daten, die Stellen, die in der gemeinsamen Datei oder in verbundenen Dateien Daten verarbeiten dürfen, sowie den Umfang ihrer Verarbeitungsbefugnis anzugeben und festzulegen, welche Stelle die datenschutzrechtliche Verantwortung gegenüber den Betroffenen trägt und die technischen und organisatorischen Maßnahmen trifft. Die Vorschriften über die Zulässigkeit der lesenden und schreibenden Datenverarbeitung im Einzelnen bleiben unberührt.

(2) Innerhalb einer Daten verarbeitenden Stelle bedarf die Einrichtung gemeinsamer oder verbundener automatisierter Dateien, mit denen personenbezogene Daten aus unterschiedlichen Aufgabengebieten verarbeitet werden sollen, der Zulassung durch die Leiterin bzw. den Leiter der Stelle. Für die Zulassung gilt Absatz 1 Sätze 3 bis 5 entsprechend.

## ZWEITER ABSCHNITT

### Rechtsgrundlagen der Datenverarbeitung

#### § 12

#### Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

(2) Personenbezogene Daten sollen bei den Betroffenen mit ihrer Kenntnis erhoben werden. Werden Daten nicht über einzelne Betroffene, sondern über einen bestimmbaren Personenkreis erhoben, so genügt es, wenn die Betroffenen in zumutbarer Weise von der Datenerhebung Kenntnis nehmen können. Bei anderen Stellen dürfen personenbezogene Daten unter den in [§ 13](#) Absatz 2 Satz 1 genannten Voraussetzungen erhoben werden. Bei Betroffenen dürfen Daten ohne ihre Kenntnis nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder der Schutz von Leben oder Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies erforderlich macht. Durch die Art und Weise des Erhebens dürfen schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden.

#### § 12 a

#### Unterrichtung bei der Erhebung

(1) Werden Daten bei Betroffenen mit ihrer Kenntnis erhoben, so sind sie, sofern sie nicht bereits auf andere Weise Kenntnis erlangt haben, von der Daten verarbeitenden Stelle über



1. die Zweckbestimmungen der Datenverarbeitung und
2. die Empfängerinnen oder Empfänger oder den Kreis der Empfängerinnen und Empfänger, soweit die Betroffenen nach den Umständen des Einzelfalls nicht damit rechnen müssen, dass diese die Daten erhalten,

aufzuklären. Werden die Daten auf Grund einer Rechtsvorschrift erhoben, so sind die Betroffenen in geeigneter Weise über diese aufzuklären. Soweit eine Auskunftspflicht besteht oder die Angaben Voraussetzung für die Gewährung von Rechtsvorteilen sind, sind die Betroffenen hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Werden die Daten schriftlich oder zur Niederschrift erhoben, so sollen die Betroffenen auch über bestehende Auskunfts- und Berichtigungsrechte aufgeklärt werden.

(2) Werden Daten bei Dritten oder bei Betroffenen ohne ihre Kenntnis erhoben, so sind die Betroffenen, sofern sie nicht bereits auf andere Weise Kenntnis erlangt haben, von der Daten verarbeitenden Stelle bei Beginn der Speicherung in einer Datei (§ 4 Absatz 6) oder im Fall einer beabsichtigten Übermittlung spätestens bei deren erster Durchführung zu benachrichtigen und dabei

1. die Art der erhobenen Daten,
2. die Zweckbestimmungen der Datenverarbeitung und
3. die Empfängerinnen oder Empfänger oder der Kreis der Empfängerinnen und Empfänger, soweit die Betroffenen nach den Umständen des Einzelfalls nicht damit rechnen müssen, dass diese die Daten erhalten,

anzugeben. Bei schriftlicher Benachrichtigung sind die Betroffenen auch über bestehende Auskunfts- und Berichtigungsrechte aufzuklären. Dienen die Daten der Erstellung einer Mitteilung an die Betroffenen, kann die Benachrichtigung mit der Mitteilung verbunden werden.

(3) Absatz 2 gilt nicht für die Verarbeitung personenbezogener Daten zur Wahrnehmung von Aufgaben der Gefahrenabwehr und der Verfolgung von Straftaten. Er gilt ferner nicht, soweit

1. die Verarbeitung der Daten durch Gesetz ausdrücklich vorgesehen ist,
2. die Benachrichtigung der Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde,
3. die Benachrichtigung die ordnungsgemäße Erfüllung von Aufgaben der Gefahrenabwehr oder die Verfolgung von Straftaten oder berufsrechtlichen Vergehen gefährden würde,
4. die Benachrichtigung die öffentliche Sicherheit oder die Sicherheit oder ein wichtiges wirtschaftliches oder finanzielles Interesse des Bundes oder eines Landes gefährden würde oder
5. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen überwiegender schutzwürdiger Interessen der Betroffenen oder Dritter geheim gehalten werden müssen.

Vor der Entscheidung, nach Satz 2 Nummer 1 oder 2 von einer Benachrichtigung abzusehen, ist die bzw. der behördliche Datenschutzbeauftragte oder, falls keine behördliche Datenschutzbeauftragte bzw. kein behördlicher Datenschutzbeauftragter bestellt wurde, der bzw. die Hamburgische Datenschutzbeauftragte zu hören, wenn sich die Entscheidung auf eine Vielzahl von Einzelfällen auswirkt.

(4) Werden Daten bei Dritten außerhalb des öffentlichen Bereichs auf Grund einer Rechtsvorschrift erhoben, so sind diese in geeigneter Weise über die Rechtsvorschrift aufzuklären. Soweit eine Auskunftspflicht besteht oder die Angaben Voraussetzung für die Gewährung von Rechten sind, sind sie hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

## § 13

### Zulässigkeit der weiteren Datenverarbeitung; Zweckbindung

(1) Die weitere Datenverarbeitung ist zulässig, wenn sie

1. erforderlich ist zur Erfüllung der Aufgaben der öffentlichen Stelle und
2. den Zwecken dient, für die die Daten erhoben wurden.

Daten, von denen die Stelle ohne Erhebung Kenntnis erlangt hat oder die bei ihr neu entstanden sind, dürfen für Zwecke verarbeitet werden, für die sie erstmals gespeichert worden sind.

(2) Die Datenverarbeitung für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies erlaubt oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung begründeten Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt,
2. bei Teilnahme am Privatrechtsverkehr oder zur Durchsetzung öffentlich-rechtlicher Geldforderungen ein rechtliches Interesse an der Kenntnis der zu verarbeitenden Daten vorliegt und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an der Geheimhaltung überwiegt,
3. Angaben der Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte dafür bestehen, dass sie unrichtig sind,
4. hierdurch erhebliche Nachteile für das Gemeinwohl oder schwerwiegende Beeinträchtigungen von gewichtigen Rechtspositionen einzelner verhindert oder beseitigt werden sollen,
5. 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 Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Erledigung eines gerichtlichen Aus-

kunftersuchens erforderlich ist und gesetzliche Regelungen nicht entgegenstehen,

6. die Einholung der Einwilligung der Betroffenen nicht möglich ist oder mit unverhältnismäßigem Aufwand verbunden wäre, aber offensichtlich ist, dass es in ihrem Interesse liegt und sie in Kenntnis des anderen Zwecks ihre Einwilligung erteilen würden,
7. die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen worden sind oder entnommen werden können oder die Daten verarbeitende Stelle sie veröffentlichen dürfte, es sei denn, dass schutzwürdige Interessen der Betroffenen offensichtlich entgegenstehen oder,
8. sie der Bearbeitung von Eingaben sowie Kleinen oder Großen Anfragen dient und überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen.

Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der öffentlichen Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden, findet Satz 1 Nummern 2 bis 8 keine Anwendung.

(3) Eine Datenverarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient. Zulässig ist auch die Verarbeitung zu Ausbildungs- und Prüfungszwecken, soweit nicht schutzwürdige Interessen der Betroffenen an der Geheimhaltung der Daten offensichtlich überwiegen.

## § 14

### Übermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der Aufgaben der übermittelnden oder der Stelle, der die Daten übermittelt werden, erforderlich ist und die Voraussetzungen des [§ 13](#) erfüllt sind. Die Übermittlung ist ferner zulässig, soweit es zur Entscheidung in einem Verwaltungsverfahren der Beteiligung mehrerer öffentlicher Stellen bedarf.

(2) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten von Betroffenen oder von Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unververtretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht schutzwürdige Interessen der Betroffenen oder Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Grund eines Ersuchens der Stelle, der die Daten übermittelt werden sollen, so hat die übermittelnde Stelle von den in die Sphäre der ersuchenden Stelle fallenden Übermittlungsvoraussetzungen lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht; die ersuchende Stelle hat ihr die für diese Prüfung erforderlichen Angaben zu machen. Erfolgt die Übermittlung durch Abruf in einem automatisierten Verfahren ([§§ 11, 11a](#)), trägt die abrufende Stelle die Verantwortung für die Rechtmäßigkeit des Abrufs.

(4) Absatz 2 gilt entsprechend, wenn personenbezogene Daten inner-

halb einer öffentlichen Stelle weitergegeben werden.

## § 15

### **Übermittlung an öffentlich-rechtliche Religionsgesellschaften**

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an öffentliche Stellen zulässig, sofern sichergestellt ist, dass bei der Stelle, der die Daten übermittelt werden, ausreichende Datenschutzmaßnahmen getroffen sind.

## § 16

### **Übermittlung an Stellen außerhalb des öffentlichen Bereichs**

(1) Die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen des [§ 13](#) Absatz 1 vorliegen,
2. die Voraussetzungen des § 13 Absatz 2 Satz 1 Nummern 1, 4, 6, 7 oder 8 vorliegen und die Daten nicht einem nach § 13 Absatz 2 Satz 2 zu wahrenen Berufs- oder Amtsgeheimnis unterliegen,
3. die Stelle, der die Daten übermittelt werden sollen, ein rechtliches Interesse an deren Kenntnis glaubhaft macht und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an der Geheimhaltung überwiegen,

4. sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die Betroffenen in diesen Fällen der Übermittlung nicht widersprochen haben.

In den Fällen des Satzes 1 Nummer 4 sind die Betroffenen über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise zu unterrichten.

(2) Die Stelle, der die Daten übermittelt werden, ist darauf hinzuweisen, dass sie sie nur zur Verarbeitung für den Zweck erhält, zu dem sie ihr übermittelt werden.

(3) Die Betroffenen können verlangen, dass die Übermittlung nach Absatz 1 Satz 1 Nummer 2 in Verbindung mit [§ 13](#) Absatz 2 Satz 1 Nummer 6 sowie nach Absatz 1 Satz 1 Nummern 3 und 4 gesperrt wird, wenn sie ein schutzwürdiges Interesse an der Sperrung darlegen.

## **§ 17**

### **Übermittlung an Stellen außerhalb der Bundesrepublik Deutschland**

(1) Die Übermittlung personenbezogener Daten in Mitgliedstaaten der Europäischen Union sowie an Organe und Einrichtungen der Europäischen Union ist unter den Voraussetzungen der [§§ 14](#), 16 und [28](#) zulässig.

(2) Die Übermittlung personenbezogener Daten in Staaten außerhalb der Europäischen Union und an über- oder zwischenstaatliche Stellen ist unter den Voraussetzungen der §§ 14, 16 und 28 zulässig, wenn in dem Staat außerhalb der Europäischen Union oder bei der über- oder

zwischenstaatlichen Stelle ein angemessenes Schutzniveau gewährleistet ist. Die Angemessenheit des Schutzniveaus ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenübermittlung von Bedeutung sind, insbesondere der Art der Daten, der Zweckbestimmung und Dauer ihrer geplanten Verarbeitung, des Herkunfts- und des Endbestimmungslandes sowie der anwendbaren Rechtsvorschriften, Landesregeln und Sicherheitsmaßnahmen.

(3) Ist in Staaten außerhalb der Europäischen Union oder bei über- oder zwischenstaatlichen Stellen kein angemessenes Schutzniveau gewährleistet, so ist die Übermittlung personenbezogener Daten nur zulässig, soweit

1. die Betroffenen eingewilligt haben,
2. die Übermittlung zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
3. die Übermittlung zur Wahrung lebenswichtiger Interessen der Betroffenen erforderlich ist oder
4. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist oder das allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall erfüllt sind.

Darüber hinaus ist die Übermittlung unter den Voraussetzungen der §§ 14, 16 und 28 zulässig, wenn die Stelle, der die Daten übermittelt werden sollen, ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts der Betroffenen und der damit verbundenen Rechte bietet; die Garantien können sich insbesondere aus vertraglichen Vereinbarungen ergeben. Die Übermittlung bedarf in diesem Falle der Zu-



lassung durch die Leiterin bzw. den Leiter der übermittelnden Stelle. Die bzw. der Hamburgische Datenschutzbeauftragte ist vorher zu hören. Zugelassene Übermittlungen sind der zuständigen Behörde mitzuteilen.

(4) [§ 16](#) Absatz 2 gilt entsprechend.

## DRITTER ABSCHNITT Rechte der Betroffenen

### § 18 Auskunft

(1) Den Betroffenen ist von der Daten verarbeitenden Stelle auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,
2. die Zweckbestimmungen und die Rechtsgrundlage der Speicherung,
3. die Herkunft der Daten und die Empfängerinnen oder Empfänger oder den Kreis der Empfängerinnen oder Empfänger; dies gilt nicht für Empfängerinnen und Empfänger, die die Daten im Einzelfall zur Verfolgung von Straftaten, Ordnungswidrigkeiten oder berufsrechtlichen Vergehen erhalten,
4. die an einem automatisierten Abrufverfahren teilnehmenden Stellen,
5. in den Fällen des [§ 5a](#) den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten,

auch soweit diese Angaben nicht zu ihrer Person gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Die Betroffenen sollen die Art der personenbezogenen Daten, über die sie Auskunft verlangen, näher bezeichnen. Aus Akten ist den Betroffenen Auskunft zu erteilen, soweit sie Angaben machen, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zum Auskunftsinteresse der Betroffenen steht. Die Daten verarbeitende Stelle bestimmt die Form der Auskunftserteilung nach pflichtgemäßem Ermessen; die Auskunft kann

auch in der Form erteilt werden, dass dem Betroffenen Akteneinsicht gewährt oder ein Ausdruck aus automatisierten Dateien überlassen wird. § 29 des Hamburgischen Verwaltungsverfahrensgesetzes bleibt unberührt.

(2) Die Verpflichtung zur Auskunftserteilung gilt nicht für die personenbezogenen Daten, die nur deshalb als gesperrte Daten gespeichert sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, sowie für solche Daten, die ausschließlich zum Zwecke der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(3) Die Auskunftserteilung unterbleibt, soweit die Voraussetzungen für das Absehen von einer Benachrichtigung nach [§ 12 a](#) Absatz 3 Satz 2 Nummern 3 bis 5 vorliegen oder die Daten ausschließlich für Zwecke der wissenschaftlichen Forschung oder der Statistik verarbeitet werden.

(4) Einer Begründung für die Auskunftsverweigerung bedarf es nur insoweit nicht, als durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind die wesentlichen Gründe für die Entscheidung aufzuzeichnen.

(5) Bezieht sich die Auskunft auf die Herkunft von personenbezogenen 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 von den in § 19 Absatz 3 des Bundesdatenschutzgesetzes genannten Behörden, ist sie nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt, soweit sich die Auskunft auf die Übermittlung personenbezogener Daten an diese Behörden bezieht. Für die Versagung der Zustimmung gelten, soweit dieses Gesetz auf die genannten Behörden Anwendung findet, die Absätze 3 und 4 entsprechend.

(6) Wird die Auskunft nicht gewährt, so sind die Betroffenen darauf hinzuweisen, dass sie sich an die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten wenden können.

## **§ 19**

### **Berichtigung, Sperrung und Löschung**

(1) Personenbezogene Daten sind unverzüglich zu berichtigen, wenn sie unrichtig sind. Sind Daten außerhalb automatisierter Dateien zu berichtigen, reicht es aus, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt oder aus welchem Grund diese Daten unrichtig waren oder unrichtig geworden sind.

(2) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit von den Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,
2. in den Fällen des Absatzes 3 Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange Betroffener beeinträchtigt würden, oder wenn Betroffene an Stelle der Löschung die Sperrung verlangen,
3. sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

Satz 1 Nummer 1 gilt nicht, wenn personenbezogene Daten in Akten gespeichert sind; in diesen Fällen ist in den Akten lediglich zu vermerken, dass die Daten von den Betroffenen bestritten worden sind. Gesperrte Daten sind als solche zu kennzeichnen. Ohne Einwilligung der Betroffenen dürfen sie nur weiterverarbeitet werden, wenn es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der Daten verarbei-

tenden Stelle oder Dritter liegenden Gründen unerlässlich ist und die Voraussetzungen des [§ 13](#) oder des [§ 27](#) vorliegen.

(3) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.

Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Satz 1 Nummer 2 nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist; soweit hiernach eine Löschung nicht in Betracht kommt, sind die personenbezogenen Daten zu sperren.

(4) Abgesehen von den Fällen des Absatzes 3 Satz 1 Nummer 1 sind die Daten vor einer Löschung dem zuständigen öffentlichen Archiv nach Maßgabe des § 3 des Hamburgischen Archivgesetzes vom 21. Januar 1991 (HmbGVBl. S. 7), geändert am 30. Januar 2001 (HmbGVBl. S. 9,16) in seiner jeweiligen Fassung anzubieten.

(5) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener oder unzulässig gespeicherter Daten und der Löschung unzulässig gespeicherter Daten sind unverzüglich die Stellen zu verständigen, denen die Daten übermittelt worden sind; die Verständigung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Im Übrigen liegt die Verständigung im pflichtgemäßen Ermessen der Daten verarbeitenden Stelle.

(6) In automatisierten Dateien gespeicherte Daten sind regelmäßig alle vier Jahre auf ihre Erforderlichkeit hin zu überprüfen und die Datenbestände gemäß Absatz 3 zu bereinigen.

## **§ 20**

### **Schadensersatz**

(1) Werden Betroffene durch eine unzulässige oder unrichtige Datenverarbeitung in ihren schutzwürdigen Belangen beeinträchtigt, so hat ihnen der Träger der in § 2 Absatz 1 Satz 1 genannten Stelle den daraus entstehenden Schaden zu ersetzen. In schweren Fällen können Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Die Ersatzpflicht tritt nicht ein, soweit die Daten verarbeitende Stelle den Umstand, durch den der Schaden eingetreten ist, nicht zu vertreten hat. Beruht der Schaden auf einer unzulässigen oder unrichtigen automatisierten Datenverarbeitung, so tritt die Ersatzpflicht auch im Falle des Satzes 3 ein, beschränkt sich jedoch in diesem Falle gegenüber jeder betroffenen Person auf zweihundertfünfzigtausend Euro) für jedes schädigende Ereignis.

(2) Auf das Mitverschulden von Verletzten sind § 254 und § 839 Absatz 3 des Bürgerlichen Gesetzbuches und auf die Verjährung die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(3) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

## VIERTER ABSCHNITT

### Die bzw. der Hamburgische Datenschutzbeauftragte

#### **§ 21**

#### **Berufung**

(1) Auf Vorschlag des Senats wählt die Bürgerschaft eine Hamburgische Datenschutzbeauftragte oder einen Hamburgischen Datenschutzbeauftragten; die Wiederwahl ist einmal zulässig. Die bzw. der Hamburgische Datenschutzbeauftragte muss die Befähigung zum Richteramt oder zum höheren Verwaltungsdienst haben und die zur Erfüllung ihrer bzw. seiner Aufgaben erforderliche Fachkunde besitzen. Sie bzw. er muss bei ihrer bzw. seiner Bestellung das 35. Lebensjahr vollendet haben.

(2) Der Senat bestellt die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten für eine Amtszeit von sechs Jahren.

(3) Die bzw. der Hamburgische Datenschutzbeauftragte ist verpflichtet, das Amt bis zur Bestellung einer Nachfolgerin oder eines Nachfolgers weiterzuführen; die Amtszeit gilt als entsprechend verlängert. Kommt die bzw. der Hamburgische Datenschutzbeauftragte der Verpflichtung nach Satz 1 nicht nach, ist sie bzw. er zu entlassen.

#### **§ 22**

#### **Rechtsstellung**

(1) In Ausübung des Amtes ist die bzw. der Hamburgische Datenschutzbeauftragte unabhängig und nur dem Gesetz unterworfen. Sie

bzw. er ist insoweit oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung sowie oberste Aufsichtsbehörde im Sinne des § 99 der Verwaltungsgerichtsordnung und trifft die Entscheidungen nach den §§ 65 und 66 des Hamburgischen Beamtengesetzes für sich und die ihr bzw. ihm zugewiesenen Bediensteten. Sie bzw. er untersteht der Dienstaufsicht des Senats.

(2) Der bzw. dem Hamburgischen Datenschutzbeauftragten wird die zur Aufgabenerfüllung notwendige Personal- und Sachausstattung vom Senat im Rahmen der haushaltsmäßigen Bestimmungen zur Verfügung gestellt. Die Stellen werden auf Vorschlag der bzw. des Hamburgischen Datenschutzbeauftragten besetzt. Die Mitarbeiterinnen und Mitarbeiter können nur im Einvernehmen mit ihr bzw. ihm versetzt oder abgeordnet werden. Die bzw. der Hamburgische Datenschutzbeauftragte ist Dienstvorgesetzte bzw. Dienstvorgesetzter ihrer bzw. seiner Mitarbeiterinnen und Mitarbeiter; diese sind in ihrer Tätigkeit nach diesem Gesetz nur an ihre bzw. seine Weisungen gebunden.

(3) Die bzw. der Hamburgische Datenschutzbeauftragte bestimmt eine Mitarbeiterin oder einen Mitarbeiter zur Vertreterin bzw. zum Vertreter. Diese bzw. dieser nimmt die Befugnisse der bzw. des Hamburgischen Datenschutzbeauftragten im Falle von deren bzw. dessen Verhinderung wahr. Dauert die Verhinderung länger als zwei Monate, so kann der Senat eine Person mit der Wahrnehmung der Geschäfte beauftragen; die bzw. der Hamburgische Datenschutzbeauftragte soll hierzu gehört werden. Endet das Amtsverhältnis der bzw. des Hamburgischen Datenschutzbeauftragten, gelten Satz 2 und Satz 3 erster Halbsatz bis zur Bestellung einer Nachfolgerin oder eines Nachfolgers entsprechend.



## **§ 23** **Aufgaben**

(1) Die bzw. der Hamburgische Datenschutzbeauftragte überwacht bei den in [§ 2](#) Absatz 1 Satz 1 genannten Stellen und bei anderen Stellen, soweit sie sich auf Grund gesetzlicher Vorschriften ihrer bzw. seiner Überwachung unterworfen haben, die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Die Bürgerschaft, die Gerichte und der Rechnungshof unterliegen der Überwachung durch die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden; die Einschränkung gilt nicht für Gerichtsvollzieherinnen und Gerichtsvollzieher. Bei den Gerichten und beim Rechnungshof überwacht die bzw. der Hamburgische Datenschutzbeauftragte darüber hinaus, ob die erforderlichen technischen und organisatorischen Maßnahmen getroffen und eingehalten werden.

(2) Die bzw. der Hamburgische Datenschutzbeauftragte kann Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere soll sie bzw. er den Senat und die übrigen in [§ 2](#) Absatz 1 Satz 1 genannten Stellen in Fragen des Datenschutzes beraten.

(3) Auf Anforderung des Senats oder auf Verlangen eines Viertels der Abgeordneten der Bürgerschaft hat die bzw. der Hamburgische Datenschutzbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Außerdem erstattet sie bzw. er Senat und Bürgerschaft mindestens alle zwei Jahre einen Tätigkeitsbericht. Sie bzw. er kann sich jederzeit an die Bürgerschaft wenden. Schriftliche Äußerungen gegenüber der Bürgerschaft sind gleichzeitig dem Senat vorzulegen. Auf Ersuchen des Senats geht die bzw. der Hamburgische Datenschutzbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge nach, die ihren bzw. seinen Aufgabenbereich unmittelbar betreffen.

(4) Die bzw. der Hamburgische Datenschutzbeauftragte soll zu den Auswirkungen der Nutzung neuer Informations- und Kommunikationstechniken auf den Datenschutz Stellung nehmen. Sie bzw. er ist über Planungen neuer Anwendungen zur Nutzung der Informations- und Kommunikationstechnik rechtzeitig zu unterrichten, sofern dabei personenbezogene Daten verarbeitet werden sollen.

(5) Die in Absatz 1 Satz 1 genannten Stellen sind verpflichtet, die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten und ihre bzw. seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie die Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme,
2. jederzeit Zutritt zu allen Diensträumen zu gewähren.

Gesetzliche Geheimhaltungsvorschriften können einem Auskunfts- oder Einsichtsverlangen nicht entgegengehalten werden.

(6) Absatz 5 Sätze 1 und 2 gilt für das Landesamt für Verfassungsschutz, die Behörden der Staatsanwaltschaft und der Polizei sowie gegenüber Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, mit der Maßgabe, dass die Unterstützung nur der bzw. dem Hamburgischen Datenschutzbeauftragten selbst und den von ihr bzw. ihm schriftlich damit betrauten Beauftragten zu gewähren ist. Absatz 5 Satz 2 gilt für die genannten Behörden nicht, soweit der Senat im Einzelfall feststellt, dass die Einsicht in Akten die Sicherheit des Bundes oder eines Landes gefährdet.

(7) Der Senat kann der bzw. dem Hamburgischen Datenschutzbeauftragten die Aufgaben der Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung übertragen. Auch über diesen Tätigkeitsbereich ist ein Bericht nach Absatz 3 Satz 2 zu erstatten.

## **§ 24**

*(aufgehoben)*

## **§ 25**

### **Beanstandungen**

(1) Stellt die bzw. der Hamburgische Datenschutzbeauftragte Verstöße gegen dieses Gesetz oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Datenverarbeitung fest, so beanstandet sie bzw. er dies

1. im Bereich der Verwaltung und der Gerichte der Freien und Hansestadt Hamburg gegenüber dem für die Behörde oder das Gericht verantwortlichen Senatsmitglied, im Bereich der Bezirksverwaltung gegenüber dem für die Aufsichtsbehörde verantwortlichen Senatsmitglied,
2. im Bereich der der Aufsicht der Freien und Hansestadt Hamburg unterstehenden juristischen Personen des öffentlichen Rechts und deren öffentlich-rechtlich organisierten Einrichtungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ,
3. im Bereich der Bürgerschaft und des Rechnungshofs gegenüber der jeweiligen Präsidentin bzw. dem jeweiligen Präsidenten

und fordert zur Behebung der Mängel und zur Stellungnahme innerhalb einer von ihr bzw. ihm zu bestimmenden Frist auf. Werden die Mängel

nicht fristgemäß behoben, richtet die bzw. der Hamburgische Datenschutzbeauftragte eine weitere Beanstandung in den Fällen des Satzes 1 Nummer 1 an den Senat, in den Fällen des Satzes 1 Nummer 2 an die zuständige Aufsichtsbehörde; im übrigen gilt Satz 1 entsprechend.

(2) Die bzw. der Hamburgische Datenschutzbeauftragte kann von einer Beanstandung absehen, insbesondere wenn die Mängel von geringer Bedeutung sind, bereits behoben sind oder ihre Behebung sichergestellt ist.

(3) Mit der Beanstandung kann die bzw. der Hamburgische Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Absatz 1 abzugebenden Stellungnahmen sollen auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung getroffen worden sind. Die in Absatz 1 Satz 1 Nummer 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme zu.

## **§ 26 Anrufung**

(1) Jede Person kann sich an die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten im Überwachungsbereich nach [§ 23](#) Absatz 1 in ihren Rechten verletzt worden zu sein.

(2) Niemand darf wegen der Mitteilung von Tatsachen, die geeignet sind, den Verdacht aufkommen zu lassen, das Hamburgische Daten-

schutzgesetz oder eine andere Rechtsvorschrift über den Datenschutz sei verletzt worden, gemäßregelt oder benachteiligt werden. Bedienstete der Freien und Hansestadt Hamburg sind nicht verpflichtet, der bzw. dem Hamburgischen Datenschutzbeauftragten gegenüber den Dienstweg einzuhalten.

## FÜNFTER ABSCHNITT

### Besondere Vorschriften über den Datenschutz

#### § 27

#### **Datenverarbeitung zum Zwecke wissenschaftlicher Forschung**

(1) Die in [§ 2](#) Absatz 1 Satz 1 genannten Stellen dürfen personenbezogene Daten ohne Einwilligung der Betroffenen für ein bestimmtes Forschungsvorhaben verarbeiten, soweit deren schutzwürdige Interessen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Der Einwilligung des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Interessen der Durchführung des Forschungsvorhabens die schutzwürdigen Interessen des Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(2) Über die Übermittlung entscheidet die Leiterin bzw. der Leiter der übermittelnden Stelle oder die von ihr bzw. ihm bestimmte Mitarbeiterin oder ein entsprechender Mitarbeiter. Die Entscheidung muss die Stelle, der die Daten übermittelt werden, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen; sie ist der bzw. dem Hamburgischen Datenschutzbeauftragten mitzuteilen.

(3) Die Daten sind, sobald der Forschungszweck es gestattet, zu anonymisieren. Die Merkmale, mit denen ein Bezug auf eine bestimmte natürliche Person wiederhergestellt werden kann, sind gesondert zu speichern; sie sind zu löschen, sobald der Forschungszweck dies gestattet.

(4) Die übermittelten personenbezogenen Daten dürfen nur mit Einwilligung der Betroffenen weiter übermittelt oder für einen anderen als den ursprünglichen Zweck verarbeitet werden.

(5) Die wissenschaftliche Forschung betreibenden in [§ 2](#) Absatz 1 Satz 1 genannten Stellen dürfen personenbezogene Daten ohne Einwilligung der Betroffenen nur veröffentlichen, wenn dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(6) Soweit die Vorschriften dieses Gesetzes auf die Stelle, der die Daten übermittelt werden sollen, keine Anwendung finden, dürfen sie ihr nur übermittelt werden, wenn sie sich verpflichtet, die Vorschriften der Absätze 3 bis 5 einzuhalten, und sich der Überwachung der bzw. des für den Ort der Forschungsstätte zu-ständigen Datenschutzbeauftragten unterwirft. Befindet sich der Ort der Forschungsstätte außerhalb der Europäischen Union, ist eine Übermittlung nur zulässig, wenn kein Grund zu der Annahme besteht, dass bei der Durchführung des Forschungsvorhabens gegen Inhalt und Zweck eines deutschen Gesetzes verstoßen wird.

(7) Die Absätze 1, 3 und 4 gelten entsprechend bei der Datenverarbeitung zur Vorbereitung oder Überprüfung von Regelungen allgemeiner Art durch eine in [§ 2](#) Absatz 1 Satz 1 genannte Stelle.

## **§ 28**

### **Datenverarbeitung bei Beschäftigungsverhältnissen**

(1) Die in [§ 2](#) Absatz 1 Satz 1 genannten Stellen dürfen personenbezogene Daten 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 die nachfolgenden Absätze.

(2) Die in [§ 2](#) Absatz 1 Satz 1 genannten Stellen dürfen, soweit die nachfolgenden Absätze keine besonderen Regelungen enthalten, personenbezogene Daten 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) Die §§ 96 bis 96h des Hamburgischen Beamtengesetzes (HmbBG) in der Fassung vom 29. November 1977 (HmbGVBl. S. 367), zuletzt geändert am 27. April 2000 (HmbGVBl. S. 85), sind in der jeweils geltenden Fassung 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 abweichend von [§ 16](#) Absatz 1 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 § 96e HmbBG bleibt unberührt.

(5) Verlangt eine in [§ 2](#) Absatz 1 Satz 1 genannte 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

(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. [§ 19](#) Absatz 4 findet Anwendung.

(7) Soweit Daten der Beschäftigten im Rahmen der technischen und organisatorischen Maßnahmen nach § 8 Absatz 2 gespeichert werden,

dürfen sie nicht zu anderen Zwecken, insbesondere nicht zu Zwecken der Verhaltens- oder Leistungskontrolle, genutzt werden.

(8) [§ 27](#) findet Anwendung.

## § 29

### Fernmessen und Fernwirken

(1) In [§ 2](#) Absatz 1 Satz 1 genannte Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) in Wohn- oder Geschäftsräumen Privater nur vornehmen, wenn die Betroffenen zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden sind und nach der Unterrichtung schriftlich eingewilligt haben. Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohn- oder Geschäftsräumen Privat

(2) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, dass die Betroffenen nach Absatz 1 Satz 1 oder Satz 2 einwilligen. Verweigern oder widerrufen sie ihre Einwilligung, so dürfen ihnen keine Nachteile entstehen, die über die nachweisbaren Mehrkosten einer anderen Art der Datenerhebung hinausgehen.

(3) Soweit im Rahmen von Fernmess- und Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

(4) Die Absätze 1 und 2 gelten nicht für Fernmess- und Fernwirkdienste der Versorgungsunternehmen und für entsprechende Dienste von

Wohnungsunternehmen.

### **§ 30**

#### **Datenverarbeitung für Planungszwecke**

(1) Für Zwecke der öffentlichen Planung können personenbezogene Daten verarbeitet werden, wenn der Planungszweck auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann und das öffentliche Interesse an der Planung die schutzwürdigen Interessen der Betroffenen erheblich überwiegt.

(2) Die zu Planungszwecken gespeicherten personenbezogenen Daten dürfen nicht für andere Zwecke genutzt werden. Sobald es der Zweck der Planungsaufgabe erlaubt, sind die zu diesem Zweck verarbeiteten personenbezogenen Daten zu anonymisieren. Eine Übermittlung von Daten, aus denen Rückschlüsse auf Einzelpersonen gezogen werden können, ist unzulässig.

(3) Soweit Daten für längere Zeit gespeichert werden, ist durch geeignete Maßnahmen sicherzustellen, dass sie innerhalb der Daten verarbeitenden Stelle getrennt von der Erfüllung anderer Verwaltungsaufgaben verarbeitet werden.

### **§ 31**

*(aufgehoben)*

## SECHSTER ABSCHNITT Straf- und Bußgeldvorschriften; Gebührenvorschrift; Inkrafttreten

### § 32 Straftaten

(1) 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,

1. unbefugt erhebt, speichert, löscht, sperrt, verändert, übermittelt oder nutzt oder
2. durch Vortäuschung falscher Tatsachen an sich oder eine andere bzw. einen anderen übermitteln lässt,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Die Tat wird nur auf Antrag verfolgt.

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

### § 33 Ordnungswidrigkeiten

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

1. unbefugt erhebt, speichert, löscht, sperrt, verändert, übermittelt oder nutzt oder

2. durch Vortäuschung falscher Tatsachen an sich oder eine andere bzw. einen anderen übermitteln lässt.

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

### **§ 34**

#### **Verwaltungsgebühren**

(1) Für Amtshandlungen, die der Kontrolle nicht-öffentlicher Stellen durch die Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes dienen, werden Gebühren, Zinsen und Auslagen erhoben. Der Senat wird ermächtigt, die gebührenpflichtigen Tatbestände und die Gebührensätze 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. Werden, im Fall des Satzes 2 keine Mängel festgestellt, sind die Gebühren, Zinsen und Auslagen von denjenigen zu tragen, die die Kontrolle veranlasst haben, soweit dies der Billigkeit entspricht.

*§ 35 Inkrafttreten  
(nicht aufgenommen)*

