HAMBURGISCHES GESETZ- UND VERORDNUNGSBLATT

TEIL I

HmbGVBl. Nr. 51 MONTAG, DEN 23. DEZEMBER 2019

Gesetz über die Datenverarbeitung der Polizei und zur Änderung weiterer polizeirechtlicher Vorschriften

Vom 12. Dezember 2019

Der Senat verkündet das nachstehende von der Bürgerschaft beschlossene Gesetz:

Artikel 1

Gesetz über die Datenverarbeitung der Polizei (PolDVG)

Inhaltsverzeichnis

Abschnitt 1

Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze

§ 1

Anwendungsbereich

(1) Dieses Gesetz findet Anwendung, soweit die Vollzugspolizei (Polizei) zur Erfüllung ihrer Aufgaben Daten zur Gefahrenabwehr verarbeitet. Zu den in Satz 1 genannten Aufgaben gehört auch die Erhebung und weitere Verarbeitung von Daten

1. zur Verhütung von Straftaten und zur Vorsorge für die Verfolgung künftiger Straftaten (vorbeugende Bekämpfung von Straftaten) und
2. zur Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen.

(2) Mit diesem Gesetz werden auch Regelungen zur Umsetzung 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 Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr getroffen.

(3) Im Anwendungsbereich 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 2016 Nr. L 119 S. 1, Nr. L 314 S. 72, 2018 Nr. L 127 S. 2) stellen insbesondere die Befugnisse in Abschnitt 2 dieses Gesetzes und § 51 zugleich spezifische Bestimmungen im Sinne von Artikel 6 Absätze 2 und 3 sowie Artikel 10 der Verordnung (EU) 2016/679 dar. § 4 dieses Gesetzes stellt im Anwendungsbereich der Verordnung (EU) 2016/679 eine spezifische Regelung im Sinne von Artikel 9 Absätze 2 und 4 der Verordnung (EU) 2016/679 dar. Im Übrigen gilt die Verordnung (EU) 2016/679 sowie das Hamburgische Datenschutzgesetz vom 18. Mai 2018 (HmbGVBl. S. 145) in der jeweils geltenden Fassung unmittelbar.

§ 2

Begriffsbestimmungen

(1) Polizei im Sinne dieses Gesetzes sind die für vollzugspolizeiliche Aufgaben, insbesondere die für unaufschiebbare Maßnahmen in allen Fällen der Gefahrenabwehr (§ 3 Absatz 2 Satz 1 Buchstabe a des Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung – SOG – vom 14. März 1966 (HmbGVBl. S. 77), zuletzt geändert am 12. Dezember 2019 (HmbGVBl. S. 485, 513), in der jeweils geltenden Fassung) und die Verfolgung von Straftaten und Ordnungswidrigkeiten zuständigen Organisationseinheiten innerhalb der zuständigen Behörde.

(2) Straftaten von erheblicher Bedeutung sind

1. Verbrechen,
2. Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie
   a) sich gegen Leib, Leben oder Freiheit einer Person oder bedeutende Sach- oder Vermögenswerte richten,
   b) auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- oder Wertzeichenfälschung, der Vorteilsannahme oder -gewährung, der Bestechlichkeit oder Bestechung (§§ 331 bis 335 des Strafgesetzbuches) oder des Staatsschutzes (§§ 74a und 120 des Gerichtsverfassungsgesetzes) begangen werden oder,
   c) gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangen werden.

(3) Abwehr einer Gefahr im Sinne dieses Gesetzes ist auch die Beseitigung einer Störung der öffentlichen Sicherheit oder Ordnung.

(4) Kontakt- oder Begleitpersonen im Sinne dieses Gesetzes sind Personen, die mit einer Person, von der tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass diese Person Straftaten begehen wird, in einer Weise in Verbindung stehen, die die Erhebung ihrer personenbezogenen Daten zur vorbeugenden Bekämpfung dieser Straftaten erfordert. Vorausgesetzt sind konkrete Tatsachen für einen objektiven Tatbezug und damit für eine Einbeziehung in den Handlungskomplex der Straftatbegehung, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der Straftaten.

(5) Organisierte Kriminalität im Sinne dieses Gesetzes ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten nach Absatz 2, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig

1. unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,
2. unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder
3. unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft

zusammenwirken.

(6) Ein Schengen-assoziierter Staat im Sinne dieses Gesetzes ist ein Staat, der die Bestimmungen des Schengen-Besitzstandes auf Grund eines Assoziierungsabkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwendet.

(7) „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann.

(8) „Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(9) „Einschränkung der Verarbeitung“ meint die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

(10) „Profiling“ ist jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der

Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

(11) „Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können.

(12) „Anonymisierung“ 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 bestimmbaren natürlichen Person zugeordnet werden können.

(13) „Dateisystem“ ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

(14) „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(15) „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(16) „Empfänger“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Europäischen Recht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

(17) „Verletzung des Schutzes personenbezogener Daten“ ist eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden.

(18) „Genetische Daten“ sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden.

(19) „Biometrische Daten“ sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten.

(20) „Gesundheitsdaten“ sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

(21) „Besondere Kategorien personenbezogener Daten“ sind

a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

b) genetische Daten,

c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

d) Gesundheitsdaten und

e) Daten zum Sexualleben oder zur sexuellen Orientierung.

(22) „Einwilligung“ ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

§ 3

Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten

1. müssen auf rechtmäßige Weise verarbeitet werden,
2. müssen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3. müssen dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung darf nicht außer Verhältnis zu diesem Zweck stehen,
4. müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,
5. dürfen nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,
6. müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

§ 4

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist zulässig, wenn dies

1. zur Erfüllung polizeilicher Aufgaben oder
2. zu Zwecken der Eigensicherung,

unbedingt erforderlich ist.

(2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorzusehen. Geeignete Garantien können insbesondere sein

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,

2. die Festlegung von besonderen Aussonderungsprüffristen,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle,
5. die von anderen Daten getrennte Verarbeitung,
6. die Pseudonymisierung personenbezogener Daten,
7. die Verschlüsselung personenbezogener Daten oder
8. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

§ 5

Einwilligung

(1) Eine Einwilligung in die Verarbeitung personenbezogener Daten ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

(2) Soweit die Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung erfolgt, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(3) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

(4) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der auf Grund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

§ 6

Datengeheimnis

Denjenigen Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu verarbeiten. Dieses Verbot besteht auch nach Beendigung der Tätigkeit fort.

§ 7

Verarbeitungen auf Weisung des Verantwortlichen

Der Auftragsverarbeiter und jede einem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet sind.

§ 8

Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

Bei der Verarbeitung personenbezogener Daten ist so weit wie möglich danach zu unterscheiden, ob diese auf Tatsachen oder auf persönlichen Einschätzungen beruhen.

§ 9

Automatisierte Einzelentscheidungen

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist, die geeignete Garantien für die Rechtsgüter der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen.

(2) Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

(3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

Abschnitt 2

Unterabschnitt 1

Allgemeine Befugnisse zur Datenverarbeitung

§ 10

Grundsätze der Datenverarbeitung

(1) Die Polizei darf personenbezogene Daten nur verarbeiten, soweit dies durch dieses Gesetz zugelassen ist. Anderweitige besondere Rechtsvorschriften über die Datenverarbeitung bleiben unberührt.

(2) Personenbezogene Daten sollen bei der betroffenen Person oder öffentlichen Stellen erhoben werden. Ohne deren Kenntnis dürfen sie bei anderen nichtöffentlichen Stellen erhoben werden, wenn die Erhebung bei der betroffenen Personen oder bei öffentlichen Stellen

1. nicht oder nicht rechtzeitig möglich ist,
2. nur mit unverhältnismäßig hohem Aufwand möglich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person beeinträchtigt werden, oder
3. die Erfüllung der Aufgaben gefährden würde.

(3) Personenbezogene Daten sollen offen erhoben werden. Eine Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar ist, ist zulässig, wenn durch anderes Handeln die Erfüllung einer bestimmten polizeilichen Aufgabe erheblich erschwert oder gefährdet würde und die Maßnahme nicht gezielt verdeckt wird. Eine Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar sein soll (verdeckte Datenerhebung), ist außer in den in diesem Gesetz ausdrücklich zugelassenen Fällen nur zulässig, wenn die Erfüllung einer bestimmten polizeilichen Aufgabe bei anderem Handeln aussichtslos wäre oder wenn dies den überwiegenden Interessen der betroffenen Person entspricht.

(4) Werden personenbezogene Daten bei der betroffenen Person oder bei Dritten erhoben, sind diese in geeigneter Weise hinzuweisen auf

1. die Rechtsgrundlage der Datenerhebung,
2. eine im Einzelfall bestehende Auskunftspflicht oder die Freiwilligkeit der Auskunft und
3. die beabsichtigte Verwendung der Daten.

Dieser Hinweis kann unterbleiben, wenn er wegen der besonderen Umstände offenkundig nicht erforderlich ist oder wenn hierdurch die Erfüllung der polizeilichen Aufgabe oder die schutzwürdigen Belange Dritter beeinträchtigt oder gefährdet würden.

§ 11

Voraussetzungen der Datenverarbeitung

(1) Die Polizei darf personenbezogene Daten verarbeiten,

1. soweit es im Einzelfall erforderlich ist zur Abwehr einer bevorstehenden Gefahr, zur Wahrnehmung grenzpolizeilicher Aufgaben oder in Erfüllung einer Verpflichtung zur Amts- oder Vollzugshilfe,
2. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können und dies zur Erfüllung ihrer Aufgaben erforderlich ist,
3. wenn dies zur Vorbereitung und Durchführung eines Einsatzes erforderlich ist, bei dem erfahrungsgemäß eine besondere Gefährdungslage besteht,
4. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person Opfer einer Straftat werden wird, und dies zur Wahrnehmung der Schutzaufgabe erforderlich ist,
5. wenn die Person sich im räumlichen Umfeld einer Person aufhält, die auf Grund ihrer beruflichen Tätigkeit oder ihrer Stellung in der Öffentlichkeit besonders gefährdet erscheint, und dies zum Schutz der gefährdeten Person erforderlich ist,
6. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird, und die Erhebung zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist,
7. über Kontakt- oder Begleitpersonen, wenn dies zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist.

(2) Die Polizei darf personenbezogene Daten verarbeiten, wenn die Person in Kenntnis des Zwecks der Erhebung in diese nach § 5 eingewilligt hat.

§ 12

Befragung und Auskunftspflicht

(1) Die Polizei darf jede Person befragen, wenn auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie sachdienliche Angaben machen kann, die für die Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich sind. Für die Dauer der Befragung dürfen diese Personen angehalten werden.

(2) Eine Person, deren Befragung nach Absatz 1 zulässig ist, ist verpflichtet, auf Frage ihren Namen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Staatsangehörigkeit anzugeben. Sie ist zu weiteren Auskünften nur verpflichtet, soweit gesetzliche Handlungspflichten bestehen oder Tatsachen die Annahme rechtfertigen, dass sie sachdienliche Angaben zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte machen kann. Eingriffe in das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) sind nur unter den Voraussetzungen der §§ 21 bis 26 zulässig.

(3) §§ 52 bis 55 und 136a der Strafprozessordnung gelten entsprechend.

§ 13

Identitätsfeststellung und Prüfung von Berechtigungsscheinen

(1) Die Polizei darf die Identität einer Person feststellen,

1. soweit es im Einzelfall erforderlich ist zur Abwehr einer bevorstehenden Gefahr oder in Erfüllung einer Verpflichtung zur Amts- oder Vollzugshilfe,
2. wenn sie an einem Ort angetroffen wird, von dem Tatsachen die Annahme rechtfertigen, dass dort
   a) Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben,
   b) Personen angetroffen werden, die gegen aufenthaltsrechtliche Straf- oder Ordnungswidrigkeitenvorschriften verstoßen,
   c) sich gesuchte Straftäter verbergen,
3. wenn sie in einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel, Amtsgebäude oder einem besonders gefährdeten Objekt oder in dessen unmittelbarer Nähe angetroffen wird und Tatsachen die Annahme rechtfertigen, dass in diesem Objekt oder in dessen unmittelbarer Nähe Straftaten begangen werden sollen, durch die Personen oder das Objekt gefährdet sind,
4. an einer Kontrollstelle, die von der Polizei eingerichtet worden ist, um eine Straftat nach § 129a des Strafgesetzbuchs, auch in Verbindung mit § 129b Absatz 1 des Strafgesetzbuchs, eine der in dieser Vorschrift bezeichneten Straftaten oder eine Straftat nach § 250 Absatz 1 oder nach § 255 des Strafgesetzbuchs in den vorgenannten Begehungsformen oder nach § 27 Absatz 1 und Absatz 2 Nummer 3 Buchstabe a des Versammlungsgesetzes in der Fassung vom 15. November 1978 (BGBl. I S. 1790), zuletzt geändert am 8. Dezember 2008 (BGBl. I S. 2366), in der jeweils geltenden Fassung zu verhüten, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass solche Straftaten begangen werden sollen.

(2) Die Polizei darf an einem Ort, für den durch Rechtsverordnung nach § 42 des Waffengesetzes vom 11. Oktober 2002 (BGBl. 2002 I S. 3970, 4592, 2003 I S. 1957), zuletzt geändert am 30. Juni 2017 (BGBl. I S. 2133), in der jeweils geltenden Fassung und nach § 1 SOG das Führen von Waffen im Sinne des § 1 Absatz 2 des Waffengesetzes und gefährlichen Gegenständen verboten oder beschränkt worden ist, Personen kurzfristig anhalten, befragen, ihre Identität feststellen und sie sowie die von ihnen mitgeführten Sachen durchsuchen, soweit auf Grund von konkreten Lageerkenntnissen anzunehmen ist, dass diese Personen verbotene Waffen oder gefährliche Gegenstände mit sich führen. Die Durchsuchungsbefugnisse aus Satz 1 treten mit Ablauf des 30. Juni 2021 außer Kraft.

(3) Zur Feststellung der Identität dürfen Namen, frühere Namen, Vornamen, Geburtsdatum, Geburtsort, Geschlecht, Staatsangehörigkeit und Anschrift erhoben werden.

(4) Zur Feststellung der Identität darf die Polizei die erforderlichen Maßnahmen treffen. Sie darf

1. die betroffene Person anhalten,
2. die betroffene Person oder Auskunftspersonen nach seiner oder ihrer Identität befragen,
3. verlangen, dass die betroffene Person mitgeführte Ausweispapiere zur Prüfung aushändigt,
4. die betroffene Person festhalten,
5. die betroffene Person und die von ihr mitgeführten Sachen nach Gegenständen durchsuchen, die zur Identitätsfeststellung dienen können,

6. die betroffene Person zur Dienststelle bringen,
7. in den Fällen des Absatzes 1 unter den Voraussetzungen des § 16 erkennungsdienstliche Maßnahmen durchführen.

Maßnahmen nach Satz 2 Nummern 4 bis 6 dürfen nur getroffen werden, wenn die Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann oder wenn tatsächliche Anhaltspunkte dafür bestehen, dass Angaben unrichtig sind.

(5) Die Polizei darf verlangen, dass ein Berechtigungsschein zur Prüfung ausgehändigt wird, wenn der Betroffene auf Grund einer Rechtsvorschrift oder einer vollziehbaren Auflage in einem Erlaubnisbescheid verpflichtet ist, diesen Berechtigungsschein mitzuführen.

§ 14

Datenverarbeitung zur Vorbereitung auf die Hilfeleistung in Gefahrenfällen

(1) Die Polizei darf über

1. Personen, deren besondere Kenntnisse oder Fähigkeiten zur Gefahrenabwehr benötigt werden,
2. Verantwortliche für Anlagen oder Einrichtungen, von denen eine erhebliche Gefahr ausgehen kann,
3. Verantwortliche für gefährdete Anlagen oder Einrichtungen,
4. Verantwortliche für Veranstaltungen in der Öffentlichkeit

Namen, Vornamen, akademische Grade, Anschriften, Telefonnummern und andere Informationen über die Erreichbarkeit sowie nähere Angaben über die Zugehörigkeit zu einer der genannten Personengruppen verarbeiten, soweit dies zur Vorbereitung auf die Hilfeleistung in Gefahrenfällen erforderlich ist. Eine verdeckte Datenerhebung ist unzulässig.

(2) Die nach Absatz 1 Satz 1 Nummer 4 erhobenen personenbezogenen Daten, die in Dateien suchfähig gespeichert wurden, und Akten, die zur Person des Verantwortlichen angelegt wurden, sind spätestens einen Monat nach Beendigung des Anlasses zu löschen oder zu vernichten, sofern es sich nicht um regelmäßig wiederkehrende Veranstaltungen handelt.

§ 15

Datenverarbeitung bei Notrufen, Aufzeichnung von Anrufen und Funkverkehr

Die Polizei kann Anrufe über Notrufeinrichtungen sowie den Funkverkehr ihrer Leitstelle aufzeichnen. Im Übrigen ist eine Aufzeichnung von Anrufen zulässig, soweit sie zur Gefahrenabwehr oder zur Verhütung von Straftaten erforderlich ist. Die Aufzeichnungen sind spätestens sechs Monate nach ihrer Erhebung zu löschen, es sei denn, die Daten werden zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt.

Unterabschnitt 2

Besondere Befugnisse zur Datenverarbeitung

§ 16

Erkennungsdienstliche Maßnahmen und Identifizierung unbekannter Toter durch DNA-Material

(1) Die Polizei darf erkennungsdienstliche Maßnahmen durchführen

1. zum Zweck der Identitätsfeststellung (§ 13 Absatz 4), wenn dies auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist,
2. zur vorbeugenden Bekämpfung von Straftaten, wenn die betroffene Person verdächtig ist, eine mit Strafe bedrohte Tat begangen zu haben, und wegen der Art oder Ausführung der Tat sowie der Persönlichkeit der betroffenen Person die Gefahr der Begehung weiterer Straftaten besteht.

(2) Ist die Identität festgestellt, sind in den Fällen des Absatzes 1 Nummer 1 die im Zusammenhang mit der Feststellung angefallenen Unterlagen zu vernichten, es sei denn, ihre weitere Aufbewahrung ist für Zwecke nach Absatz 1 Nummer 2 oder nach anderen Rechtsvorschriften zulässig.

(3) Erkennungsdienstliche Maßnahmen sind

1. die Abnahme von Finger- und Handflächenabdrücken,
2. die Aufnahme von Lichtbildern,
3. die Feststellung äußerlich wahrnehmbarer Merkmale,
4. Messungen.

Soweit es zur Feststellung der Identität erforderlich ist, darf die Polizei auch Befragungen anderer Personen vornehmen, Urkunden oder sonstige Unterlagen einsehen und das Bundesverwaltungsamt um einen Datenabgleich mit der Fundpapier-Datenbank nach § 89a Absatz 6 Satz 1 Nummer 2 des Aufenthaltsgesetzes in der Fassung vom 25. Februar 2008 (BGBl. I S. 163), zuletzt geändert am 12. Juli 2018 (BGBl. I S. 1147), ersuchen. Regelungen über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt. Erkennungsdienstliche Maßnahmen dürfen nur von besonders ermächtigten Bediensteten angeordnet werden.

(4) Ist eine Identitätsfeststellung unbekannter Toter auf andere Weise nicht möglich, darf die Polizei DNA-Material von vermissten Personen und unbekannten Toten sicherstellen und molekulargenetische Untersuchungen durchführen. Das erlangte DNA-Identifizierungsmuster kann zu diesem Zweck in einem Dateisystem verarbeitet werden. Eine Verarbeitung für andere Zwecke ist nicht zulässig. Nach Beendigung der Maßnahme ist das DNA-Identifizierungsmuster zu vernichten. Molekulargenetische Untersuchungen bedürfen der richterlichen Anordnung. Zuständig ist das Amtsgericht Hamburg. Das Verfahren richtet sich nach dem Buch 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586, 2587), zuletzt geändert am 18. Dezember 2018 (BGBl. I S. 2639, 2646), in der jeweils geltenden Fassung. § 81f Absatz 1 Satz 2 und Absatz 2 der Strafprozessordnung gilt entsprechend. Liegt eine Naturkatastrophe oder ein besonders schwerer Unglücksfall vor, so sind Maßnahmen nach Satz 1 auch dann zulässig, wenn eine Identitätsfeststellung unbekannter Toter oder Schwerstverletzter auf andere Weise nicht möglich oder wesentlich erschwert wäre; einer richterlichen Anordnung bedarf es in diesen Fällen nicht. Sätze 2 bis 4 gelten entsprechend.

§ 17

Aufnahme von Lichtbildern in Gewahrsamseinrichtungen

Die Polizei darf von Personen, die sich in amtlichem Gewahrsam befinden, Lichtbilder verarbeiten, wenn dies zur Aufrechterhaltung der Sicherheit und Ordnung im Gewahrsam oder zur Identitätsfeststellung erforderlich ist. Diese personenbezogenen Daten sind spätestens mit der Entlassung aus dem Gewahrsam zu löschen. § 34 bleibt unberührt.

§ 18

Datenverarbeitung im öffentlichen Raum und an besonders gefährdeten Objekten

(1) Die Polizei darf bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen personenbezo-

gene Daten von Teilnehmern auch durch den Einsatz technischer Mittel zum Zwecke der Bild- und Tonübertragung verarbeiten, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden. Der Einsatz technischer Mittel zum Zwecke der Bild- und Tonaufzeichnung ist nur gegen die für eine Gefahr Verantwortlichen zulässig. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Bild- und Tonaufzeichnungen, sowie in Dateisystemen suchfähig gespeicherte personenbezogene Daten sind spätestens einen Monat nach der Datenerhebung zu löschen oder zu vernichten. Dies gilt nicht, wenn die Daten zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten benötigt werden oder Tatsachen die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird, und die Aufbewahrung zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist.

(2) Die Polizei darf an oder in den in § 13 Absatz 1 Nummer 3 genannten Objekten Bild- und Tonaufzeichnungen über die für eine Gefahr Verantwortlichen anfertigen und verarbeiten, soweit Tatsachen die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder andere darin befindliche Sachen gefährdet sind. Absatz 1 Sätze 3 bis 5 gilt entsprechend. Auf den Einsatz von Aufzeichnungsgeräten ist hinzuweisen, soweit dadurch nicht der Zweck der Maßnahme gefährdet wird.

(3) Die Polizei darf zur vorbeugenden Bekämpfung von Straftaten öffentlich zugängliche Straßen, Wege und Plätze mittels Bildübertragung offen beobachten und Bildaufzeichnungen von Personen verarbeiten, soweit an diesen Orten wiederholt Straftaten der Straßenkriminalität begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung derartiger Straftaten zu rechnen ist. Absatz 1 Sätze 3 bis 5 gilt entsprechend.

(4) Die Polizei darf von Personen, die sich in amtlichem Gewahrsam befinden, durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen längstens bis zum Ende des Tages nach deren Ergreifen Daten verarbeiten, wenn dies zum Schutz der Betroffenen oder der Vollzugsbediensteten oder zur Verhütung von Straftaten in polizeilich genutzten Räumen erforderlich ist. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Eingriffe in ein durch Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinne der §§ 53 und 53a der Strafprozessordnung sind unzulässig. Bild- und Tonaufzeichnungen sind spätestens nach vier Tagen zu löschen, soweit sie nicht für Zwecke der Strafverfolgung benötigt werden.

(5) Die Polizei darf bei der Durchführung von Maßnahmen zur Gefahrenabwehr oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten in öffentlich zugänglichen Bereichen personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen verarbeiten, wenn dies nach den Umständen zum Schutz von Vollzugsbediensteten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Aufzeichnungen sind unzulässig in Bereichen, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgern nach § 53 Absatz 1 der Strafprozessordnung dienen. Absatz 4 Sätze 2 und 4 gilt entsprechend.

(6) § 37 und § 59 Absatz 4 bleiben unberührt.

§ 19

Datenverarbeitung durch den Einsatz von automatischen Kennzeichenlesesystemen

(1) Bei Kontrollen im öffentlichen Verkehrsraum nach diesem Gesetz und anderen Gesetzen darf die Polizei zur Eigensicherung, zur Verhinderung des Gebrauchs gestohlener Kraftfahrzeuge und Kraftfahrzeugkennzeichen und zur Verhütung von Anschlussstraftaten automatisiert Kennzeichen von Kraftfahrzeugen erfassen, soweit jeweils eine Anhaltemöglichkeit besteht und die Erhebung offen erfolgt. Die Kennzeichenerfassung darf nicht flächendeckend eingesetzt werden.

(2) Die erfassten Kennzeichen dürfen mit dem Fahndungsbestand der Sachfahndungsdateien des beim Bundeskriminalamt nach den Vorschriften des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl. 2017 I S. 1354, 2019 I S. 400) in der jeweils geltenden Fassung und des beim Landeskriminalamt Hamburg nach den Vorschriften dieses Gesetzes geführten polizeilichen Informationssystems abgeglichen werden. Der Abgleich nach Satz 1 beschränkt sich auf Kennzeichen von Fahrzeugen, die

1. nach § 31 dieses Gesetzes, §§ 163e und 463a der Strafprozessordnung, Artikel 36 und 37 des Beschlusses 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (ABl. EU Nr. L 205 S. 63), zuletzt geändert am 7. Dezember 2018 (ABl. EU Nr. L 312 S. 56), § 17 Absatz 3 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert am 30. Juni 2017 (BGBl. I S. 2097, 2128), und § 47 des Bundeskriminalamtgesetzes,
2. auf Grund einer Gefahr für Zwecke der Gefahrenabwehr,
3. auf Grund des Verdachts einer Straftat für Zwecke der Strafverfolgung,
4. aus Gründen der Strafvollstreckung

ausgeschrieben sind. Der Abgleich darf nur mit vollständigen Kennzeichen des Fahndungsbestands erfolgen. Bewegungsprofile dürfen nicht erstellt werden.

(3) Sofern das ermittelte Kennzeichen nicht im Fahndungsbestand enthalten ist (Nichttrefferfall), sind die erhobenen Daten unverzüglich nach Durchführung des Datenabgleichs automatisiert zu löschen. Ist das ermittelte Kennzeichen im Fahndungsbestand enthalten (Trefferfall), dürfen das Kennzeichen sowie Angaben zu Ort, Datum, Uhrzeit und Fahrtrichtung gespeichert werden. Das Fahrzeug und die Insassen sollen im Trefferfall angehalten werden. Weitere Maßnahmen dürfen erst nach Überprüfung des Trefferfalls anhand des aktuellen Fahndungsdatenbestands erfolgen. Die nach Satz 2 gespeicherten Daten dürfen weiterverarbeitet werden, soweit dies für Zwecke der Gefahrenabwehr erforderlich ist.

§ 20

Datenverarbeitung durch Observation

(1) Die Polizei darf personenbezogene Daten verarbeiten durch eine planmäßig angelegte Beobachtung, die innerhalb einer Woche länger als 24 Stunden oder über den Zeitraum einer Woche hinaus vorgesehen ist oder tatsächlich durchgeführt wird (längerfristige Observation),

1. über die für eine Gefahr Verantwortlichen und unter den Voraussetzungen von § 10 SOG über die dort genannten Personen, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist,

2. über Personen, soweit Tatsachen, die ein wenigstens seiner Art nach konkretes und zeitlich absehbares Geschehen erkennen lassen, die Annahme rechtfertigen, dass diese Personen Straftaten von erheblicher Bedeutung begehen werden, wenn die Datenerhebung zur Verhütung dieser Straftaten erforderlich ist, sowie über deren Kontakt- oder Begleitpersonen, wenn die Aufklärung des Sachverhaltes auf andere Weise aussichtslos wäre.

Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Verbrechen sowie Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, und sich gegen bedeutende Sach- oder Vermögenswerte richten, sind nur dann als Straftat von erheblicher Bedeutung im Sinne von § 2 Absatz 2 Nummer 2 anzusehen, wenn die Erhaltung der bedeutenden Sach- und Vermögenswerte im öffentlichen Interesse liegt.

(2) Der Einsatz nach Absatz 1 bedarf der richterlichen Anordnung. Bei Gefahr im Verzug kann die Maßnahme durch die Polizeipräsidentin oder den Polizeipräsidenten oder die Vertretung im Amt angeordnet werden; die Anordnung ist aktenkundig zu machen. Eine richterliche Bestätigung ist unverzüglich einzuholen. Die Maßnahme ist zu beenden, wenn sie nicht innerhalb von drei Tagen richterlich bestätigt wird; in diesem Fall sind die erhobenen Daten unverzüglich zu vernichten. Zuständig ist das Amtsgericht Hamburg. Für das Verfahren findet Buch 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend Anwendung. Von einer Anhörung der betroffenen Person durch das Gericht und der Bekanntgabe der richterlichen Entscheidung an die betroffene Person ist abzusehen, wenn die vorherige Anhörung oder die Bekanntgabe der Entscheidung den Zweck der Maßnahme gefährden würde. Die richterliche Entscheidung wird mit ihrer Bekanntgabe an die beantragende Stelle wirksam. Die Anordnung ergeht schriftlich. Sie ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen für die Maßnahme noch vorliegen. Aus der Anordnung müssen sich

1. die Person, gegen sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,
2. Art, Beginn und Ende der Maßnahme,
3. Tatsachen, die den Einsatz der Maßnahme begründen

ergeben.

(3) Personen, gegen die sich Datenerhebungen richteten, sind nach Abschluss der Maßnahme hierüber durch die Polizei zu unterrichten.

(4) Auf eine Observation, die nicht die in Absatz 1 genannten Voraussetzungen erfüllt (kurzfristige Observation), finden die Absätze 1 bis 3 keine Anwendung. Durch eine kurzfristige Observation darf die Polizei Daten nur verarbeiten, soweit dies zum Zwecke der Gefahrenabwehr (§ 1) erforderlich ist und ohne diese Maßnahme die Erfüllung der polizeilichen Aufgabe gefährdet wird.

§ 21

Datenverarbeitung durch den verdeckten Einsatz technischer Mittel

(1) Die Polizei darf personenbezogene Daten verarbeiten durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes

1. über die für eine Gefahr Verantwortlichen und unter den Voraussetzungen von § 10 SOG über die dort genannten Personen, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist,
2. über Personen, soweit Tatsachen, die ein wenigstens seiner Art nach konkretes und zeitlich absehbares Geschehen erkennen lassen, die Annahme rechtfertigen, dass diese Personen Straftaten von erheblicher Bedeutung begehen werden, wenn die Datenerhebung zur Verhütung dieser Straftaten erforderlich ist, sowie über deren Kontakt- und Begleitpersonen, wenn die Aufklärung des Sachverhalts auf andere Weise aussichtslos wäre.

Unter den Voraussetzungen des Satzes 1 darf die Polizei besondere für Observationszwecke bestimmte technische Mittel zur Ermittlung des Aufenthaltsortes des Betroffenen verwenden. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Verbrechen sowie Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, und sich gegen bedeutende Sach- oder Vermögenswerte richten, sind nur dann als Straftat von erheblicher Bedeutung im Sinne von § 2 Absatz 2 Nummer 2 anzusehen, wenn die Erhaltung der bedeutenden Sach- und Vermögenswerte im öffentlichen Interesse liegt.

(2) Das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes nach Absatz 1 Satz 1 bedarf der richterlichen Anordnung; § 20 Absatz 2 gilt entsprechend. Die Anfertigung von Bildaufnahmen und Bildaufzeichnungen nach Absatz 1 Satz 1 sowie Maßnahmen nach Absatz 1 Satz 2 dürfen von der Polizeipräsidentin oder dem Polizeipräsidenten oder der Vertretung im Amt, bei Gefahr im Verzug auch von der Polizeiführerin oder dem Polizeiführer vom Dienst angeordnet werden. Die Anordnung ist aktenkundig zu machen. Aus der Anordnung müssen sich

1. Art, Beginn und Ende der Maßnahme,
2. Tatsachen, die den Einsatz der Maßnahme begründen,
3. Zeitpunkt der Anordnung und Name sowie Dienststellung des Anordnenden

ergeben. Eine Verlängerung der Maßnahme ist zulässig, soweit die Voraussetzungen für die Maßnahme noch vorliegen.

(3) Datenerhebungen sind unzulässig, wenn in ein durch Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinne der §§ 53 und 53a der Strafprozessordnung eingegriffen wird. Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Wird bei einer Maßnahme erkennbar, dass Gespräche geführt werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind das Abhören und die Beobachtung unverzüglich zu unterbrechen. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Automatische Aufzeichnungen nach Satz 3 sind unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. Nach einer Unterbrechung oder einer Aufzeichnung gemäß Satz 3 darf die Erhebung fortgesetzt werden, wenn zu erwarten ist, dass die Gründe, die zur Unterbrechung oder Aufzeichnung geführt haben, nicht mehr vorliegen. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht

mehr erforderlich ist, spätestens jedoch am Ende des zweiten Kalenderjahres, das dem Jahr der Dokumentation folgt.

(4) Einer Anordnung nach Absatz 2 bedarf es nicht, wenn technische Mittel ausschließlich zum Schutz der bei einem Polizeieinsatz tätigen Personen mitgeführt und verwendet werden. Der Einsatz darf nur durch die Leitung des Landeskriminalamtes oder die Vertretung im Amt angeordnet werden. Eine anderweitige Verwertung der erlangten Erkenntnisse ist nur zur Gefahrenabwehr oder zur Strafverfolgung und nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. Aufzeichnungen sind unverzüglich nach Beendigung des Einsatzes zu löschen, es sei denn, sie werden zur Gefahrenabwehr oder Strafverfolgung benötigt.

(5) Personen, gegen die sich Datenerhebungen richteten, sind nach Abschluss der Maßnahme hierüber durch die Polizei zu benachrichtigen.

§ 22

Datenverarbeitung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen

(1) Die Polizei darf personenbezogene Daten verarbeiten durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des gesprochenen Wortes in oder aus Wohnungen über die für eine Gefahr Verantwortlichen, wenn dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist. Die Maßnahme darf sich nur gegen den für die Gefahr Verantwortlichen richten und nur in dessen Wohnungen durchgeführt werden. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der für die Gefahr Verantwortliche sich dort aufhält und
2. die Maßnahme in Wohnungen des für die Gefahr Verantwortlichen allein nicht zur Abwehr der Gefahr führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Datenerhebungen sind unzulässig, wenn in ein durch Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinne der §§ 53 und 53a der Strafprozessordnung eingegriffen wird.

(3) Die Datenerhebung nach Absatz 1 bedarf der richterlichen Anordnung. Die Anordnung ergeht schriftlich. Sie muss insbesondere Namen und Anschrift der betroffenen Person, gegen die sie sich richtet, enthalten und die Wohnung, in oder aus der die Daten erhoben werden sollen, bezeichnen. In ihr sind Art, Umfang und Dauer der Maßnahme zu bestimmen. Sie ist höchstens auf vier Wochen zu befristen. Eine Verlängerung um jeweils nicht mehr als vier Wochen ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen fortbestehen. Bei Gefahr im Verzug kann die Maßnahme durch die Polizeipräsidentin oder den Polizeipräsidenten oder die Vertretung im Amt angeordnet werden. Eine richterliche Bestätigung ist unverzüglich einzuholen. Die Maßnahme ist zu beenden, wenn sie nicht innerhalb von drei Tagen richterlich bestätigt wird; in diesem Fall sind Bild- und Tonaufzeichnungen unverzüglich zu vernichten, sofern die Aufzeichnungen nicht zur Verfolgung von Straftaten benötigt werden. Zuständig ist das Amtsgericht Hamburg. Für das Verfahren findet Buch 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend Anwendung. Von einer Anhörung der betroffenen Person durch das Gericht und der Bekanntgabe der richterlichen Entscheidung an die betroffene Person ist abzusehen, wenn die vorherige Anhörung oder die Bekanntgabe der Entscheidung den Zweck der Maßnahme gefährden würde. Die richterliche Entscheidung wird mit ihrer Bekanntgabe an die beantragende Stelle wirksam.

(4) Die Maßnahme darf nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und zum Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Vorgänge, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Wird bei einer Maßnahme erkennbar, dass Gespräche geführt werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind das Abhören und die Beobachtung unverzüglich zu unterbrechen. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Nach einer Unterbrechung oder einer Aufzeichnung gemäß Satz 2 darf die Erhebung fortgesetzt werden, wenn zu erwarten ist, dass die Gründe, die zur Unterbrechung oder Aufzeichnung geführt haben, nicht mehr vorliegen.

(5) Die durch eine Maßnahme nach Absatz 1 erlangten Aufzeichnungen, sind dem anordnenden Gericht unverzüglich vorzulegen. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt worden sind, dürfen nicht verwertet werden. Sofern die Voraussetzungen der Anordnung nicht mehr vorliegen, ordnet es die Aufhebung der Datenerhebung an. Polizeiliche Maßnahmen nach Absatz 1 Satz 1 können durch das anordnende Gericht jederzeit aufgehoben, geändert oder angeordnet werden. Bei Gefahr im Verzug kann die Polizeipräsidentin oder der Polizeipräsident oder die Vertretung im Amt über die Verwertung der Erkenntnisse entscheiden. Eine richterliche Bestätigung nach Satz 2 ist unverzüglich einzuholen.

(6) Die durch eine Maßnahme nach Absatz 1 erlangten personenbezogenen Daten dürfen nur zu den in Absatz 1 Satz 1 genannten Zwecken verwendet werden. Zu Zwecken der Strafverfolgung dürfen sie verwendet werden, wenn sie auch dafür unter Einsatz derselben Befugnisse hätten erhoben werden dürfen; eine Zweckänderung ist zu dokumentieren. Stellt sich nach Auswertung der Daten heraus, dass diese einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, dürfen sie nicht verwendet werden. Daten, die keinen unmittelbaren Bezug zu den der Anordnung zugrunde liegenden Gefahren haben, dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer anderweitigen unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder zur Strafverfolgung unter der Voraussetzung von Satz 2 erforderlich. Über eine Verwendung der Daten entscheidet das Gericht, das die Maßnahme angeordnet hat; bei Gefahr im Verzug gilt Absatz 3 Sätze 7 bis 9 entsprechend.

(7) Personen, gegen die sich die Datenerhebungen richteten oder die von ihr sonst betroffen wurden, sind nach Abschluss der Maßnahme darüber zu benachrichtigen.

(8) Sind die nach Absatz 1 erlangten Daten nicht mehr zur Aufgabenerfüllung erforderlich, sind sie zu löschen. Die Löschung ist zu protokollieren. Die Löschung unterbleibt, soweit die Daten für eine Mitteilung an den Betroffenen nach Absatz 7 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme nach Absatz 1 von Bedeutung sein können. In diesem Fall ist die Verarbeitung der Daten einzuschränken und sie dürfen nur zu diesen Zwecken verarbeitet werden. Im Fall der Unterrichtung der betroffenen Person sind die Daten zu löschen, wenn diese nach Ablauf eines

Monats nach seiner Benachrichtigung keine Klage erhebt; auf diese Frist ist in der Benachrichtigung hinzuweisen. Daten, die dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, sind unverzüglich zu löschen; § 21 Absatz 3 Sätze 9 bis 11 gilt entsprechend. Daten, die keinen unmittelbaren Bezug zu den der Anordnung zugrunde liegenden Gefahren haben, sind unverzüglich zu löschen, es sei denn, ihre Verwendung ist zur Abwehr einer anderweitigen unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder zur Strafverfolgung im Sinne von Absatz 6 Satz 2 erforderlich.

(9) Einer Anordnung nach Absatz 3 bedarf es nicht, wenn technische Mittel ausschließlich zum Schutz der bei einem Polizeieinsatz tätigen Personen mitgeführt und verwendet werden. Der Einsatz darf nur durch die Leitung des Landeskriminalamtes oder die Polizeiführerin oder den Polizeiführer vom Dienst angeordnet werden. Eine anderweitige Verwertung der erlangten Erkenntnisse ist nur zur Gefahrenabwehr oder zur Strafverfolgung und nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. Aufzeichnungen sind unverzüglich nach Beendigung des Einsatzes zu löschen, es sei denn, sie werden zur Gefahrenabwehr oder Strafverfolgung benötigt.

§ 23
Datenverarbeitung durch Telekommunikationsüberwachung und Eingriff in die Telekommunikation

(1) Die Polizei darf durch die Überwachung und Aufzeichnung von Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes abgelegten Inhalte Daten erheben

1. über die für eine Gefahr Verantwortlichen, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist,
2. über Personen, soweit Tatsachen die Annahme rechtfertigen, dass
   a) sie für Personen nach Nummer 1 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder weitergeben oder
   b) die unter Nummer 1 genannten Personen ihre Kommunikationseinrichtungen benutzen werden.

Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die polizeiliche Aufgabenerfüllung auf andere Weise aussichtslos oder wesentlich erschwert wäre. § 21 Absatz 3 Sätze 1 bis 6 gilt entsprechend.

(2) Durch den Einsatz technischer Mittel dürfen unter den Voraussetzungen des Absatzes 1 Kommunikationsverbindungen unterbrochen oder verhindert werden. Kommunikationsverbindungen Dritter dürfen nur unterbrochen oder verhindert werden, wenn dies zur Abwehr einer unmittelbar bevorstehenden erheblichen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist.

(3) Auf Grund der Anordnung einer Datenerhebung nach Absatz 1 oder einer Maßnahme nach Absatz 2 hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert am 29. November 2018 (BGBl. I S. 2230), in der jeweils geltenden Fassung und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen der Polizei die Überwachung, Aufzeichnung, Unterbrechung und Verhinderung von Telekommunikationsverbindungen zu ermöglichen.

§ 24
Telekommunikationsüberwachung an informationstechnischen Systemen

(1) Zur Durchführung einer Maßnahme nach § 23 Absatz 1 darf durch den verdeckten Einsatz technischer Mittel in die vom Betroffenen genutzten informationstechnischen Systeme eingegriffen werden, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung von Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(3) Die Maßnahme darf sich nur gegen die für eine Gefahr Verantwortlichen richten. Sie darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

§ 25
Verkehrsdatenverarbeitung, Nutzungsdatenverarbeitung und Einsatz besonderer technischer Mittel zur Datenerhebung

(1) Die Polizei darf unter den Voraussetzungen des § 23 Absatz 1 Verkehrsdaten und Nutzungsdaten erheben.

(2) Die Erteilung einer Auskunft darüber, ob von einem Telekommunikationsanschluss Telekommunikationsverbindungen zu den in § 23 Absatz 1 genannten Personen hergestellt worden sind (Zielsuchlauf), darf nur angeordnet werden, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre.

(3) Durch den Einsatz technischer Mittel darf

1. zur Vorbereitung einer Maßnahme nach § 23 Absatz 1 die Geräte- und Kartennummer,
2. zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person der Standort eines aktiv geschalteten Mobilfunkendgerätes

ermittelt werden. Die Maßnahme nach Satz 1 Nummer 1 ist nur zulässig, wenn die Voraussetzungen des § 23 Absatz 1 vorliegen und die Durchführung der Überwachungsmaßnahme ohne die Geräte- und Kartennummer nicht möglich oder wesentlich erschwert wäre. Die Maßnahme nach Satz 1 Nummer 2 ist nur dann zulässig, wenn die Ermittlung des Aufenthaltsortes auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist.

(4) Jeder Diensteanbieter ist verpflichtet, der Polizei auf Grund der Anordnung einer Datenerhebung nach Absatz 1

1. vorhandene Telekommunikationsdaten und Nutzungsdaten zu übermitteln,
2. Daten über zukünftige Telekommunikationsverbindungen und Nutzungsdaten zu übermitteln oder
3. die für die Ermittlung des Standortes eines Mobilfunkendgerätes nach Absatz 3 erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartennummer mitzuteilen.

Die Daten sind der Polizei unverzüglich oder innerhalb der in der Anordnung bestimmten Zeitspanne sowie auf dem darin bestimmten Übermittlungsweg zu übermitteln. Für die Entschädigung gilt § 23 des Justizvergütungs- und -entschädigungsgesetzes vom 5. Mai 2004 (BGBl. I S. 718, 776), zuletzt geändert am 11. Oktober 2016 (BGBl. I S. 2222, 2224), in der jeweils geltenden Fassung entsprechend.

(5) Verkehrsdaten sind alle nicht inhaltsbezogenen Daten, die im Zusammenhang mit einer Telekommunikation auch unabhängig von einer konkreten Telekommunikationsverbindung technisch erhoben und erfasst werden, insbesondere

1. Berechtigungskennung, Kartennummer, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung,
2. Beginn und Ende der Verbindung nach Datum und Uhrzeit,
3. vom Kunden in Anspruch genommene Telekommunikationsdienstleistung,
4. Endpunkte fest geschalteter Verbindungen, ihr Beginn und Ende nach Datum und Uhrzeit.

(6) Nutzungsdaten sind personenbezogene Daten einer Nutzerin oder eines Nutzers von Telemedien, die durch denjenigen, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereit hält oder den Zugang zur Nutzung vermittelt, erhoben werden, um die Inanspruchnahme von Telemedien zu ermöglichen oder abzurechnen, insbesondere

1. Merkmale zur Identifikation der Nutzerin oder des Nutzers,
2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

§ 26
Anordnung und Ausführung

(1) Maßnahmen nach §§ 23 bis 25 bedürfen einer richterlichen Anordnung. Bei Gefahr im Verzug kann die Maßnahme durch die Polizeipräsidentin oder den Polizeipräsidenten oder die Vertretung im Amt angeordnet werden. Eine richterliche Bestätigung ist unverzüglich einzuholen. Die Maßnahme ist zu beenden, wenn sie nicht innerhalb von drei Tagen richterlich bestätigt wird; in diesem Fall sind die Datenaufzeichnungen unverzüglich zu vernichten, wenn diese nicht zur Strafverfolgung benötigt werden. Zuständig ist das Amtsgericht Hamburg. Für das Verfahren findet Buch 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend Anwendung. Von einer Anhörung der betroffenen Person durch das Gericht und der Bekanntgabe der richterlichen Entscheidung an die betroffene Person ist abzusehen, wenn die vorherige Anhörung oder die Bekanntgabe der Entscheidung den Zweck der Maßnahme gefährden würde. Die richterliche Entscheidung wird mit ihrer Bekanntgabe an die beantragende Stelle wirksam.

(2) Die Anordnung nach §§ 23 bis 25 muss den Namen und die Anschrift der betroffenen Person, gegen die sie sich richtet, sowie die Rufnummer oder eine andere Kennung ihres Telekommunikationsanschlusses oder ihres Endgerätes, wenn diese allein dem zu überwachenden Endgerät zuzuordnen ist, enthalten oder das informationstechnische System bezeichnen. Sofern andernfalls die Erreichung des Zwecks aussichtslos oder erheblich erschwert wäre, genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, über die personenbezogene Daten erhoben oder über die Auskunft erteilt werden soll. Die Anordnung einer Maßnahme nach § 24 darf auch zur nicht offenen Durchsuchung von Sachen sowie zum verdeckten Betreten und Durchsuchen der Wohnung des Betroffenen ermächtigen, soweit dies zur Durchführung der Maßnahme erforderlich ist. Die Anordnung nach § 23 Absatz 1, § 24 Absatz 1 und § 25 Absatz 2 ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, wenn die Voraussetzungen für die Maßnahme noch vorliegen. Die Anordnung nach § 23 Absatz 2 Satz 1 ist auf höchstens zwei Wochen und die Anordnung nach § 23 Absatz 2 Satz 2 auf höchstens zwei Tage zu befristen.

(3) Die durch eine Maßnahme nach §§ 23 bis 25 erlangten Daten dürfen nur zu den Zwecken verwendet werden, zu denen sie erhoben wurden. Zu Zwecken der Strafverfolgung dürfen sie verwendet werden, wenn sie auch dafür unter Einsatz derselben Befugnisse hätten erhoben werden dürfen. Die Daten, welche auf Grund einer Maßnahme nach § 25 Absatz 2 erlangt werden, dürfen über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus nicht verwendet werden. Daten, bei denen sich nach der Auswertung herausstellt, dass sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, dürfen nicht verwendet werden. Daten, die keinen unmittelbaren Bezug zu den der Anordnung zugrunde liegenden Gefahren haben, dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer anderweitigen unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder zur Strafverfolgung unter der Voraussetzung von Satz 3 erforderlich. § 22 Absatz 5 Satz 5 gilt entsprechend.

(4) Personen, gegen die sich die Datenerhebungen nach den §§ 23 bis 25 richteten oder die von ihr sonst betroffen wurden, sind nach Abschluss der Maßnahme hierüber zu benachrichtigen.

(5) Sind die nach §§ 23 bis 25 erlangten Daten zur Aufgabenerfüllung nicht mehr erforderlich, sind sie zu löschen. Die Löschung unterbleibt, soweit die Daten für eine Mitteilung an den Betroffenen nach Absatz 4 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme von Bedeutung sein können. In diesem Fall ist die Verarbeitung der Daten einzuschränken und sie dürfen nur zu diesen Zwecken verarbeitet werden. § 22 Absatz 8 Satz 5 gilt entsprechend. Daten, die dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, sind unverzüglich zu löschen; § 21 Absatz 3 Sätze 9 bis 11 gilt entsprechend. Daten, die keinen unmittelbaren Bezug zu den der Anordnung zugrunde liegenden Gefahren haben, sind zu löschen, es sei denn, ihre Verwendung ist zur Abwehr einer anderweitigen unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder zur Strafverfolgung unter der Voraussetzung von Absatz 3 Satz 3 erforderlich.

(6) Werden Maßnahmen nach §§ 23 bis 25 durchgeführt, so darf diese Tatsache von Personen, die Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden. Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen Satz 1 eine Mitteilung macht. Die in Satz 1 genannten Personen sind von dem nach § 25 Absatz 4 Verpflichteten

über das Mitteilungsverbot sowie über die Strafbarkeit zu belehren; die Belehrung ist aktenkundig zu machen.

§ 27

Bestandsdatenverarbeitung

(1) Die Polizei darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt, Auskunft über Bestandsdaten über die für eine Gefahr Verantwortlichen und unter den Voraussetzungen von § 10 SOG über die dort genannten Personen verlangen, wenn dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist. Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten verlangt werden.

(3) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. Für die Entschädigung der Diensteanbieter gilt § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend.

(4) In den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 darf die Maßnahme nur von der Polizeipräsidentin oder vom Polizeipräsidenten oder der Vertretung im Amt, bei Gefahr im Verzug auch von der Polizeiführerin oder dem Polizeiführer vom Dienst angeordnet werden. Für die Benachrichtigung von Personen, gegen die sich die Datenerhebungen richteten, gilt § 21 Absatz 3 in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 entsprechend. Satz 2 findet keine Anwendung, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder für die Nutzung der durch die Auskunft erlangten Daten eine gesetzliche Benachrichtigungspflicht vorgesehen ist.

(5) Bestandsdaten im Sinne des Absatzes 1 oder 2 sind die nach §§ 95 und 111 des Telekommunikationsgesetzes und die nach § 14 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert am 28. September 2017 (BGBl. I S. 3530), in der jeweils geltenden Fassung erhobenen Daten.

§ 28

Datenverarbeitung durch den Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist

(1) Die Polizei darf unter den Voraussetzungen von § 20 Absatz 1 Satz 1 Daten verarbeiten durch den Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Der Einsatz nach Absatz 1 bedarf der richterlichen Anordnung. § 20 Absatz 2 gilt entsprechend. Der Einsatz ist auf höchstens neun Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als neun Monate ist zulässig, soweit die Voraussetzungen für die Maßnahme noch vorliegen. Personen, gegen die sich Datenerhebungen richteten, sind nach Abschluss der Maßnahme hierüber durch die Polizei zu benachrichtigen.

(3) Werden der Person, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung bekannt, gilt § 21 Absatz 3 Sätze 7 bis 11 entsprechend.

§ 29

Datenverarbeitung durch den Einsatz Verdeckter Ermittler

(1) Die Polizei darf durch eine Vollzugsbeamtin oder einen Vollzugsbeamten, der unter einer ihr oder ihm verliehenen, auf Dauer angelegten, veränderten Identität (Legende) eingesetzt wird (Verdeckte Ermittler), personenbezogene Daten über die für eine Gefahr Verantwortlichen und deren Kontakt- und Begleitpersonen verarbeiten, wenn

1. dies zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,
2. Tatsachen, die ein wenigstens seiner Art nach konkretes und zeitlich absehbares Geschehen erkennen lassen, die Annahme rechtfertigen, dass Straftaten von erheblicher Bedeutung begangen werden sollen und der Einsatz zur Verhütung dieser Straftaten erforderlich ist.

Verbrechen sowie Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, und sich gegen bedeutende Sach- oder Vermögenswerte richten, sind nur dann als Straftat von erheblicher Bedeutung im Sinne von § 2 Absatz 2 Nummer 2 anzusehen, wenn die Erhaltung der bedeutenden Sach- und Vermögenswerte im öffentlichen Interesse liegt.

(2) Soweit es für den Aufbau und zur Aufrechterhaltung der Legende unerlässlich ist, dürfen entsprechende Urkunden hergestellt oder verändert werden. Ein Verdeckter Ermittler darf zur Erfüllung seines Auftrages unter der Legende am Rechtsverkehr teilnehmen.

(3) Ein Verdeckter Ermittler darf unter der Legende mit Einverständnis des Berechtigten dessen Wohnung betreten. Das Einverständnis darf nicht durch ein über die Nutzung der Legende hinausgehendes Vortäuschen eines Zutrittsrechts herbeigeführt werden. Im Übrigen richten sich die Befugnisse eines Verdeckten Ermittlers nach diesem Gesetz oder anderen Rechtsvorschriften.

(4) Der Einsatz nach Absatz 1 bedarf der richterlichen Anordnung. § 20 Absatz 2 gilt entsprechend. Der Einsatz ist auf höchstens neun Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als neun Monate ist zulässig, soweit die Voraussetzungen für die Maßnahme noch vorliegen. Personen, gegen die sich Datenerhebungen richteten, sind nach Abschluss der Maßnahme hierüber durch die Polizei zu benachrichtigen.

(5) Werden dem Verdeckten Ermittler Erkenntnisse aus dem Kernbereich privater Lebensgestaltung bekannt, gilt § 21 Absatz 3 Sätze 7 bis 11 entsprechend.

§ 30

Elektronische Aufenthaltsüberwachung

(1) Die Polizei darf eine Person verpflichten, ein technisches Mittel, mit dem der Aufenthaltsort dieser Person elektronisch überwacht werden kann, ständig in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen, wenn

1. bestimmte Tatsachen, die ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennen lassen, die Annahme rechtfertigen, dass diese Person eine terroristische Straftat begehen wird, oder

2. deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird,

und die Datenerhebung und weitere Verarbeitung zur Verhütung dieser Straftaten erforderlich ist oder

3. dies zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und die zu verpflichtende Person für die Gefahr verantwortlich ist.

Die Anordnung kann insbesondere mit einer Maßnahme nach § 12b Absatz 2 SOG verbunden werden. Eine terroristische Straftat im Sinne des Satz 1 sind die in § 89c Absatz 1 des Strafgesetzbuchs bezeichneten Straftaten sowie §§ 89b, 89c, 129 und 310 des Strafgesetzbuchs im In- und Ausland, wenn diese Straftaten dazu bestimmt sind,

1. die Bevölkerung auf erhebliche Weise einzuschüchtern,
2. eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder
3. die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen.

(2) Die Polizei verarbeitet mit Hilfe der von der betroffenen Person mitgeführten technischen Mittel automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung. Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Soweit dies zur Erfüllung des Überwachungszweckes erforderlich ist, dürfen die Daten zu einem Bewegungsbild verbunden werden. Die Daten dürfen ohne Einwilligung der betroffenen Person nur verwendet werden, soweit dies erforderlich ist für die folgenden Zwecke:

1. zur Verhütung oder zur Verfolgung von Straftaten im Sinne von Absatz 1 Satz 3,
2. zur Feststellung von Verstößen gegen ein Aufenthaltsverbot nach § 12b Absatz 2 SOG,
3. zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder
4. zur Aufrechterhaltung der Funktionsfähigkeit der technischen Mittel.

(3) Die Maßnahme nach Absatz 1 bedarf der richterlichen Anordnung. Zuständig ist das Amtsgericht Hamburg. Für das Verfahren findet Buch 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend Anwendung. Von einer Anhörung der betroffenen Person durch das Gericht ist abzusehen, wenn die vorherige Anhörung oder die Bekanntgabe der Entscheidung den Zweck der Maßnahme gefährden würde. Die Erstellung eines Bewegungsbildes ist nur zulässig, wenn dies richterlich besonders gestattet wird.

(4) Die Anordnung nach Absatz 3 ist auf höchstens drei Monate zu befristen. Sie ist aktenkundig zu machen. Aus der Anordnung müssen sich

1. die Person, gegen die sich die Maßnahme richtet, mit Name und Anschrift,
2. Art, Beginn und Ende der Maßnahme,
3. Tatsachen, die den Einsatz der Maßnahme begründen,

ergeben.

Eine Verlängerung der Maßnahme um jeweils drei Monate ist zulässig, soweit die Voraussetzungen für die Maßnahme noch vorliegen.

(5) Die über eine Maßnahme nach Absatz 1 erhobenen Daten sind spätestens zwei Monate nach Beendigung der Maßnahme zu löschen, soweit sie nicht für die in Absatz 2 genannten Zwecke erforderlich sind. Bei jedem Abruf der Daten sind der Zeitpunkt, die abgerufenen Daten und die bearbeitende Person zu dokumentieren. Die in der Dokumentation enthaltenen Daten dürfen ausschließlich zur Kontrolle der Zulässigkeit der Abrufe verwendet werden und sind nach zwölf Monaten zu löschen. Werden innerhalb der Wohnung der betroffenen Person über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben, dürfen diese nicht verändert, genutzt oder übermittelt werden; sie sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die in der Dokumentation enthaltenen Daten dürfen ausschließlich zur Datenschutzkontrolle verwendet werden. Die Dokumentation ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des zweiten Kalenderjahres, das dem Jahr der Dokumentation folgt.

(6) Auf Ersuchen der Polizei übermitteln die zuständigen Polizeien des Bundes und der Länder sowie sonstige öffentliche Stellen dieser im Rahmen der geltenden Gesetze personenbezogene Daten über die betroffene Person, soweit dies zur Durchführung der Maßnahme nach den Absätzen 1 und 2 erforderlich ist. Die Polizei kann zu diesem Zwecke auch bei anderen Stellen personenbezogene Daten über die betroffene Person erheben.

§ 31

Polizeiliche Beobachtung, gezielte Kontrolle

(1) Die Polizei darf personenbezogene Daten, insbesondere die Personalien einer Person sowie das amtliche Kennzeichen des von ihr benutzten oder eingesetzten Kraftfahrzeuges, zur polizeilichen Beobachtung in einem Dateisystem verarbeiten (Ausschreibung zur polizeilichen Beobachtung), wenn

1. die Gesamtwürdigung der Person und der von ihr bisher begangenen Straftaten erwarten lassen, dass sie auch künftig Straftaten von erheblicher Bedeutung begehen wird,
2. Tatsachen die Annahme rechtfertigen, dass die Person Straftaten von erheblicher Bedeutung begehen wird,

und dies zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist. Unter den Voraussetzungen von Satz 1 ist auch die Ausschreibung zur gezielten Kontrolle zulässig.

(2) Im Falle eines Antreffens der Person oder des Kraftfahrzeugs dürfen die Personalien der Person und die von Begleitern, das Kennzeichen des benutzten oder eingesetzten Kraftfahrzeugs sowie Erkenntnisse über Zeit, Ort, mitgeführten Sachen, Verhalten, Vorhaben und sonstige Umstände des Antreffens an die ausschreibende Polizeibehörde übermittelt werden.

(3) § 21 Absatz 2 Sätze 2 bis 5 gilt entsprechend. Die Anordnung ist auf höchstens ein Jahr zu befristen. Spätestens nach Ablauf von sechs Monaten ist zu prüfen, ob die Voraussetzungen für die Anordnung noch bestehen. Das Ergebnis dieser Prüfung ist aktenkundig zu machen. Zur Verlängerung der Frist bedarf es einer neuen Anordnung.

(4) Liegen die Voraussetzungen für die Anordnung nicht mehr vor, ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, ist die Ausschreibung zur polizeilichen Beobachtung oder gezielten Kontrolle unverzüglich zu löschen. Personen, gegen die sich Datenerhebungen

richteten, sind nach Abschluss der Maßnahme hierüber durch die Polizei zu benachrichtigen.

§ 32

Anerkennung von richterlichen Anordnungen anderer Länder

Richterliche Anordnungen anderer Länder, die personenbezogene Datenerhebungen nach §§ 20 und 21 oder §§ 28 bis 30 betreffen, werden als nach diesem Gesetz angeordnete Maßnahme anerkannt, wenn sie auch hiernach unter Einsatz derselben Befugnisse hätten angeordnet werden dürfen.

§ 33

Opferschutzmaßnahmen

(1) Für eine Person, die Opfer einer Straftat wurde oder bei der davon auszugehen ist, dass sie in absehbarer Zeit Opfer einer Straftat werden kann, dürfen auf Anordnung der Leitung des Landeskriminalamtes oder durch die Vertretung im Amt Urkunden und sonstige Dokumente zum Aufbau und zur Aufrechterhaltung einer vorübergehend geänderten Identität hergestellt, vorübergehend verändert und die entsprechend geänderten Daten verarbeitet werden, wenn dies zu ihrem Schutz vor einer Gefahr für

1. Leib, Leben oder Freiheit der Person erforderlich ist und
2. die Person für diese Schutzmaßnahme geeignet ist.

Die zu schützende Person darf unter der vorübergehend geänderten Identität am Rechtsverkehr teilnehmen.

(2) Soweit erforderlich, können Maßnahmen nach Absatz 1 auch auf Angehörige einer in Absatz 1 genannten Person oder ihr sonst nahe stehende Personen erstreckt werden.

(3) § 29 Absatz 2 findet auf die mit dem Schutz betrauten Polizeibeamtinnen oder Polizeibeamten Anwendung, soweit dies zur Vorbereitung, Durchführung, Lenkung oder Absicherung der Schutzmaßnahmen erforderlich ist.

(4) Die Polizei darf zur Erfüllung des Schutzauftrages personenbezogene Daten Dritter, die mit der zu schützenden Person in Kontakt stehen, verarbeiten.

Abschnitt 3

Weitere Datenverarbeitung

§ 34

Grundsätze der Zweckbindung

(1) Die Polizei darf personenbezogene Daten verarbeiten

1. zu dem Zweck, zu dem diese Daten erlangt worden sind,
2. zu einem anderen polizeilichen Zweck, soweit die Polizei die Daten zu diesem Zweck erheben dürfte.

Eine Verarbeitung für andere Zwecke liegt nicht vor, soweit diese der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen, der Datensicherung, Datenschutzkontrolle oder der Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dient.

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

1. eine gesetzliche Vorschrift dies für den Geltungsbereich dieses Gesetzes vorsieht oder zwingend voraussetzt,
2. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die Verteidigung oder die nationale Sicherheit 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 Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Erledigung eines gerichtlichen Auskunftsersuchens erforderlich ist 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 dies im Interesse der betroffenen Person liegt und sie 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.

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

(4) Daten, die mit besonderen Mitteln nach den §§ 20 bis 31 sowie nach § 50 erhoben wurden, dürfen für andere Verfahren nur verarbeitet werden, wenn sie auch dafür unter Einsatz dieser Befugnisse hätten erhoben werden dürfen. Sie dürfen nach Maßgabe bundesgesetzlicher Regelungen auch für gemeinsame Dateien des Bundes und der Länder auf den Gebieten des Staatsschutzes und der organisierten Kriminalität in Fällen von erheblicher Bedeutung einschließlich der Vorfeldbeobachtung verarbeitet werden; dies gilt auch für Dateien, die nicht in der Verantwortung von Polizeibehörden errichtet werden. Daten, die nach § 14 erhoben wurden, dürfen für andere Zwecke nur verarbeitet werden, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist oder Anhaltspunkte dafür vorliegen, dass die Verfolgung einer Straftat von erheblicher Bedeutung ansonsten aussichtslos oder wesentlich erschwert wäre.

(5) Werden wertende Angaben in Dateisystemen gespeichert, muss feststellbar sein, bei welcher Stelle die den Angaben zugrunde liegenden Informationen vorhanden sind. Das Gleiche gilt, wenn in einem Dateisystem Kurzinformationen über bestimmte Sachverhalte gespeichert werden. Wertende Angaben dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen wurden.

(6) In den Fällen, in denen bereits Daten zu einer Person vorhanden sind, können zu dieser Person auch personengebundene Hinweise, die zum Schutz dieser Person oder zum Schutz der Bediensteten der Gefahrenabwehr- und der Polizeibehörden erforderlich sind, und weitere Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermitt-

lungsansätzen zu dienen, verarbeitet werden. Bei personengebundenen Hinweisen, die zugleich den besonderen Kategorien personenbezogener Daten entsprechen, sind die Vorgaben des § 4 zu beachten.

(7) Für die Planung von Maßnahmen der Kriminalitätsbekämpfung kann die Polizei vorhandene personenbezogene Daten über Vermisstenfälle, auswertungsrelevante Straftaten und verdächtige Wahrnehmungen zur Erstellung eines Kriminalitätslagebildes verarbeiten. Ein Kriminalitätslagebild darf Daten von Geschädigten, Zeugen sowie anderen nicht tatverdächtigen Personen nur enthalten, soweit dies zur Zweckerreichung erforderlich ist. Die automatisiert verarbeiteten personenbezogenen Daten sind spätestens am Ende des der Speicherung folgenden Jahres zu löschen.

§ 35

Dauer der Datenspeicherung

(1) Daten dürfen solange gespeichert werden, wie es für die Aufgabenerfüllung erforderlich ist.

(2) Für automatisierte Dateisysteme sind Fristen festzulegen, nach deren Ablauf spätestens überprüft werden muss, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungsfristen). Für nicht automatisierte Dateisysteme sind Prüfungsfristen oder Aufbewahrungsfristen festzulegen. Die Fristen dürfen bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre nicht überschreiten, wobei der Speicherungszweck sowie Art und Bedeutung des Anlasses der Speicherung zu berücksichtigen sind. Nach Ablauf der Prüfungsfristen ist eine weitere Speicherung nur zulässig, wenn dies wegen besonderer Gründe im Einzelfall erforderlich ist. Die Erforderlichkeit der Speicherung ist zu dokumentieren und spätestens nach Ablauf von drei Jahren erneut zu prüfen.

(3) Die Frist beginnt mit dem Tag, an dem das letzte Ereignis erfasst worden ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung eines Betroffenen aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Werden innerhalb der Fristen weitere personenbezogene Daten über dieselbe Person gespeichert, so gilt für alle Speicherungen gemeinsam die Frist, die als letztes endet. Soweit hierdurch für zeitlich frühere Speicherungen die in Absatz 2 Satz 3 genannte Höchstprüffrist zweimal erreicht wird, ist eine weitere Speicherung dieser personenbezogenen Daten nur zulässig, wenn dies wegen besonderer Gründe im Einzelfall erforderlich ist. Die Erforderlichkeit der Speicherung ist zu dokumentieren und spätestens nach Ablauf von drei Jahren erneut zu prüfen.

§ 36

Weitere Verarbeitung von personenbezogenen Daten

(1) Die Polizei darf personenbezogene Daten in Dateisystemen verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben, einschließlich einer zeitlich befristeten Dokumentation oder der Vorgangsverwaltung erforderlich ist.

(2) Dabei darf die Polizei auch die im Rahmen der Verfolgung von Straftaten gewonnenen personenbezogenen Daten zum Zwecke der Gefahrenabwehr (§ 1 Absatz 1) verarbeiten. Soweit die Daten ausschließlich auf Grund von Befugnissen erhoben wurden, die den in §§ 20 bis 31 und 50 genannten Befugnissen entsprechen, dürfen sie für andere Verfahren nur verarbeitet werden, wenn sie auch dafür unter Einsatz dieser Befugnisse hätten erhoben werden dürfen. Für die Dauer von zwei Jahren ist eine suchfähige Speicherung dieser Daten erforderlich, wenn gegen diese Personen ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist. Entfällt der dem Ermittlungsverfahren zugrunde liegende Verdacht, sind die Daten zu löschen. Eine weitere Speicherung, Veränderung und Nutzung zur vorbeugenden Bekämpfung von Straftaten ist zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person zukünftig eine Straftat begehen wird. Tatsächliche Anhaltspunkte können sich insbesondere aus Art, Ausführung und Schwere der Tat ergeben. Lagen solche Anhaltspunkte im Zeitpunkt der Speicherung der personenbezogenen Daten noch nicht vor, dürfen die Daten zur vorbeugenden Bekämpfung von Straftaten über die Dauer von zwei Jahren hinaus nur dann gespeichert, verändert und genutzt werden, wenn auf Grund tatsächlicher Anhaltspunkte der Verdacht besteht, dass die betroffene Person innerhalb dieser zwei Jahre eine weitere Straftat begangen hat.

(3) Die Polizei darf personenbezogene Daten von Kontakt- oder Begleitpersonen einer Person, bei der tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie künftig Straftaten begehen wird, sowie über Auskunftspersonen in Dateisystemen suchfähig verarbeiten, soweit dies zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Die Speicherungsdauer darf drei Jahre nicht überschreiten. Nach jeweils einem Jahr, gerechnet vom Zeitpunkt der letzten Speicherung, ist zu prüfen, ob die Voraussetzungen nach Satz 1 noch vorliegen; die Entscheidung kann nur durch einen besonders ermächtigten Bediensteten getroffen werden.

(4) Die Polizei darf personenbezogene Daten verarbeiten, um festzustellen, ob die betreffenden Personen die Voraussetzungen nach den Absätzen 1 bis 3 erfüllen. Die Daten dürfen ausschließlich zu diesem Zweck weiterverarbeitet werden und sind gesondert zu speichern. Die Daten sind nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach den Absätzen 1 bis 3 erfüllt.

§ 37

Verarbeitung von Daten zu archivarischen, wissenschaftlichen, historischen und statistischen Zwecken sowie zur Aus- und Fortbildung

(1) Die Polizei darf personenbezogene Daten auch über die nach anderen Vorschriften zulässige Speicherungsdauer hinaus zur Aus- und Fortbildung verarbeiten. Dabei ist sicherzustellen, dass die Einzelangaben über persönliche oder sachliche Verhältnisse anonymisiert werden. Die Anonymisierung kann unterbleiben, wenn diese nicht mit vertretbarem Aufwand möglich ist oder dem Aus- und Fortbildungszweck entgegensteht und jeweils die schutzwürdigen Belange des Betroffenen nicht offensichtlich überwiegen.

(2) Die Polizei darf gespeicherte personenbezogene Daten zu archivarischen, wissenschaftlichen, historischen oder statistischen Zwecken verarbeiten; die Daten sind, soweit und sobald der Zweck dies zulässt, zu anonymisieren. Eine Veröffentlichung ist zu statistischen Zwecken nur zulässig, wenn kein Rückschluss auf die Verhältnisse einer natürlichen Person möglich ist; zu archivarischen, wissenschaftlichen oder historischen Zwecken ist eine Veröffentlichung nur zulässig, wenn

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

§ 38

Allgemeine Regelungen der Datenübermittlung

(1) Die Polizei darf personenbezogene Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck übermit-

teln, zu dem sie die Daten erlangt oder gespeichert hat. § 34 Absatz 4 gilt entsprechend. Datenübermittlung im Sinne dieses Gesetzes ist auch die Weitergabe polizeilicher Daten innerhalb der zuständigen Behörde an andere als die in § 2 Absatz 1 genannten Organisationseinheiten.

(2) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderem Amtsgeheimnis und sind sie der Polizei von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist die Datenübermittlung durch die Polizei nur zulässig, wenn der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die Polizei erlangt hat.

(3) Die Verantwortung für die Übermittlung trägt die Polizei. Diese prüft die Zulässigkeit der Datenübermittlung. Erfolgt die Datenübermittlung auf Grund eines Ersuchens des Empfängers, hat dieser die zur Prüfung erforderlichen Angaben zu machen. Bei Ersuchen von Polizeidienststellen sowie anderen Behörden und öffentlichen Stellen prüft die Polizei nur, ob das Ersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, im Einzelfall besteht Anlass zu einer weitergehenden Überprüfung. Erfolgt die Datenübermittlung durch automatisierten Abruf, trägt der Empfänger die Verantwortung für die Rechtmäßigkeit des Abrufs.

(4) Die Polizei hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat sie, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat sie zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(5) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.

(6) Der Empfänger darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verarbeiten, zu dem sie ihm übermittelt worden sind. Ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie Personen und Stellen außerhalb des öffentlichen Bereichs sind bei der Datenübermittlung darauf hinzuweisen.

§ 39

Besondere Grundsätze der Datenverarbeitung im Rahmen der polizeilichen Zusammenarbeit zwischen Mitgliedstaaten der Europäischen Union und Schengen-assoziierten Staaten

(1) Die von einer öffentlichen Stelle eines Mitgliedstaates der Europäischen Union übermittelten personenbezogenen Daten sind besonders zu kennzeichnen. Sie dürfen vorbehaltlich entgegenstehender gesetzlicher Verwendungsbeschränkungen für andere Zwecke als diejenigen, für die sie übermittelt wurden, verarbeitet werden für

1. die Verhütung oder Verfolgung von Straftaten oder Vollstreckung von strafrechtlichen Sanktionen,
2. andere mit den Zwecken nach Nummer 1 unmittelbar zusammenhängende justizielle und verwaltungsbehördliche Verfahren,
3. die Abwehr einer unmittelbar bevorstehenden erheblichen Gefahr für die öffentliche Sicherheit oder
4. jeden anderen Zweck mit Einwilligung der übermittelnden Stelle oder der betroffenen Person.

(2) Sofern die Polizei personenbezogene Daten an eine öffentliche Stelle eines Mitgliedstaates der Europäischen Union oder an eine Agentur oder Einrichtung, die auf Grund des Vertrages über die Europäische Union oder des Vertrages über die Arbeitsweise der Europäischen Union errichtet worden ist, übermittelt, hat sie auf besondere Verwendungsbeschränkungen hinzuweisen, sofern diese auch im innerstaatlichen Recht Anwendung finden. Die von der übermittelnden Stelle für die Verwendung der Daten mitgeteilten Beschränkungen und Aufbewahrungs- und Löschungsfristen sind zu beachten. Dies gilt nicht, wenn die Daten bei Fristablauf zur Verhütung oder Verfolgung einer Straftat oder zur Strafvollstreckung benötigt werden.

(3) Die Polizei unterrichtet die übermittelnde öffentliche Stelle eines Mitgliedstaates der Europäischen Union oder die übermittelnde Agentur oder Einrichtung, die auf Grund des Vertrages über die Europäische Union oder des Vertrages über die Arbeitsweise der Europäischen Union errichtet worden ist, auf deren Ersuchen zu Zwecken der Datenschutzkontrolle über die Verarbeitung der Daten.

(4) Personenbezogene Daten, die von einer öffentlichen Stelle eines Mitgliedstaates der Europäischen Union übermittelt wurden, darf die Polizei mit Einwilligung der zuständigen Stelle dieses Staates an nicht-öffentliche Stellen in den Mitgliedstaaten nur übermitteln, wenn überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen und die Übermittlung im Einzelfall unerlässlich ist

1. zur Verhütung von Straftaten,
2. zur Abwehr einer unmittelbar bevorstehenden erheblichen Gefahr für die öffentliche Sicherheit oder
3. zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner.

(5) Für Schengen-assoziierte Staaten gelten die Absätze 1 bis 4 entsprechend.

§ 40

Datenübermittlung zwischen Polizeidienststellen

An andere Polizeidienststellen dürfen personenbezogene Daten übermittelt werden, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist.

§ 41

Datenübermittlung im innerstaatlichen Bereich und im Bereich der Europäischen Union und deren Mitgliedstaaten

(1) Die Polizei darf personenbezogene Daten an öffentliche Stellen übermitteln, soweit dies erforderlich ist

1. zur Erfüllung polizeilicher Aufgaben,
2. zur Abwehr einer bevorstehenden Gefahr durch den Empfänger,
3. zur Teilnahme am Privatrechtsverkehr oder zur Durchsetzung öffentlich-rechtlicher Geldforderungen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an der Geheimhaltung überwiegt,
4. in besonders gelagerten Einzelfällen zur Feststellung der gesetzlichen Voraussetzungen für den Erlass eines Verwaltungsaktes durch eine andere für Aufgaben der Gefahrenabwehr zuständige öffentliche Stelle, oder

5. zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder schwer wiegender Beeinträchtigungen von gewichtigen Rechtspositionen einzelner, insbesondere zur Abwehr von Gefahren für Leib, Leben, Gesundheit, persönliche Freiheit oder erhebliche Vermögenswerte.

Die Übermittlung zu einem anderen Zweck, als dem, zu dem die Polizei die Daten erlangt oder gespeichert hat, ist nur zulässig, wenn der Empfänger die Daten auf andere Weise

1. nicht oder nicht rechtzeitig erlangen kann oder
2. nur mit unverhältnismäßig hohem Aufwand erlangen kann und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

In den Fällen von Satz 1 Nummern 1 und 4 ist die Übermittlung zu einem anderen Zweck darüber hinaus nur zulässig, wenn die Übermittlung zur Abwehr einer bevorstehenden Gefahr erforderlich ist.

(2) Die Polizei darf personenbezogene Daten, die sie anlässlich ihrer Aufgabenerfüllung erlangt hat, an andere für Aufgaben der Gefahrenabwehr zuständige öffentliche Stellen übermitteln, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben des Empfängers erforderlich ist.

(3) Die Absätze 1 und 2 gelten entsprechend für die Übermittlung von personenbezogenen Daten an

1. öffentliche und nichtöffentliche Stellen in Mitgliedstaaten der Europäischen Union sowie an zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten,
2. Schengen-assoziierte Staaten.

(4) Anderweitige besondere Rechtsvorschriften über die Datenübermittlung an öffentliche Stellen bleiben unberührt.

§ 42
Datenübermittlung an Mitgliedstaaten der Europäischen Union und Schengen-assoziierte Staaten nach Maßgabe des Rahmenbeschlusses 2006/960/JI

(1) Die Polizei darf auf ein Ersuchen einer Polizeibehörde oder einer sonstigen für die Verhütung und Verfolgung von Straftaten zuständigen öffentlichen Stelle eines Mitgliedstaates der Europäischen Union, das nach Maßgabe des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. EU 2006 Nr. L 386 S. 89, 2007 Nr. L 75 S. 26) gestellt worden ist, vorhandene personenbezogene Daten zum Zweck der Verhütung von Straftaten übermitteln. Für die Übermittlung dieser Daten gelten die Vorschriften über die Datenübermittlung im innerstaatlichen Bereich entsprechend.

(2) Die Übermittlung personenbezogener Daten nach Absatz 1 ist nur zulässig, wenn das Ersuchen mindestens folgende Angaben enthält:

1. die Bezeichnung und die Anschrift der ersuchenden Behörde,
2. die Bezeichnung der Straftat, zu deren Verhütung die Daten benötigt werden,
3. die Beschreibung des Sachverhalts, der dem Ersuchen zugrunde liegt,
4. die Benennung des Zwecks, zu dem die Daten erbeten werden, und
5. Einzelheiten zur Identität der betroffenen Person, sofern sich das Ersuchen auf eine bekannte Person bezieht.

(3) Die Polizei darf auch ohne Ersuchen personenbezogene Daten an eine Polizeibehörde oder eine sonstige für die Verhütung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union übermitteln, wenn Tatsachen die Annahme rechtfertigen, dass eine Straftat im Sinne des Artikels 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. EG Nr. L 190 S. 1), geändert am 26. Februar 2009 (ABl. EU Nr. L 81 S. 24), begangen werden soll und zu erwarten ist, dass die Datenübermittlung zur Verhütung einer solchen Straftat erforderlich ist. Für die Übermittlung dieser Daten gelten die Vorschriften über die Datenübermittlung im innerstaatlichen Bereich entsprechend.

(4) Die Datenübermittlung nach den Absätzen 1 und 3 kann unterbleiben, wenn

1. hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder beeinträchtigt würden,
2. die Übermittlung der Daten unverhältnismäßig wäre oder die Daten für die Zwecke, für die sie übermittelt werden sollen, nicht erforderlich sind,
3. hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde oder
4. die Tat, zu deren Verhütung die Daten übermittelt werden sollen, nach deutschem Recht mit einer Freiheitsstrafe von im Höchstmaß einem Jahr oder weniger bedroht ist.

(5) Die nach dem Rahmenbeschluss 2006/960/JI an die Polizei übermittelten Daten dürfen nur für die Zwecke, für die sie übermittelt wurden, oder zur Abwehr einer unmittelbar bevorstehenden erheblichen Gefahr für die öffentliche Sicherheit verwendet werden. Für einen anderen Zweck oder als Beweismittel in einem gerichtlichen Verfahren dürfen sie nur verwendet werden, wenn die übermittelnde öffentliche Stelle eingewilligt hat.

(6) Für Schengen-assoziierte Staaten gelten die Absätze 1 bis 5 entsprechend.

§ 43
Allgemeine Voraussetzungen der Datenübermittlungen an Drittstatten und an über- und zwischenstaatliche Stellen

(1) Die Übermittlung personenbezogener Daten an Stellen in anderen als den in § 41 Absatz 3 genannten Staaten (Drittstaaten) oder an andere als die in § 41 Absatz 3 genannten über- und zwischenstaatliche Stellen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die in Artikel 1 Absatz 1 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) genannten Zwecke zuständig ist und
2. die Europäische Kommission gemäß Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

(2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Absatzes 1 Nummer 2 und des zu berücksichtigenden öffentlichen Interesses an der Datenübermittlung zu unter-

bleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Bei dieser Beurteilung hat die Polizei maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaates genehmigt werden. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbar bevorstehende und erhebliche Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaates abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satzes 2 ist die Stelle des anderen Mitgliedstaates, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

(4) Übermittelt die Polizei Daten nach Absatz 1, ist durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn die Polizei diese Übermittlung zuvor genehmigt hat. Bei der Entscheidung über die Erteilung der Genehmigung hat die Polizei alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an den oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder die andere internationale Organisation zulässig wäre. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 44

Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 43 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 43 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
2. nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Die Polizei hat Übermittlungen nach Absatz 1 Nummer 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit auf Anforderung zur Verfügung zu stellen.

(3) Die Polizei hat der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zumindest jährlich über Übermittlungen zu unterrichten, die auf Grund einer Beurteilung nach Absatz 1 Nummer 2 erfolgt sind. In der Unterrichtung können die Empfänger und die Übermittlungszwecke angemessen kategorisiert werden.

§ 45

Datenübermittlung ohne geeignete Garantie

(1) Liegt entgegen § 43 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 44 Absatz 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 43 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,
2. zur Wahrung berechtigter Interessen der betroffenen Person,
3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. im Einzelfall für die in Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 genannten Zwecken.

(2) Von einer Übermittlung nach Absatz 1 ist abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Für Übermittlungen nach Absatz 1 gilt § 44 Absatz 2 entsprechend.

§ 46

Sonstige Datenübermittlung an Empfänger in Drittstaaten

(1) Die Polizei kann bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 43 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,
2. die Übermittlung an die in § 43 Absatz 1 Nummer 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
3. dem Empfänger die Zwecke der Verarbeitung mitgeteilt werden und er darauf hingewiesen wird, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

(2) Im Fall des Absatzes 1 sind die in § 43 Absatz 1 Nummer 1 genannten Stellen durch die Polizei unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 44 Absätze 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Absatz 1 ist der Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne Zustimmung der Polizei nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

(5) Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

§ 47

Datenübermittlung an Personen und Stellen außerhalb des öffentlichen Bereichs, Bekanntgabe an die Öffentlichkeit

(1) Die Polizei darf personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit

1. dies zur Erfüllung polizeilicher Aufgaben erforderlich ist,
2. dies zur Abwehr einer Gefahr erforderlich ist,
3. der Auskunftsbegehrende ein berechtigtes Interesse geltend macht und offensichtlich ist, dass die Datenübermittlung im Interesse des Betroffenen liegt und er in Kenntnis der Sachlage seine Einwilligung hierzu erteilen würde.

§ 41 Absatz 1 Sätze 2 und 3 gilt entsprechend. Bewertungen sowie die nach § 36 Absatz 3 gespeicherten personenbezogenen Daten dürfen nicht übermittelt werden.

(2) Die Polizei darf personenbezogene Daten und Abbildungen zum Zwecke der Ermittlung der Identität oder des Aufenthaltes oder zur Warnung öffentlich bekannt geben, wenn die Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder bedeutende Vermögenswerte auf andere Weise nicht möglich erscheint. Die Bekanntgabe an die Öffentlichkeit nach Satz 1 bedarf der richterlichen Anordnung. Die Anordnung ergeht schriftlich. Bei Gefahr im Verzug kann die Maßnahme durch die Polizeipräsidentin oder den Polizeipräsidenten oder seine Vertretung im Amt angeordnet werden. Eine richterliche Bestätigung ist unverzüglich nachzuholen. § 22 Absatz 3 Sätze 9 bis 11 gilt entsprechend.

§ 48

Datenabgleich

(1) Die Polizei darf personenbezogene Daten der für eine Gefahr Verantwortlichen sowie der in § 11 Absatz 1 Nummer 6 genannten Personen mit dem Inhalt polizeilicher Dateisysteme abgleichen. Personenbezogene Daten anderer Personen darf die Polizei nur abgleichen, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich ist. Die Polizei darf rechtmäßig erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen.

(2) Wird der Betroffene zur Durchführung einer nach einer anderen Rechtsvorschrift zulässigen Maßnahme angehalten und kann der Datenabgleich mit dem Fahndungsbestand nicht bis zum Abschluss dieser Maßnahme vorgenommen werden, darf der Betroffene weiterhin für den Zeitraum festgehalten werden, der regelmäßig für die Durchführung eines Datenabgleiches notwendig ist.

(3) Rechtsvorschriften über den Datenabgleich in anderen Fällen bleiben unberührt.

§ 49

Automatisierte Anwendung zur Auswertung vorhandener Daten

(1) Die Polizei darf in begründeten Einzelfällen in polizeilichen Dateisystemen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenauswertung verarbeiten, wenn dies zur vorbeugenden Bekämpfung von in § 100a Absatz 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist.

(2) Im Rahmen der Verarbeitung nach Absatz 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(3) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung nach Absatz 1 erfolgen durch Anordnung der Polizeipräsidentin oder des Polizeipräsidenten oder der Vertretung im Amt. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen.

§ 50

Rasterfahndung

(1) Die Polizei darf von öffentlichen und nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist (Rasterfahndung).

(2) Die Merkmale, die für den Abgleich maßgeblich sein sollen, sind zuvor schriftlich festzulegen. Das Übermittlungsersuchen ist auf Namen, Vornamen, Geburtsdatum, Geburtsort und Anschrift sowie auf im Einzelfall festzulegende Merkmale zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Vom Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwandes eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen von der Polizei nicht weiterverarbeitet werden. § 10 SOG gilt entsprechend.

(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Akten zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. Hierüber ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren.

(4) Die Maßnahme bedarf der richterlichen Anordnung. § 20 Absatz 2 gilt entsprechend. Nach Abschluss der Maßnahme werden die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und die Bürgerschaft unverzüglich über Anlass und Umfang der veranlassten Maßnahmen unterrichtet.

(5) Nach Durchführung des Abgleichs sind die von weiterführenden polizeilichen Maßnahmen betroffenen Personen hiervon zu unterrichten, soweit dadurch nicht die Erfüllung polizeilicher Aufgaben vereitelt oder erheblich gefährdet würde oder sich an den auslösenden Sachverhalt ein strafrechtliches Ermittlungsverfahren anschließt.

§ 51

Zuverlässigkeitsüberprüfung

Die Polizei darf personenbezogene Daten auf Ersuchen einer öffentlichen oder einer nicht öffentlichen Stelle für Zwecke einer Zuverlässigkeitsüberprüfung verarbeiten, soweit dies

1. mit Zustimmung der betroffenen Person erfolgt und
2. im Hinblick auf den Anlass dieser Überprüfung, insbesondere den Zugang der betroffenen Person zu einer besonders gefährdeten Veranstaltung und mit Rücksicht auf ein berechtigtes Interesse des Empfängers erforderlich ist.

Die Polizei kann hierfür die Identität der Person feststellen, deren Zuverlässigkeit überprüft werden soll, und zu diesem Zweck vorgelegte Ausweisdokumente kopieren oder Kopien von Ausweisdokumenten anfordern. Die Überprüfung erfolgt anhand von Dateisystemen der Polizei. Die ersuchende Stelle hat die betroffene Person vor der schriftlichen Zustimmung über den konkreten Inhalt der Übermittlung und das Verfahren zu belehren und darüber aufzuklären, dass sie die Zustimmung verweigern sowie jederzeit widerrufen kann. Sie ist ferner über die ihr nach diesem Gesetz gegenüber der Polizei zustehenden Rechte nach §§ 69 und 70 zu informieren und darauf hinzuweisen, dass sie sich jederzeit an die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit wenden kann. Die Beschränkungen des § 34 Absatz 4 Satz 1, auch in Verbindung mit § 38 Absatz 1 Satz 2, finden keine Anwendung. Die Rückmeldung an eine nichtöffentliche Stelle beschränkt sich auf die Auskunft zum Vorliegen von Zuverlässigkeitsbedenken. Die Durchführung von Zuverlässigkeitsüberprüfungen durch die Polizei nach Maßgabe anderer Vorschriften bleibt unberührt.

Abschnitt 4

Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 52

Auftragsverarbeitung

(1) Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

(3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen.

(4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon auf Grund anderer Vorschriften verbindlich sind. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(5) Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren,
2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten,
4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht,
5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 63 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt,
6. Überprüfungen, die von dem Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt,
7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält,
8. alle gemäß § 54 erforderlichen Maßnahmen ergreift und
9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 54 bis 58 und 60 bis 61 genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Absatzes 5 ist schriftlich oder elektronisch abzufassen.

(7) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

§ 53

Gemeinsam Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam Verantwortliche. Gemeinsam Verantwortliche haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können. Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

§ 54

Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Imple-

mentierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Höhe des Risikos soll anhand einer objektiven Beurteilung festgestellt werden, bei der die Eintrittswahrscheinlichkeit und Schwere der Verletzung nach der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung bestimmt werden.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Nummern 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 55
Verzeichnis von Verarbeitungstätigkeit

(1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie die Kontaktdaten der oder des Datenschutzbeauftragten,
2. die Zwecke der Verarbeitung,
3. die Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
5. gegebenenfalls die Verwendung von Profiling,
6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
7. Angaben über die Rechtsgrundlage der Verarbeitung,
8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
9. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 54.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt, das Folgendes zu enthalten hat:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls die Kontaktdaten der oder des Datenschutzbeauftragten,
2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates oder der Organisation und
3. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 54.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch zu führen.

(4) Verantwortliche und Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zur Verfügung zu stellen.

§ 56

Technikgestaltung und datenschutzfreundliche Voreinstellung

(1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Er hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

(2) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

§ 57

Datenschutz-Folgeabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, auf Grund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. § 54 Absatz 1 Satz 2 gilt entsprechend.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche hat die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Durchführung der Datenschutz-Folgenabschätzung zu beteiligen.

(4) Die Datenschutz-Folgenabschätzung hat den Rechten und den berechtigten Interessen der von der Verarbeitung betroffenen Personen und sonstiger Betroffener Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

(5) Soweit erforderlich, hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben.

§ 58

Anhörung der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 57 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.

Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur vorherigen Anhörung nach Satz 1 unterliegen. § 54 Absatz 1 Satz 2 gilt entsprechend.

(2) Der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit sind im Fall des Absatzes 1 vorzulegen:

1. die nach § 57 durchgeführte Datenschutz-Folgenabschätzung,
2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,
3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,
4. Angaben zu den zum Schutz der Rechte und Freiheiten der betroffenen Personen vorgesehenen Maßnahmen und Garantien und
5. die Kontaktdaten der oder des Datenschutzbeauftragten.

Auf Anfrage sind der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Risiken und die diesbezüglichen Garantien bewerten zu können.

(3) Falls die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergrif-

fen werden sollten. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders schwierig ist. Sie oder er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zusammen mit den Gründen für die Verzögerung zu informieren.

(4) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 3 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit im Nachhinein zu berücksichtigen und ist die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

§ 59

Berichtigung, Löschung und Einschränkung der Verarbeitung

(1) Personenbezogene Daten sind unverzüglich zu berichtigen, wenn sie unrichtig sind. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Beurteilung, sondern die Tatsache, dass die Aussage oder Beurteilung so erfolgt ist. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. Sind Daten in nichtautomatisierten Dateien oder in Akten zu berichtigen, reicht es aus, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind.

(2) In Dateisystemen suchfähig gespeicherte personenbezogene Daten sind zu löschen und die dazugehörigen, zu den Personen suchfähig angelegten Akten sind zu vernichten, wenn

1. dies durch dieses Gesetz bestimmt ist,
2. ihre Speicherung unzulässig ist oder
3. bei der zu bestimmten Fristen oder Terminen vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

In Dateisystemen nicht suchfähig gespeicherte Daten sind unter den Voraussetzungen von Satz 1 Nummern 1 bis 3 zu löschen, soweit die Speicherung festgestellt wird. Andere als die in Satz 1 genannten Akten sind nach Ablauf der jeweiligen Aufbewahrungsfrist oder bei unzulässiger Speicherung aller in ihnen enthaltenen Daten zu vernichten.

(3) Die Vernichtung von Akten ist bei Vorliegen der Voraussetzungen nach Absatz 2 Satz 1 Nummer 3 nur durchzuführen, wenn die gesamte Akte für die Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn, dass der Betroffene die Vernichtung von Teilen der Akte verlangt und die weitere Speicherung ihn in unangemessener Weise beeinträchtigt. Soweit hiernach eine Vernichtung nicht in Betracht kommt, tritt an die Stelle der Vernichtung eine Einschränkung der Verarbeitung.

(4) Anstatt die personenbezogenen Daten zu löschen oder zu vernichten, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass dadurch schutzwürdige Interessen der betroffenen Person beeinträchtigt würden,
2. die Daten, in einem Verfahren, das den Anlass der Erhebung oder weiteren Verarbeitung dieser Daten betrifft, zu Beweiszwecken weiter aufbewahrt werden müssen,
3. die Nutzung der Daten für ein bestimmtes Forschungsvorhaben erforderlich ist,
4. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist,
5. die Daten für die Zwecke eines parlamentarischen Untersuchungsausschusses erforderlich sind.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu den in Satz 1 genannten Zwecken oder sonst mit Einwilligung des Betroffenen genutzt werden.

(5) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(6) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken. Stellt der Verantwortliche fest, dass unrichtige oder nach Absatz 2 Satz 1 Nummer 2 zu löschende Daten übermittelt worden sind, ist dem Empfänger die Berichtigung oder Löschung mitzuteilen, es sei denn, dass die Mitteilung für die Beurteilung der Person oder des Sachverhaltes nicht oder nicht mehr wesentlich ist.

(7) Anstelle der Löschung und Vernichtung in den Fällen des Absatzes 2 Satz 1 Nummer 3 können die Datenträger an das zuständige staatliche Archiv abgegeben werden, soweit archivrechtliche Regelungen dies vorsehen.

§ 60

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

(1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zu melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit nicht innerhalb von 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. § 54 Absatz 1 Satz 2 gilt entsprechend.

(2) Der Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden.

(3) Die Meldung nach Absatz 1 hat zumindest folgende Informationen zu enthalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,

2. den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Stelle für weitere Informationen,
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und
4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, hat der Verantwortliche sie unverzüglich nachzureichen, sobald sie ihm vorliegen.

(5) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Absatz 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

§ 61

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen. § 54 Absatz 1 Satz 2 gilt entsprechend.

(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 60 Absatz 3 Nummern 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.

(3) Die Benachrichtigung der betroffenen Person nach Absatz 1 ist nicht erforderlich, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht werden,
2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen im Sinne des Absatz 1 nicht mehr besteht, oder
3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verlangen, dies nachzuholen oder verbindlich feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind. Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko im Sinne von Absatz 1 führt.

(5) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in § 68 Absatz 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person auf Grund des von der Verletzung ausgehenden hohen Risikos im Sinne von Absatz 1 überwiegen.

§ 62

Automatisierte Dateisysteme und Verfahren, Datenverbund

(1) Die Einrichtung automatisierter Dateisysteme ist nur zulässig, wenn das öffentliche Interesse an der Einrichtung gegenüber möglichen Gefahren für schutzwürdige Belange der Betroffenen überwiegt. Durch die Automatisierung darf keine unangemessene Verkürzung oder Verzerrung des Sachverhalts entstehen. Durch geeignete technische und organisatorische Maßnahmen ist insbesondere sicherzustellen, dass der Abruf der Daten nur den Bediensteten möglich ist, die hierfür im Einzelfall zuständig sind. Neben den nach § 54 Absatz 3 zu treffenden Maßnahmen zur Datensicherung sind Maßnahmen zu treffen, die eine stichprobenweise Kontrolle der Zulässigkeit der Abrufe ermöglichen, soweit der damit verbundene Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht.

(2) Für die Einrichtung eines Verfahrens, das der Polizei den automatisierten Abruf personenbezogener Daten aus einem von einer anderen öffentlichen Stelle geführten Dateisystem ermöglicht, gelten die Vorgaben des § 53, soweit die Polizei und die andere öffentliche Stelle gemeinsam Verantwortliche im Sinne des § 53 Satz 1 sind.

(3) Die zuständige Behörde darf zur Erfüllung von Aufgaben, die nicht nur örtliche Bedeutung haben, mit anderen Ländern und dem Bund einen Datenverbund vereinbaren, der eine automatisierte Datenübermittlung ermöglicht. In der Vereinbarung ist auch festzulegen, welcher Behörde die nach diesem Gesetz oder nach anderen Rechtsvorschriften bestehenden Pflichten einer speichernden Stelle obliegen. § 53 gilt entsprechend.

§ 63

Protokollierung in automatisierten Dateisystemen und Verfahren

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,
2. Veränderung,
3. Abfrage,
4. Offenlegung einschließlich Übermittlung,
5. Kombination und
6. Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die

personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokolldaten dürfen nur für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung, durch eine dazu befugte öffentliche Stelle, sowie für die Eigenüberwachung, der Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren verwendet werden. Die Protokolldaten sind am Ende des auf die Generierung folgenden Jahres zu löschen, es sei denn, dass sie für den in Satz 1 genannten Zweck noch erforderlich sind.

(4) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit auf Anforderung zur Verfügung zu stellen.

§ 64

Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen

(1) Bei der Erhebung von Daten nach den §§ 20 bis 31 und 50 sind zu protokollieren:

1. das zur Datenerhebung eingesetzte Mittel,
2. der Zeitpunkt des Einsatzes,
3. Angaben, die die Feststellung der erhobenen Daten ermöglichen, sowie
4. die Organisationseinheit, die die Maßnahme durchführt.

(2) Zu protokollieren sind auch

1. bei Maßnahmen nach § 20 Absatz 1 und § 21 Absatz 1 die Zielperson sowie die erheblich mitbetroffenen Personen,
2. bei Maßnahmen nach § 22
   a) die Person, gegen die sich die Maßnahme richtete,
   b) sonstige überwachte Personen sowie
   c) Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,
3. bei Maßnahmen nach § 23 die Beteiligten der überwachten Telekommunikation,
4. bei Maßnahmen nach § 24 die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
5. bei Maßnahmen nach § 25 die Beteiligten der betroffenen Telekommunikation,
6. bei Maßnahmen nach § 25 Absatz 3 die Zielperson,
7. bei Maßnahmen nach § 27 die betroffene Person,
8. bei Maßnahmen nach §§ 28 und 29
   a) die Zielperson,
   b) die erheblich mitbetroffene Person,
   c) die Personen, deren nicht allgemein zugängliche Wohnung die Vertrauensperson oder der Verdeckte Ermittler betreten hat,
9. bei Maßnahmen nach § 31 die Zielperson und die Personen, deren personenbezogene Daten gemeldet worden sind,
10. bei Maßnahmen nach § 50
    a) die im Übermittlungsersuchen nach § 50 Absatz 2 enthaltenen Merkmale sowie
    b) die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden.

(3) Nachforschungen zur Feststellung der Identität einer in Absatz 2 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Die Zahl der Personen, deren Protokollierung unterblieben ist, ist im Protokoll anzugeben.

(4) Die Protokolldaten dürfen nur verwendet werden für Zwecke der Benachrichtigung und um der betroffenen Person oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahmen rechtmäßig durchgeführt worden sind. Sie sind bis zum Abschluss der Kontrolle nach § 73 aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 1 genannten Zweck noch erforderlich sind.

§ 65

Kennzeichnung bei verdeckten und eingriffsintensiven Maßnahmen

(1) Die nach den §§ 20 bis 31 und 50 erhobenen personenbezogenen Daten sind unter Angabe des eingesetzten Mittels oder der eingesetzten Methode oder Maßnahme zu kennzeichnen. Die Kennzeichnung kann durch Angabe der Rechtsgrundlage ergänzt werden. Personenbezogene Daten, die nicht entsprechend den Anforderungen des Satzes 1 gekennzeichnet sind, dürfen solange nicht weiterverarbeitet oder übermittelt werden, bis eine Kennzeichnung entsprechend den Anforderungen des Satzes 1 erfolgt ist.

(2) Bei einer Übermittlung an eine andere Stelle ist die empfangende Stelle darauf hinzuweisen, dass die Kennzeichnung nach Absatz 1 Satz 1 aufrechtzuerhalten ist.

Abschnitt 5

Rechte der betroffenen Person

§ 66

Verfahren der Kommunikation mit Betroffenen

(1) Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwenden.

(2) Die Benachrichtigungen nach den §§ 61 und 68 und die Bearbeitung von Anträgen nach den §§ 69 und 70 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 69 und 70 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, auf Grund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(3) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach § 69 oder § 70 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 67

Allgemeine Informationen zur Datenverarbeitung

Die Polizei hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke, zu denen personenbezogene Daten verarbeitet werden,
2. die Rechte auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten,
3. die Kontaktdaten des Verantwortlichen und die Kontaktdaten der oder des behördlichen Datenschutzbeauftragten,
4. das Recht, die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit anzurufen und
5. die Kontaktdaten der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

§ 68

Benachrichtigung betroffener Personen

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender Daten nach diesem Gesetz vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. allgemeine Informationen zur Datenverarbeitung:
   a) die Zwecke der von dem Verantwortlichen vorgenommenen Verarbeitungen,
   b) die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,
   c) den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten,
   d) das Recht, die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit anzurufen und
   e) die Erreichbarkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit,
2. die Rechtsgrundlage der Verarbeitung,
3. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie
5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer betroffenen Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen ist und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer betroffenen Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(2) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, des Bestandes des Staates, von Leib, Leben oder Freiheit einer Person möglich ist. Im Falle der §§ 28 und 29 erfolgt die Benachrichtigung erst, sobald dies auch ohne Gefährdung der Möglichkeit der weiteren Verwendung der Vertrauensperson oder des Verdeckten Ermittlers möglich ist. Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren eingeleitet worden, erfolgt die Benachrichtigung in Abstimmung mit der Staatsanwaltschaft, sobald dies der Stand des Ermittlungsverfahrens zulässt. Wird die Benachrichtigung aus einem der vorgenannten Gründe zurückgestellt, ist dies zu dokumentieren.

(3) Erfolgt nach Beendigung einer Maßnahme die Benachrichtigung nicht innerhalb von zwölf Monaten, bedarf die weitere Zurückstellung der Benachrichtigung der gerichtlichen Zustimmung. Im Falle der §§ 22 und 25 beträgt die Frist sechs Monate. Über die Zurückstellung entscheidet das Gericht, das für die Anordnung der Maßnahme zuständig gewesen ist. Im Falle einer erstmaligen gerichtlichen Befassung gilt § 20 Absatz 2 Sätze 5 bis 9 entsprechend. Das Gericht bestimmt die Dauer der weiteren Zurückstellung, im Falle der §§ 22 und 25 jedoch nicht länger als sechs Monate. Fünf Jahre nach Beendigung der Maßnahme kann mit gerichtlicher Zustimmung endgültig von der Benachrichtigung abgesehen werden, wenn

1. die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden,
2. die Voraussetzungen für eine Löschung sowohl bei der Polizei als auch bei den Empfängern von Datenübermittlungen vorliegen und
3. die Daten gelöscht wurden.

(4) Bezieht sich die Benachrichtigung auf die Herkunft von oder die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

§ 69

Auskunftsrecht

(1) Der betroffenen Person ist auf Antrag Auskunft darüber zu erteilen, ob sie betreffende Daten verarbeitet werden. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind und die Kategorie zu der sie gehören,
2. die verfügbaren Informationen über die Herkunft der Daten sowie
3. die in § 68 Absatz 1 Satz 1 genannten Angaben.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder die ausschließlich Zwecken der Datensicherung, der Datenschutzkontrolle oder der Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Bei nicht automatisiert suchfähig verarbeiteten Daten kann von der Auskunftserteilung abgesehen werden, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand insoweit außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Statt einer Auskunft über personenbezogene Daten kann der betroffenen Person Akteneinsicht gewährt werden.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 68 Absatz 2 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 2 teilweise oder vollständig einschränken.

(5) Bezieht sich die Auskunftserteilung auf die Herkunft von oder die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) Der Verantwortliche hat die betroffene Person über das Absehen von einer Auskunft oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, soweit bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 68 Absatz 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

(7) Wird die betroffene Person nach Absatz 6 über das Absehen von einer Auskunft oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit anrufen oder gerichtlichen Rechtsschutz suchen kann. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat die betroffene Person darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie oder ihn stattgefunden hat. Die Mitteilung der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(8) Der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

§ 70

Recht auf Berichtigung, Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Beurteilung, sondern die Tatsache, dass die Aussage oder Beurteilung so erfolgt ist. Tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) In den Fällen des § 59 Absatz 2 hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen.

(3) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 68 Absatz 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.

(4) § 69 Absätze 7 und 8 gilt entsprechend.

(5) In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 und 2 hat der Verantwortliche anderen Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen.

§ 71

Recht auf Schadensersatz und Entschädigung

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist. Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise sein Rechtsträger.

(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

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

(4) Weitergehende sonstige Schadenersatzansprüche bleiben unberührt.

Abschnitt 6

Die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

§ 72

Befugnisse

(1) Stellt die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit bei Datenverarbeitungen durch die Polizei, deren Auftragsdatenverarbeiter oder die Stellen, auf die die Polizei ihre Aufgaben ganz oder teilweise übertragen hat, Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies und fordert innerhalb einer von ihr oder ihm zu bestimmenden Frist zur Stellungnahme auf. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn die Mängel von geringer Bedeutung sind, bereits behoben sind oder ihre Behebung sichergestellt ist. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung der oder des Hamburgischen Beauftragten für Daten-

schutz und Informationsfreiheit getroffen worden sind. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kann die Polizei auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen. Sofern die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Verstöße gemäß Satz 1 beanstandet hat und der Verstoß nach der Stellungnahme fortbesteht, kann sie oder er das Vorliegen eines von ihr oder ihm beanstandeten Verstoßes gegen datenschutzrechtliche Vorschriften gerichtlich feststellen lassen.

(2) Stellt die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit einen strafbewehrten Verstoß gegen dieses Gesetz oder gegen andere Vorschriften des Datenschutzes fest, ist sie oder er befugt, diesen zur Anzeige zu bringen.

(3) Die Polizei, ihre Auftragsdatenverarbeiter und die Stellen, auf die die Polizei ihre Aufgaben ganz oder teilweise übertragen hat, sind verpflichtet, der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

1. jederzeit Zugang zu den Grundstücken und Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer oder seiner Aufgaben notwendig sind, zu gewähren und
2. alle Informationen, die für die Erfüllung ihrer oder seiner Aufgaben erforderlich sind, bereitzustellen.

§ 73

Besondere Kontrollpflichten

Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kontrolliert die Einhaltung der gesetzlichen Vorschriften über die Verarbeitung von personenbezogenen Daten nach den §§ 20 bis 31 und 50 im Abstand von höchstens zwei Jahren.

§ 74

Zusammenarbeit

Der Verantwortliche und der Auftragsverarbeiter haben mit der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

Abschnitt 7

Schlussbestimmungen

§ 75

Berichtspflicht gegenüber der Bürgerschaft

Der Senat unterrichtet die Bürgerschaft jährlich über die nach den §§ 19 bis 30 und 49 angeordneten Maßnahmen sowie über Übermittlungen nach § 45. Der Senat berichtet auch, wenn keine Maßnahmen durchgeführt worden sind. Über den nach § 22 Absatz 1 und soweit richterlich überprüfungsbedürftig, nach § 22 Absatz 8 erfolgten Einsatz technischer Mittel übt ein von der Bürgerschaft gewähltes Gremium auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. Dieses Gremium besteht aus sieben Mitgliedern der Bürgerschaft. Sie werden in geheimer Abstimmung gewählt.

§ 76

Strafvorschriften

(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 verarbeitet 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. 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.

(5) Eine Meldung von Verletzungen des Schutzes personenbezogener Daten an die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit nach § 60 oder eine Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffene Person nach § 61 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 77

Einschränkung von Grundrechten

Durch dieses Gesetz werden die Grundrechte auf Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes), auf Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) und des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) eingeschränkt.

§ 78

Übergangsbestimmungen

(1) Abweichend von § 65 dürfen personenbezogene Daten auch ohne eine dort vorgesehene Kennzeichnung nach dem 23. Dezember 2019 für die betreffenden Dateien und automatisierten Verfahren geltenden Errichtungsanordnungen weiterverarbeitet, insbesondere übermittelt werden.

(2) Protokollierungen im Sinne von § 63 Absatz 1 müssen bei vor dem 6. Mai 2018 eingerichteten, automatisierten Verarbeitungssystemen erst bis zum 6. Mai 2023 erfolgen, wenn andernfalls ein unverhältnismäßiger Aufwand entstünde. Die Anwendung von Satz 1 ist zu begründen und zu dokumentieren.

(3) Der Turnus für Prüfungen nach § 73 und Unterrichtungen nach § 75 beginnt erstmals am 1. Januar 2022. Bis zu diesem Zeitpunkt finden § 10a Absatz 9 sowie § 10e Absatz 7 des Gesetzes über die Datenverarbeitung der Polizei vom 2. Mai 1991 (HmbGVBl. S. 187, 191) in der am 23. Dezember 2019 geltenden Fassung sinngemäß Anwendung.

Artikel 2

Elftes Gesetz zur Änderung des Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung

Das Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung vom 14. März 1966 (HmbGVBl. S. 77), zuletzt geändert 8. Dezember 2016 (HmbGVBl. S. 514), wird wie folgt geändert:

1. In der Inhaltsübersicht wird hinter dem Eintrag zu § 11 folgender Eintrag eingefügt:

   „§ 11a Meldeauflage“.

2. Hinter § 11 wird folgender § 11a eingefügt:

   „§ 11a

   Meldeauflage

   Zur Verhütung von Straftaten kann einer Person aufgegeben werden, sich an bestimmten Tagen zu bestimmten Zeiten bei einer bestimmten Polizeidienststelle zu melden, wenn Tatsachen die Annahme rechtfertigen, dass diese Person eine Straftat begehen wird und die Maßnahme zur Verhütung dieser Straftat erforderlich ist. Die Anordnung bedarf der Schriftform und ist auf höchstens sechs Monate zu befristen. Verlängerungen sind zulässig, sofern die Voraussetzungen weiterhin vorliegen.“

2a. In § 12b Absatz 2 wird hinter Satz 2 folgender Satz eingefügt:

   „Verlängerungen sind zulässig, sofern die Voraussetzungen weiterhin vorliegen.“

2b. In § 13b Absatz 4 wird die Textstelle „§§ 171, 173 bis 175 und § 178 Absatz 3“ durch die Textstelle „§§ 171, 171a, 173 bis 175 und § 178 Absatz 2“ ersetzt.

3. In § 15 Absatz 1 Nummer 3 wird der Punkt am Ende durch das Wort „oder“ ersetzt und folgende Nummer 4 angefügt:

   „4. sie zur gezielten Kontrolle nach § 31 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) vom 12. Dezember 2019 (HmbGVBl. S. 485) in der jeweils geltenden Fassung oder einer vergleichbaren Rechtsvorschrift ausgeschrieben ist.“

4. § 15a Absatz 1 Satz 1 wird wie folgt geändert:

   a) In Nummer 7 wird das Wort „oder“ am Ende durch ein Komma ersetzt.

   b) In Nummer 8 wird der Punkt am Ende durch das Wort „oder“ ersetzt und folgende Nummer 9 angefügt:

      „9. sie von einer Person mitgeführt wird, die zur gezielten Kontrolle nach § 31 PolDVG oder einer vergleichbaren Rechtsvorschrift ausgeschrieben ist, oder es sich um ein derart ausgeschriebenes Kraftfahrzeug handelt; im Falle einer Ausschreibung des Kraftfahrzeugs kann sich die Durchsuchung auch auf die in oder an dem Fahrzeug enthaltenen Sachen erstrecken.“

5. § 23 wird wie folgt geändert:

   a) Der Wortlaut wird Absatz 1.

   b) Folgender Absatz 2 wird angefügt:

      „(2) Durch die Polizei ist eine Fixierung sämtlicher Gliedmaßen einer Person nur zulässig, wenn dies zur Abwehr einer gegenwärtigen erheblichen Gefahr einer Selbsttötung, Selbstverletzung oder von Angriffen gegen eine andere Person unerlässlich ist. Eine nicht nur kurzfristige Fixierung im Sinne von Satz 1 bedarf der gerichtlichen Anordnung. Bei Gefahr im Verzug können die Leitung der zuständigen Polizeidienststelle, die Vertretung im Amt oder, wenn deren Entscheidung nicht rechtzeitig eingeholt werden kann, andere Polizeivollzugsbeamte die Maßnahme nach Satz 2 vorläufig anordnen; eine richterliche Bestätigung ist unverzüglich herbeizuführen. Einer solchen bedarf es nicht, wenn anzunehmen ist, dass die Entscheidung erst nach Wegfall des Grundes der Maßnahme ergehen würde oder die Maßnahme vor Herbeiführung der Entscheidung tatsächlich beendet und auch keine Wiederholung zu erwarten ist. Während der Maßnahme ist die betroffene Person fortlaufend durch einen für die Überwachung von Fixierungen geschulten Bediensteten zu überwachen. Nach Beendigung der Maßnahme ist die betroffene Person unverzüglich auf ihr Recht hinzuweisen, die Rechtmäßigkeit der Maßnahme gerichtlich überprüfen zu lassen. Die Maßnahme ist zu dokumentieren; diese Dokumentation beinhaltet:

      1. die Anordnung und die dafür maßgeblichen Gründe,
      2. den Verlauf,
      3. die Dauer,
      4. die Art der Überwachung,
      5. die Beendigung und
      6. den Hinweis nach Satz 6.

      § 13a Absatz 2 gilt entsprechend.“

6. In § 30a Absatz 1 Satz 1 wird hinter dem Wort „Landes“ die Textstelle „und Beamte der Zollverwaltung, denen der Gebrauch von Schusswaffen bei Anwendung des unmittelbaren Zwangs bei Ausübung öffentlicher Gewalt gestattet ist,“ eingefügt.

Artikel 3

Änderung des Hafensicherheitsgesetzes

§ 2 Absatz 1 Satz 2 des Hafensicherheitsgesetzes vom 6. Oktober 2005 (HmbGVBl. S. 424), zuletzt geändert am 18. Mai 2018 (HmbGVBl. S. 182, 183), erhält folgende Fassung: „§ 13 Absatz 3, Absatz 4 Satz 1 und Absatz 4 Satz 2 Nummern 1 bis 6 und Absatz 4 Satz 3 des Gesetzes über die Datenverarbeitung der Polizei vom 12. Dezember 2019 (HmbGVBl. S. 485) gilt entsprechend.“

Artikel 4

Änderung des Hamburgischen Verfassungsschutzgesetzes

Das Hamburgische Verfassungsschutzgesetz vom 7. März 1995 (HmbGVBl. S. 45), zuletzt geändert am 19. Juni 2013 (HmbGVBl. S. 293), wird wie folgt geändert:

1. In § 14 Absatz 2 Satz 2 wird die Textstelle „§§ 9 bis 12 und § 23 Gesetz über die Datenverarbeitung der Polizei vom 2. Mai 1991 (HmbGVBl. S. 187, 191), zuletzt geändert am 30. Mai 2012 (HmbGVBl. S. 204),“ durch die Textstelle „§§ 20 bis 29 und 50 des Gesetzes über die Datenverarbeitung der Polizei vom 12. Dezember 2019 (HmbGVBl. S. 485)“ ersetzt.

2. In 19 Absatz 4 Satz 3 wird die Textstelle „§ 2 Absatz 3 Satz 3 oder nach den §§ 9 bis 12“ durch die Textstelle „§ 10 Absatz 3 Satz 3 oder nach den §§ 20 bis 29“ ersetzt.

Artikel 5

Außerkrafttreten

Das Gesetz über die Datenverarbeitung der Polizei vom 2. Mai 1991 (HmbGVBl. S. 187, 191) in der geltenden Fassung wird aufgehoben.

Ausgefertigt Hamburg, den 12. Dezember 2019.

Der Senat

Elfte Verordnung zur Änderung der Gebührenordnung für die Feuerwehr

Vom 17. Dezember 2019

Auf Grund von § 31 Absatz 3 in Verbindung mit § 18 Absatz 1 des Hamburgischen Rettungsdienstgesetzes vom 30. Oktober 2019 (HmbGVBl. S. 367) wird verordnet:

§ 1

Änderung der Gebührenordnung für die Feuerwehr

Die Nummern 4.1 bis 4.9 der Anlage der Gebührenordnung für die Feuerwehr vom 2. Dezember 1997 (HmbGVBl. S. 530), zuletzt geändert am 3. Dezember 2019 (HmbGVBl. S. 448, 452), werden durch folgende Nummern 4.1 bis 4.8 ersetzt:

„4.1	Notfallbeförderung mit einem Rettungswagen, Babynotarztwagen, Infektionsrettungswagen oder Großrettungswagen	534,—
4.2	Einsatz eines Rettungswagens, Babynotarztwagens, Infektionsrettungswagens oder Großrettungswagens ohne Beförderung	448,—
4.3	Einsatz eines Notarzteinsatzfahrzeuges oder arztbesetzen Rettungsmittels	
4.3.1	Einsatz eines Notarzteinsatzfahrzeuges	380,—
4.3.2	Einsatz eines Notarzteinsatzfahrzeuges mit Behandlung durch eine Notärztin oder einen Notarzt	430,—
4.3.3	Einsatz eines Notarzteinsatzfahrzeuges mit Behandlung und Begleitung durch eine Notärztin oder einen Notarzt	541,—
4.3.4	Einsatz eines Notarztwagens mit Behandlung und Begleitung durch eine Notärztin oder einen Notarzt	602,—
4.4	Krankenbeförderung innerhalb Hamburgs	579,—
4.5	Frei aus redaktionellen Gründen	
4.6	Alleinige Beförderung von Blutkonserven, Arzneimitteln, Sauerstoffflaschen oder anderen dem Gesundheitsdienst dienenden Gegenständen sowie alleinige Beförderung von medizinischem Personal oder Blutspendern innerhalb Hamburgs	160,—
4.7	Einsätze gemäß den Nummern 4.1 bis 4.6 von Hamburg nach außerhalb und umgekehrt	
4.7.1	für die ersten 20 km	Gebühr nach Nummern 4.1 bis 4.6
4.7.2	für jeden weiteren Kilometer . .	3,55
4.8	Einfache Hilfeleistungen im Rahmen eines Rettungsdiensteinsatzes (Tragehilfe) ohne den Einsatz von technischem Gerät	195,—“.

§ 2

Inkrafttreten

Diese Verordnung tritt am 1. Januar 2020 in Kraft.

Gegeben in der Versammlung des Senats,

Hamburg, den 17. Dezember 2019.

Viertes Gesetz zur Neuregelung des Glücksspielwesens

Vom 19. Dezember 2019

Der Senat verkündet das nachstehende von der Bürgerschaft beschlossene Gesetz:

Artikel 1

Gesetz zum Dritten Glücksspieländerungsstaatsvertrag

§ 1

Dem vom 26. März bis 18. April 2019 unterzeichneten Dritten Glücksspieländerungsstaatsvertrag wird zugestimmt.

§ 2

Der Staatsvertrag wird nachstehend mit Gesetzeskraft veröffentlicht.

§ 3

Der Tag, an dem der Staatsvertrag nach seinem Artikel 2 Absatz 1 Satz 1 in Kraft tritt, ist im Hamburgischen Gesetz- und Verordnungsblatt bekannt zu geben.

§ 4

Ist der Staatsvertrag nach seinem Artikel 2 Absatz 1 Satz 2 gegenstandslos, ist dies bis zum 1. Februar 2020 im Hamburgischen Gesetz- und Verordnungsblatt bekannt zu geben.

Artikel 2

Änderung des Hamburgischen Glücksspieländerungsstaatsvertrags-Ausführungsgesetzes

Das Hamburgische Glücksspieländerungsstaatsvertrags-Ausführungsgesetz vom 29. Juni 2012 (HmbGVBl. S. 235), geändert am 12. Dezember 2017 (HmbGVBl. S. 386), wird wie folgt geändert:

1. § 8 wird wie folgt geändert:

1.1 In Absatz 1 Satz 2 wird die Textstelle „§ 10a Absatz 5 Satz 2 GlüStV“ durch die Textstelle „§ 10a Absatz 4 Satz 2 GlüStV“ ersetzt.

1.2 Absatz 9 wird wie folgt geändert:

1.2.1 Satz 1 wird wie folgt geändert:

a) Nummern 1 bis 3 werden durch folgende Nummer 1 ersetzt:

„1. die Abgabe, der Konsum oder Verkauf von Speisen und Getränken für den Verzehr an Ort und Stelle sowie außer Haus und“.

b) Nummer 4 wird Nummer 2.

1.2.2 In Satz 2 Nummer 4 wird die Textstelle „vom 9. September 1998 (BGBl. I S. 2777), zuletzt geändert am 17. Juli 2017 (BGBl. I S. 2446, 2491, 2492, 2493),“ durch die Textstelle „in der Fassung vom 9. September 1998 (BGBl. I S. 2777), zuletzt geändert am 25. März 2019 (BGBl. I S. 357, 359), in der jeweils geltenden Fassung“ ersetzt.

1.3 Absatz 11 wird aufgehoben.

1.4 Absatz 12 wird Absatz 11 und wie folgt geändert:

1.4.1 In Satz 1 wird die Textstelle „30. April 2018“ durch die Textstelle „31. Mai 2020“ und die Bezeichnung „Absatz 13“ durch die Bezeichnung „Absatz 12“ ersetzt.

1.4.2 In Satz 2 wird die Textstelle „30. April 2018“ durch die Textstelle „31. Mai 2020“ und die Bezeichnung „Absatz 13“ durch die Bezeichnung „Absatz 12“ ersetzt.

1.5 Absatz 13 wird Absatz 12 und wie folgt geändert:

1.5.1 In Satz 1 wird die Zahl „12“ durch die Zahl „11“ ersetzt.

1.5.2 Satz 6 wird gestrichen.

2. § 12 wird wie folgt geändert:

2.1 In Absatz 1 Satz 3 wird die Textstelle „§ 8 Absatz 2“ durch die Textstelle „§ 8 Absatz 2 GlüStV“ ersetzt.

2.2 In Absatz 3 Satz 2 werden die Wörter „sowie einverstanden ist“ durch die Wörter „ist sowie eingewilligt hat“ ersetzt.

2.3 Absatz 5 erhält folgende Fassung:

„(5) Verantwortliche im Sinne des Datenschutzes für die in Absätze 1 bis 4 geregelte Verarbeitung sind außer der zuständigen Behörde nach § 23 Absatz 1 Satz 1 GlüStV auch diejenigen Stellen, welche die Sperre ausgesprochen oder den Antrag auf Selbstsperre entgegengenommen haben oder Sperrvermerke gemäß Absatz 3 Satz 2 abfragen, soweit sie allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheiden.“

2.4 In Absatz 7 wird folgender Satz angefügt:

„Die Auskunftsrechte nach Artikel 15 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 2016 Nr. L 119 S. 1, L 314 S. 72, 2018 Nr. L 127 S. 2) bleiben hiervon unberührt.“

3. § 18 Absatz 1 wird wie folgt geändert:

3.1 Hinter Nummer 2 wird folgende neue Nummer 3 eingefügt:

„3. entgegen § 5 Absatz 5 GlüStV für unerlaubtes Glücksspiel wirbt,“.

3.2 Die bisherigen Nummern 3 bis 6 werden Nummern 4 bis 7.

3.3 In Nummer 7 wird der Punkt am Ende durch ein Komma ersetzt und folgende Nummer 8 angefügt:

„8. beim Betrieb einer Wettvermittlungsstelle gegen die Vorgaben des § 8 Absätze 7 bis 10 Satz 3 verstößt.“

Artikel 3

Änderung des Feiertagsgesetzes

§ 2a Satz 3 des Feiertagsgesetzes vom 16. Oktober 1953 (Sammlung des bereinigten hamburgischen Landesrechts I 113-a), zuletzt geändert am 12. März 2018 (HmbGVBl. S. 63), wird gestrichen.

Artikel 4

Inkrafttreten

Artikel 1 tritt am Tage nach der Verkündung in Kraft. Im Übrigen tritt dieses Gesetz am 1. Januar 2020 in Kraft.

Ausgefertigt Hamburg, den 19. Dezember 2019.

Der Senat

Dritter Staatsvertrag zur Änderung des Staatsvertrages zum Glücksspielwesen in Deutschland (Dritter Glücksspieländerungsstaatsvertrag – 3. GlüÄndStV)

Das Land Baden-Württemberg,
der Freistaat Bayern,
das Land Berlin,
das Land Brandenburg,
die Freie Hansestadt Bremen,
die Freie und Hansestadt Hamburg,
das Land Hessen,
das Land Mecklenburg-Vorpommern,
das Land Niedersachsen,
das Land Nordrhein-Westfalen,
das Land Rheinland-Pfalz,
das Saarland,
der Freistaat Sachsen,
das Land Sachsen-Anhalt,
das Land Schleswig-Holstein und
der Freistaat Thüringen
(im Folgenden: die Länder genannt)

schließen nachstehenden Staatsvertrag:

Artikel 1

Änderung des Glücksspielstaatsvertrages

Der Staatsvertrag zum Glücksspielwesen in Deutschland in der Fassung des Ersten Staatsvertrages zur Änderung des Staatsvertrages zum Glücksspielwesen in Deutschland vom 15. Dezember 2011 (Glücksspielstaatsvertrag – GlüStV) wird wie folgt geändert:

1. § 4a wird wie folgt geändert:
   a) In Absatz 1 Satz 1 werden die Wörter „, insbesondere im Rahmen einer zeitlich befristeten Experimentierklausel für Sportwetten," durch die Wörter „im Rahmen der Experimentierklausel für Sportwetten nach § 10a" ersetzt.
   b) In Absatz 2 Satz 1 wird die Angabe „Bekanntmachung (§ 4b Absatz 1)" durch das Wort „Konzession" ersetzt.
   c) Absatz 3 wird wie folgt gefasst:

      „Die Zahl der Konzessionen wird für die Dauer der Experimentierphase nicht beschränkt."
2. § 4b wird wie folgt geändert:
   a) In der Überschrift werden das Komma und das Wort „Auswahlkriterien" gestrichen.
   b) Absatz 1 wird wie folgt geändert:
      aa) In Satz 1 wird das Wort „Auswahlverfahrens" durch das Wort „Verfahrens" ersetzt.
      bb) In Satz 2 werden die Wörter „mit einer angemessenen Frist für die Einreichung von Bewerbungen" gestrichen.
   c) In Absatz 2 Satz 2 werden die Wörter „und die Auswahl nach Absatz 5 ermöglichen" gestrichen.
   d) Absatz 5 wird aufgehoben.
3. In § 5 Absatz 4 Satz 1 wird das Wort „Richtlinien" durch das Wort „Auslegungsrichtlinien" ersetzt.
4. § 9a Absatz 5 Satz 2 wird wie folgt gefasst:

   „Hierbei dient das Glücksspielkollegium den Ländern zur Umsetzung einer gemeinschaftlich auszuübenden Aufsicht der jeweiligen obersten Glücksspielaufsichtsbehörden."
5. § 10a wird wie folgt geändert:
   a) Absatz 1 wird wie folgt geändert:
      aa) In dem bisherigen Satz werden die Wörter „für einen Zeitraum von sieben Jahren ab Inkrafttreten des Ersten Glücksspieländerungsstaatsvertrages" durch die Wörter „bis zum 30. Juni 2021" ersetzt.
      bb) Es wird folgender Satz angefügt:

         „Im Falle einer Fortgeltung des Staatsvertrages nach § 35 Absatz 2 verlängert sich die Frist bis zum 30. Juni 2024."
   b) Absatz 3 wird aufgehoben.
   c) Die Absätze 4 und 5 werden die Absätze 3 und 4.
6. § 29 Absatz 1 Satz 3 wird aufgehoben.

Artikel 2

Inkrafttreten

(1) Dieser Staatsvertrag tritt am 1. Januar 2020 in Kraft. Sind bis zum 31. Dezember 2019 nicht alle Ratifikationsurkunden bei der Staatskanzlei der oder des Vorsitzenden der Ministerpräsidentenkonferenz hinterlegt, wird der Staatsvertrag gegenstandslos.

(2) Die Staatskanzlei der oder des Vorsitzenden der Ministerpräsidentenkonferenz teilt den Ländern die Hinterlegung der Ratifikationsurkunden mit.

Für das Land Baden-Württemberg
Stuttgart, den 3. April 2019
Winfried Kretschmann

Für den Freistaat Bayern
München, den 18. April 2019
Markus Söder

Für das Land Berlin
Berlin, den 26. März 2019
Michael Müller

Für das Land Brandenburg
Potsdam, den 29. März 2019
Dietmar Woidke

Für die Freie Hansestadt Bremen
Bremen, den 26. März 2019
Carsten Sieling

Für die Freie und Hansestadt Hamburg
Hamburg, den 4. April 2019
Peter Tschentscher

Für das Land Hessen
Wiesbaden, den 26. März 2019
Volker Bouffier

Für das Land Mecklenburg-Vorpommern
Schwerin, den 26. März 2019
Manuela Schwesig

Für das Land Niedersachsen
Hannover, den 28. März 2019
Stephan Weil

Für das Land Nordrhein-Westfalen
Düsseldorf, den 4. April 2019
Armin Laschet

Für das Land Rheinland-Pfalz
Mainz, den 6. April 2019
Malu Dreyer

Für das Saarland
Saarbrücken, den 5. April 2019
Tobias Hans

Für den Freistaat Sachsen
Dresden, den 30. März 2019
Michael Kretschmer

Für das Land Sachsen-Anhalt
Magdeburg, den 28. März 2019
Reiner Haseloff

Für das Land Schleswig-Holstein
Kiel, den 9. April 2019
Daniel Günther

Für den Freistaat Thüringen
Erfurt, den 28. März 2019
Bodo Ramelow

Herausgegeben von der Justizbehörde der Freien und Hansestadt Hamburg.
Druck, Verlag und Ausgabestelle Lütcke & Wulff, Rondenbarg 8, 22525 Hamburg, — Telefon: 23 51 29-0 — Telefax: 23 51 29 77.
Bestellungen nimmt der Verlag entgegen. Bezugspreis für Teil I und II zusammen jährlich 75,– Euro. Einzelstücke je angefangene vier Seiten 0,26 Euro (Preise einschließlich 7 % Mehrwertsteuer).