ULD

# Datenschutzrecht in Schleswig-Holstein

6. Auflage 2016

- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetz (LDSG)
- Datenschutzverordnung (DSVO)
- Informationszugangsgesetz (IZG-SH)
- Geodatenzugangsgesetz (GeoZG)
- Geodateninfrastrukturgesetz Schleswig-Holstein (GDIG)
- Telemediengesetz (TMG)
- Datenschutzgütesiegelverordnung (DSGSVO)
- Schul-Datenschutzverordnung (Schul-DSVO)

... und andere

Eine Infobroschüre des **ULD**
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Datenschutz und Informationsfreiheit in Schleswig-Holstein
— Gesetze und Ausführungsbestimmungen —

**6. überarbeitete Auflage, Kiel 2016**

Stand 1. August 2016

**Herausgeber:**

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98
24103 Kiel

Telefon: 0431 988-1200
Fax: 0431 988-1223
E-Mail: mail@datenschutzzentrum.de
Internet: www.datenschutzzentrum.de

Umschlaggestaltung: Eyekey Design
Layout und Satz: ULD unter Verwendung von LaTeX
Druck: Schmidt & Klaunig, Kiel

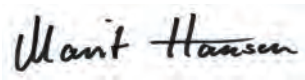
# Vorwort

Datenschutz und Informationsfreiheit sind wichtig für unsere Wissensgesellschaft: der Schutz für jeden Menschen vor einer informationellen Ausbeutung und Überwachung auf der einen Seite und der freie Zugang zu öffentlichen Verwaltungsinformationen auf der anderen Seite. Für beide Themen ist das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein zuständig.

Vordergründig geht es bei „Datenschutz“ nur um den Schutz personenbezogener Daten und bei „Informationsfreiheit“ nur um die Freiheit von Informationen. Dahinter stehen aber die sehr viel größeren Konzepte der Wahrung der Persönlichkeitsrechte und der Fairness mit Blick auf das Machtgefälle zwischen den Datenverarbeitern und den Betroffenen. Denn wer Daten nutzen kann, gewinnt damit an Macht.

Die Rechte der Betroffenen und die Pflichten der Datenverarbeiter sind in Gesetzen und Verordnungen geregelt, die teilweise auf nationaler Ebene (wie das Bundesdatenschutzgesetz) und teilweise auf Landesebene (wie das Landesdatenschutzgesetz Schleswig-Holstein) bestehen. In dieser Veröffentlichung haben wir die wichtigsten Rechtsnormen zu Datenschutz und Informationsfreiheit aufgenommen, die den datenverarbeitenden Stellen aus Wirtschaft und Verwaltung in Schleswig-Holstein als Handwerkszeug dienen sollen.

Die vorliegende Zusammenstellung wird in dieser Form das letzte Mal erscheinen, denn ab Mai 2018 wird die Europäische Datenschutz-Grundverordnung unmittelbare Geltung erlangen. Aus diesem Grund wird sich ein Großteil der abgedruckten Rechtsnormen ändern, und neue Ausführungsbestimmungen werden hinzukommen. Das ULD wird den Text der Grundverordnung sowie der künftig zu ihrer Umsetzung erlassenen Vorschriften ebenfalls zur Verfügung stellen.



Landesbeauftragte für Datenschutz Schleswig-Holstein
Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

# Inhaltsverzeichnis


**Bundesdatenschutzgesetz (BDSG)** **1**

**Landesdatenschutzgesetz (LDSG)** **61**

**Datenschutzverordnung (DSVO)** **89**

**Informationszugangsgesetz (IZG-SH)** **95**

**Geodatenzugangsgesetz (GeoZG)** **105**

**Geodateninfrastrukturgesetz Schleswig-Holstein (GDIG)** **117**

**Telemediengesetz (TMG)** **129**

**§§ 1-3, 88-115 Telekommunikationsgesetz (TKG)** **145**

**§§ 201-206 Strafgesetzbuch (StGB)** **191**

**§ 23 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG)** **199**

**Datenschutzgütesiegelverordnung (DSGSVO)** **201**

**Schul-Datenschutzverordnung (Schul-DSVO)** **205**

# Bundesdatenschutzgesetz (BDSG)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Bundesdatenschutzgesetz |
| **Amtliche Abkürzung:** | BDSG |
| **Ausfertigung:** | Neugefasst durch Bekanntmachung vom 14.01.2003 BGBl. I 2003 S. 66 |
| **Inkrafttreten:** | 01.09.2009 |
| **Letzte Änderung:** | 25.02.2015, BGBl. I S. 162 |

## Inhaltsübersicht


| | | |
|---|---|---|
| **Erster Abschnitt: Allgemeine und gemeinsame Bestimmungen** | | **3** |
| § 1 | Zweck und Anwendungsbereich des Gesetzes | 3 |
| § 2 | Öffentliche und nicht-öffentliche Stellen | 4 |
| § 3 | Weitere Begriffsbestimmungen | 5 |
| § 3a | Datenvermeidung und Datensparsamkeit | 7 |
| § 4 | Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung | 7 |
| § 4a | Einwilligung | 8 |
| § 4b | Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen | 8 |
| § 4c | Ausnahmen | 9 |
| § 4d | Meldepflicht | 10 |
| § 4e | Inhalt der Meldepflicht | 11 |
| § 4f | Beauftragter für den Datenschutz | 12 |
| § 4g | Aufgaben des Beauftragten für den Datenschutz | 13 |
| § 5 | Datengeheimnis | 14 |
| § 6 | Rechte des Betroffenen | 14 |
| § 6a | Automatisierte Einzelentscheidung | 15 |
| § 6b | Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen | 15 |
| § 6c | Mobile personenbezogene Speicher- und Verarbeitungsmedien | 16 |
| § 7 | Schadensersatz | 16 |
| § 8 | Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen | 17 |
| § 9 | Technische und organisatorische Maßnahmen | 17 |
| § 9a | Datenschutzaudit | 17 |

§ 10 Einrichtung automatisierter Abrufverfahren 18
§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag 18
**Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen 20**
§ 12 Anwendungsbereich 20
§ 13 Datenerhebung 21
§ 14 Datenspeicherung, -veränderung und -nutzung 21
§ 15 Datenübermittlung an öffentliche Stellen 23
§ 16 Datenübermittlung an nicht-öffentliche Stellen 24
§ 17 (weggefallen) 25
§ 18 Durchführung des Datenschutzes in der Bundesverwaltung 25
§ 19 Auskunft an den Betroffenen 25
§ 19a Benachrichtigung 26
§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht 27
§ 21 Anrufung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 28
§ 22 Wahl und Unabhängigkeit der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 29
§ 23 Rechtsstellung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 29
§ 24 Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 32
§ 25 Beanstandungen durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 33
§ 26 Weitere Aufgaben der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 33
**Dritter Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen 34**
§ 27 Anwendungsbereich 34
§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke 35
§ 28a Datenübermittlung an Auskunfteien 38
§ 28b Scoring 39
§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung 40
§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form 41
§ 30a Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung 42
§ 31 Besondere Zweckbindung 42
§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses 43
§ 33 Benachrichtigung des Betroffenen 43
§ 34 Auskunft an den Betroffenen 45
§ 35 Berichtigung, Löschung und Sperrung von Daten 47
§ 36 (weggefallen) 49
§ 37 (weggefallen) 49
§ 38 Aufsichtsbehörde 49
§ 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen 51
**Vierter Abschnitt: Sondervorschriften 51**
§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen 51

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen 51
§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien 52
§ 42 Datenschutzbeauftragter der Deutschen Welle 53
§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten 53
**Fünfter Abschnitt: Schlussvorschriften 54**
§ 43 Bußgeldvorschriften 54
§ 44 Strafvorschriften 56
**Sechster Abschnitt: Übergangsvorschriften 57**
§ 45 Laufende Verwendungen 57
§ 46 Weitergeltung von Begriffsbestimmungen 57
§ 47 Übergangsregelung 58
§ 48 Bericht der Bundesregierung 58
**Anlage (zu § 9 Satz 1) 59**

# Erster Abschnitt: Allgemeine und gemeinsame Bestimmungen

## § 1 Zweck und Anwendungsbereich des Gesetzes

(1) [1]Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) [1]Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   (a) Bundesrecht ausführen oder
   (b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) [1]Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. [2]Die Verpflichtung zur Wahrung gesetzlicher

Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) [1]Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) [1]Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. [2]Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. [3]Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. [4]Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. [5]§ 38 Abs. 1 Satz 1 bleibt unberührt.

## § 2 Öffentliche und nicht-öffentliche Stellen

(1) [1]Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. [2]Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) [1]Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) [1]Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

[2]Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) [1]Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. [2]Nimmt eine nicht-öffentliche Stelle ho-

heitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

## § 3 Weitere Begriffsbestimmungen

(1) [1]Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) [1]Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. [2]Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) [1]Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) [1]Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. [2]Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   (a) die Daten an den Dritten weitergegeben werden oder
   (b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) [1]Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) [1]Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) [1]Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) [1]Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) [1]Empfänger ist jede Person oder Stelle, die Daten erhält. [2]Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. [3]Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(9) [1]Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) [1]Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,
2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

(11) [1]Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer,
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

## § 3a Datenvermeidung und Datensparsamkeit

[1]Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. [2]Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

## § 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) [1]Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) [1]Personenbezogene Daten sind beim Betroffenen zu erheben. [2]Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. (a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   (b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

   und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) [1]Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. [2]Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. [3]Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

## § 4a Einwilligung

(1) [1]Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. [2]Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. [3]Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. [4]Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) [1]Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. [2]In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) [1]Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

## § 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) [1]Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,
2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder
3. der Organe und Einrichtungen der Europäischen Gemeinschaften

gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30a nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

(2) [1]Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend. [2]Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. [3] Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

(3) [1]Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) [1]In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. [2]Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

(5) [1]Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(6) [1]Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.

## § 4c Ausnahmen

(1) [1]Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern

1. der Betroffene seine Einwilligung gegeben hat,
2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

[2]Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.

(2) [1]Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. [2]Bei den Post- und Telekommunikationsunternehmen ist die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. [3]Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.

(3) [1]Die Länder teilen dem Bund die nach AbSatz 2 Satz 1 ergangenen Entscheidungen mit.

## § 4d Meldepflicht

(1) [1]Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) [1]Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) [1]Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) [1]Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung,
2. zum Zweck der anonymisierten Übermittlung oder
3. für Zwecke der Markt- oder Meinungsforschung

gespeichert werden.

(5) [1]Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Be-

ginn der Verarbeitung (Vorabkontrolle). [2]Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder

2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(6) [1]Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. [2]Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. [3]Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

## § 4e Inhalt der Meldepflicht

[1]Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,

2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,

3. Anschrift der verantwortlichen Stelle,

4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,

5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,

7. Regelfristen für die Löschung der Daten,

8. eine geplante Datenübermittlung in Drittstaaten,

9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

[2]§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

## § 4f Beauftragter für den Datenschutz

(1) [1]Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. [2]Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. [3]Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. [4]Die Sätze 1 und 2 gelten nicht für die nicht-öffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. [5]Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. [6]Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

(2) [1]Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. [2]Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. [3]Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. [4]Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) [1]Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. [2]Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. [3]Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. [4]Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden. [5]Ist nach Absatz 1 ein Beauftragter für den Datenschutz zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. [6]Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündi-

gung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. [7]Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

(4) [1]Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(4a) [1]Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nichtöffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. [2]Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. [3]Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(5) [1]Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. [2]Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

## § 4g Aufgaben des Beauftragten für den Datenschutz

(1) [1]Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. [2]Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. [3]Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. [4]Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) [1]Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. [2]Der Beauftragte für den

Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.

(2a) [1]Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.

(3) [1]Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde.

## § 5 Datengeheimnis

[1]Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). [2]Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. [3]Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

## § 6 Rechte des Betroffenen

(1) [1]Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. [2]Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. [3]Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. [4]Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. [5]Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterrichten. [6]In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

(2) [1]Personenbezogene Daten über die Ausübung eines Rechts des Betroffenen, das sich aus diesem Gesetz oder aus einer anderen Vorschrift über den Datenschutz ergibt, dürfen nur zur Erfüllung der sich aus der Ausübung des Rechts ergebenden Pflichten der verantwortlichen Stelle verwendet werden.

## § 6a Automatisierte Einzelentscheidung

(1) [1]Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. [2]Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

(2) [1]Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder

2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert.

(3) [1]Das Recht des Betroffenen auf Auskunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

## § 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) [1]Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,

2. zur Wahrnehmung des Hausrechts oder

3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) [1]Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) [1]Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. [2]Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) [1]Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) [1]Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

## § 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) [1]Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) [1]Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) [1]Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

## § 7 Schadensersatz

[1]Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. [2]Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

## § 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

(1) [1]Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) [1]Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) [1]Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130.000 Euro begrenzt. [2]Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130.000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) [1]Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) [1]Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt § 254 des Bürgerlichen Gesetzbuchs.

(6) [1]Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

## § 9 Technische und organisatorische Maßnahmen

[1]Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. [2]Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

## § 9a Datenschutzaudit

[1]Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. [2]Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

## § 10 Einrichtung automatisierter Abrufverfahren

(1) [1]Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. [2]Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) [1]Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. [2]Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

[3]Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) [1]Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. [2]Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn das für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesministerium zugestimmt hat.

(4) [1]Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. [2]Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. [3]Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. [4]Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) [1]Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. [2]Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann.

## § 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) [1]Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.

[2]Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) [1]Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [2]Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

[3]Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. [4]Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. [5]Das Ergebnis ist zu dokumentieren.

(3) [1]Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. [2]Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) [1]Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. (a) öffentliche Stellen,

(b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) [1] Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

# Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen

## Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung

### § 12 Anwendungsbereich

(1) [1] Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) [1] Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 16, 19 bis 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder

2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) [1] Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.

(4) [1] Werden personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28 Absatz 2 Nummer 2 und die §§ 32 bis 35 anstelle der §§ 13 bis 16 und 19 bis 20.

## § 13 Datenerhebung

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

(1a) [1]Werden personenbezogene Daten statt beim Betroffenen bei einer nichtöffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) [1]Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,
2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,
8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder
9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

## § 14 Datenspeicherung, -veränderung und -nutzung

(1) [1]Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen

Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. [2]Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) [1]Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) [1]Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. [2]Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) [1]Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(5) [1]Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder

2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

[2]Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) [1]Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

## § 15 Datenübermittlung an öffentliche Stellen

(1) [1]Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und

2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) [1]Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. [2]Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. [3]In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. [4]§ 10 Abs. 4 bleibt unberührt.

(3) [1]Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.

(4) [1]Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.

(5) [1]Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) [1] Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

## § 16 Datenübermittlung an nicht-öffentliche Stellen

(1) [1]Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder

2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. [2]Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(2) [1]Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) [1]In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. [2]Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) [1]Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]Die übermittelnde Stelle hat ihn darauf hinzuweisen. [3]Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

## § 17 (weggefallen)

## § 18 Durchführung des Datenschutzes in der Bundesverwaltung

(1) [1]Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. [2]Das Gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) [1]Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. [2]Für ihre automatisierten Verarbeitungen haben sie die Angaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. [3]Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. [4]Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

## Zweiter Unterabschnitt: Rechte des Betroffenen

## § 19 Auskunft an den Betroffenen

(1) [1]Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

[2]In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. [3]Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche

Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. [4]Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) [1] Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) [1]Bezieht sich die Auskunftserteilung auf 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.

(4) [1]Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) [1]Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. [2]In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(6) [1]Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. [2]Die Mitteilung der oder des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) [1]Die Auskunft ist unentgeltlich.

## § 19a Benachrichtigung

(1) [1]Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. [2]Der

Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. [3]Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) [1]Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

[2]Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.

(3) [1]§ 19 Abs. 2 bis 4 gilt entsprechend.

## § 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

(1) [1]Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. [2]Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) [1]Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) [1]An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) [1]Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) [1]Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. [2]Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) [1]Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die Behörde im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(7) [1]Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(8) [1]Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(9) [1]§ 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

## § 21 Anrufung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

[1]Jedermann kann sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. [2]Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

## Dritter Unterabschnitt: Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

### § 22 Wahl und Unabhängigkeit der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) [1]Der Deutsche Bundestag wählt ohne Aussprache auf Vorschlag der Bundesregierung die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. [2]Die oder der Bundesbeauftragte muss bei ihrer oder seiner Wahl das 35. Lebensjahr vollendet haben. [3]Die oder der Gewählte ist von der Bundespräsidentin oder dem Bundespräsidenten zu ernennen.

(2) [1]Die oder der Bundesbeauftragte leistet vor der Bundespräsidentin oder dem Bundespräsidenten folgenden Eid: „Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.“[2]Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) [1]Die Amtszeit der oder des Bundesbeauftragten beträgt fünf Jahre. [2]Einmalige Wiederwahl ist zulässig.

(4) [1]Die oder der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. [2]Sie oder er ist in Ausübung ihres oder seines Amtes unabhängig und nur dem Gesetz unterworfen.

(5) [1]Die oder der Bundesbeauftragte ist eine oberste Bundesbehörde. [2]Der Dienstsitz ist Bonn. [3]Die Beamtinnen und Beamten der oder des Bundesbeauftragten sind Beamtinnen und Beamte des Bundes.

(6) [1]Die Leitende Beamtin oder der Leitende Beamte nimmt die Rechte der oder des Bundesbeauftragten wahr, wenn die oder der Bundesbeauftragte an der Ausübung ihres oder seines Amtes verhindert ist oder wenn ihr oder sein Amtsverhältnis endet und sie oder er nicht zur Weiterführung der Geschäfte verpflichtet ist. [2]Absatz 4 Satz 2 ist entsprechend anzuwenden.

### § 23 Rechtsstellung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) [1]Das Amtsverhältnis der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beginnt mit der Aushändigung der Ernennungsurkunde. [2]Es endet

1. mit Ablauf der Amtszeit,

2. mit der Entlassung.

[3]Die Bundespräsidentin oder der Bundespräsident entlässt die Bundesbeauftragte oder den Bundesbeauftragten, wenn diese oder dieser es verlangt oder auf Vorschlag der Präsidentin oder des Präsidenten des Bundestages, wenn Gründe vorliegen, die bei einer Richterin auf Lebenszeit oder einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. [4]Im Falle der Beendigung des Amtsverhältnisses erhält die oder der Bundesbeauftragte eine von der Bundespräsidentin oder dem Bundespräsidenten vollzogene Urkunde. [5]Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. [6]Endet das Amtsverhältnis mit Ablauf der Amtszeit, ist die oder der Bundesbeauftragte verpflichtet, auf Ersuchen der Präsidentin oder des Präsidenten des Bundestages die Geschäfte bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers weiterzuführen.

(2) [1]Die oder der Bundesbeauftragte darf neben ihrem oder seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. [2]Sie oder er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) [1]Die oder der Bundesbeauftragte hat der Präsidentin oder dem Präsidenten des Bundestages Mitteilung über Geschenke zu machen, die sie oder er in Bezug auf das Amt erhält. [2]Die Präsidentin oder der Präsident des Bundestages entscheidet über die Verwendung der Geschenke. [3]Sie oder er kann Verfahrensvorschriften erlassen.

(4) [1]Die oder der Bundesbeauftragte ist berechtigt, über Personen, die ihr oder ihm in ihrer oder seiner Eigenschaft als Bundesbeauftragte oder Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. [2]Dies gilt auch für die Mitarbeiterinnen und Mitarbeiter der oder des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts die oder der Bundesbeauftragte entscheidet. [3]Soweit das Zeugnisverweigerungsrecht der oder des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihr oder ihm nicht gefordert werden.

(5) [1]Die oder der Bundesbeauftragte ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. [2]Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. [3]Die oder der Bundesbeauftragte entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie oder er über solche Angelegenheiten vor Gericht oder außergerichtlich aussagt oder Erklärungen abgibt; wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Bundesbeauftragten erforderlich. [4]Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. [5]Für die Bundesbeauftragte oder den Bundesbeauftragten und ihre oder seine Mitarbeiterinnen und Mitarbeiter gelten die §§ 93, 97, 105 Abs. 1,

§ 111 Abs. 5 in Verbindung mit § 105 Abs. 1 sowie § 116 Abs. 1 der Abgabenordnung nicht. [6]Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben der oder des Auskunftspflichtigen oder der für sie oder ihn tätigen Personen handelt. [7]Stellt die oder der Bundesbeauftragte einen Datenschutzverstoß fest, ist sie oder er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.

(6) [1]Die oder der Bundesbeauftragte darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde

1. dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit der Bundesrepublik Deutschland oder Ihre Beziehungen zu anderen Staaten, oder

2. Grundrechte verletzen.

[2]Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Bundesregierung zuzurechnen sind oder sein könnten, darf die oder der Bundesbeauftragte nur im Benehmen mit der Bundesregierung aussagen. [3]§ 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.

(7) [1]Die oder der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der Besoldungsgruppe B 11 sowie den Familienzuschlag entsprechend Anlage V des Bundesbesoldungsgesetzes. [2]Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. [3]Im Übrigen sind § 12 Abs 6 sowie die §§ 13 bis 20 und 21a Abs. 5 des Bundesministergesetzes mit den Maßgaben anzuwenden, dass an die Stelle der vierjährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. [4]Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 und 21a Abs. 5 des Bundesministergesetzes berechnet sich das Ruhegehalt der oder des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und die oder der Bundesbeauftragte sich unmittelbar vor ihrer oder seiner Wahl zur oder zum Bundesbeauftragten als Beamtin oder Beamter oder als Richterin oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 11 zu durchlaufenden Amt befunden hat.

(8) [1] Absatz 5 Satz 5 bis 7 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

## § 24 Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) [1]Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) [1]Die Kontrolle der oder des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs, und

2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

[2]Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. [3]Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegen, unterliegen nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten, es sei denn, die Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. [4]Der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber der oder dem Bundesbeauftragten widerspricht.

(3) [1]Die Bundesgerichte unterliegen der Kontrolle der oder des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) [1]Die öffentlichen Stellen des Bundes sind verpflichtet, die Bundesbeauftragte oder den Bundesbeauftragten und ihre oder seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. [2]Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

[3]Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur der oder dem Bundesbeauftragten selbst und den von ihr oder ihm schriftlich besonders Beauftragten. [4]Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) [1]Die oder der Bundesbeauftragte teilt das Ergebnis ihrer oder seiner Kontrolle der öffentlichen Stelle mit. [2]Damit kann sie oder er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln

bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. [3]§ 25 bleibt unberührt.

(6) [1] Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

## § 25 Beanstandungen durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) [1]Stellt die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 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

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,
4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. [2]In den Fällen von Satz 1 Nr. 4 unterrichtet die oder der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) [1]Die oder der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) [1]Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Bundesbeauftragten getroffen worden sind. [2]Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an die Bundesbeauftragte oder den Bundesbeauftragten zu.

## § 26 Weitere Aufgaben der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) [1]Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbe-

richt. [2]Sie oder er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

(2) [1]Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat die oder der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. [2]Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht die oder der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. [3]Die oder der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) [1]Die oder der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. [2]Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch die Bundesbeauftragte oder den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) [1]Die oder der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. [2]§ 38 Abs. 1 Satz 4 und 5 gilt entsprechend.

# Dritter Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

## Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung

### § 27 Anwendungsbereich

(1) [1]Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch

1. nicht-öffentliche Stellen,
2. (a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
   (b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

[2]Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. [3]In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) [1]Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

## § 28 Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) [1]Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

[2]Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) [1]Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,

2. soweit es erforderlich ist,

   (a) zur Wahrung berechtigter Interessen eines Dritten oder

   (b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

   und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) [1]Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. [2]Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,

2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder

3. für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

[3]Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. [4]Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. [5]Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. [6]Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. [7]Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) [1]Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. [2]Soll

die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

(3b) [1]Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. [2]Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

(4) [1]Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. [2]Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. [3]Widerspricht der Betroffene bei dem Dritten, dem die Daten im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. [4]In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses.

(5) [1]Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. [2]Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. [3]Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) [1]Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung,

Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) [1]Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. [2]Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. [3]Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuchs genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) [1]Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. [2]Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) [1]Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. [2]Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. [3]Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. [4] Absatz 2 Nummer 2 Buchstabe b gilt entsprechend.

## § 28a Datenübermittlung an Auskunfteien

(1) [1]Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,

3. der Betroffene die Forderung ausdrücklich anerkannt hat,

4. (a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

   (b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

   (c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

   (d) der Betroffene die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

[2]Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

(2) [1]Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. [2]Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. [3]Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. [4]Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) [1]Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. [2]Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

## § 28b Scoring

[1]Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,

2. im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,

3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,

4. im Fall der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

## § 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung

(1) [1]Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder

3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

[2]§ 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) [1]Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und

2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

[2]§ 28 Absatz 3 bis 3b gilt entsprechend. [3]Bei der Übermittlung nach Satz 1 Nr. 1 sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. [4]Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden. [5]Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen

und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) [1]Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. [2]Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) [1]Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) [1]§ 28 Abs. 6 bis 9 gilt entsprechend.

(6) [1]Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(7) [1]Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 6 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. [2]Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. [3]§ 6a bleibt unberührt.

## § 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form

(1) [1]Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. [2]Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) [1]Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.

(3) [1]Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) [1]§ 29 gilt nicht.

(5) [1]§ 28 Abs. 6 bis 9 gilt entsprechend.

## § 30a Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung

(1) [1]Das geschäftsmäßige Erheben, Verarbeiten oder Nutzen personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung gegenüber dem Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt.

[2]Besondere Arten personenbezogener Daten (§ 3 Absatz 9) dürfen nur für ein bestimmtes Forschungsvorhaben erhoben, verarbeitet oder genutzt werden.

(2) [1]Für Zwecke der Markt- oder Meinungsforschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet oder genutzt werden. [2]Daten, die nicht aus allgemein zugänglichen Quellen entnommen worden sind und die die verantwortliche Stelle auch nicht veröffentlichen darf, dürfen nur für das Forschungsvorhaben verarbeitet oder genutzt werden, für das sie erhoben worden sind. [3]Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, wenn sie zuvor so anonymisiert werden, dass ein Personenbezug nicht mehr hergestellt werden kann.

(3) [1]Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Zweck des Forschungsvorhabens, für das die Daten erhoben worden sind, möglich ist. [2]Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. [3]Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies nach dem Zweck des Forschungsvorhabens erforderlich ist.

(4) [1]§ 29 gilt nicht.

(5) [1]§ 28 Absatz 4 und 6 bis 9 gilt entsprechend.

## § 31 Besondere Zweckbindung

[1]Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen

Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

## § 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) [1]Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. [2]Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) [1] Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) [1]Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

## Zweiter Unterabschnitt: Rechte des Betroffenen

## § 33 Benachrichtigung des Betroffenen

(1) [1]Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. [2]Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. [3]Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) [1]Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,

4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,

5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

7. die Daten für eigene Zwecke gespeichert sind und

   (a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder

   (b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,

8. die Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert sind und

   (a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder

   (b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Absatz 2 Satz 2)

   und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist,

9. aus allgemein zugänglichen Quellen entnommene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung gespeichert sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

[2]Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

## § 34 Auskunft an den Betroffenen

(1) [1]Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

[2]Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. [3]Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. [4]Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(1a) [1]Im Fall des § 28 Absatz 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. [2]Satz 1 gilt entsprechend für den Empfänger.

(2) [1]Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,
2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und
3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

[2]Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle

1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder
2. bei einer anderen Stelle gespeicherte Daten nutzt.

[3]Hat eine andere als die für die Entscheidung verantwortliche Stelle

1. den Wahrscheinlichkeitswert oder
2. einen Bestandteil des Wahrscheinlichkeitswerts

berechnet, hat sie die insoweit zur Erfüllung der Auskunftsansprüche nach den Sätzen 1 und 2 erforderlichen Angaben auf Verlangen der für die Entscheidung verantwortlichen Stelle an diese zu übermitteln. [4]Im Fall des Satzes 3 Nr. 1 hat die für die Entscheidung verantwortliche Stelle den Betroffenen zur Geltendmachung seiner Auskunftsansprüche unter Angabe des Namens und der Anschrift der anderen Stelle sowie der zur Bezeichnung des Einzelfalls notwendigen Angaben unverzüglich an diese zu verweisen, soweit sie die Auskunft nicht selbst erteilt. [5]In diesem Fall hat die andere Stelle, die den Wahrscheinlichkeitswert berechnet hat, die Auskunftsansprüche nach den Sätzen 1 und 2 gegenüber dem Betroffenen unentgeltlich zu erfüllen. [6]Die Pflicht der für die Berechnung des Wahrscheinlichkeitswerts verantwortlichen Stelle nach Satz 3 entfällt, soweit die für die Entscheidung verantwortliche Stelle von ihrem Recht nach Satz 4 Gebrauch macht.

(3) [1]Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. [2]Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die

1. gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,
2. die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung nutzt.

[3]Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(4) [1]Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,
2. die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,
3. die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie

4. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

[2]Satz 1 gilt entsprechend, wenn die verantwortliche Stelle

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

(5) [1]Die nach den Absätzen 1a bis 4 zum Zweck der Auskunftserteilung an den Betroffenen gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verwendet werden; für andere Zwecke sind sie zu sperren.

(6) [1]Die Auskunft ist auf Verlangen in Textform zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(7) [1]Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(8) [1]Die Auskunft ist unentgeltlich. [2]Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen. [3]Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. [4]Das Entgelt darf über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. [5]Ein Entgelt kann nicht verlangt werden, wenn

1. besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder

2. die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 zu berichtigen oder nach § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(9) [1]Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten zu verschaffen. [2]Er ist hierauf hinzuweisen.

## § 35 Berichtigung, Löschung und Sperrung von Daten

(1) [1]Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. [2]Geschätzte Daten sind als solche deutlich zu kennzeichnen.

(2) [1]Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. [2]Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,

2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,

3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder

4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

[3]Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

(3) [1]An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Fall des Absatzes 2 Satz 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) [1]Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(4a) [1]Die Tatsache der Sperrung darf nicht übermittelt werden.

(5) [1]Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. [2]Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) [1]Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zweck der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. [2]Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. [3]Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) [1]Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) [1]Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

## Dritter Unterabschnitt: Aufsichtsbehörde

## § 36 (weggefallen)

## § 37 (weggefallen)

## § 38 Aufsichtsbehörde

(1) [1]Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. [2]Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. [3]Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 gilt entsprechend. [4]Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. [5]Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). [6]Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen

anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. [7]Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. [8]§ 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.

(2) [1]Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. [2]Das Register kann von jedem eingesehen werden. [3]Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.

(3) [1]Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. [2]Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. [3]Der Auskunftspflichtige ist darauf hinzuweisen.

(4) [1]Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. [2]Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. [3]§ 24 Abs. 6 gilt entsprechend. [4]Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) [1]Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. [2]Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. [3]Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(6) [1]Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(7) [1]Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

### § 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

(1) [1]Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) [1]Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

## Vierter Abschnitt: Sondervorschriften

### § 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) [1]Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. [2]In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) [1]Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

### § 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) [1]Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) [1]Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. [2]Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. [3]Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) [1]Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

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

## § 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) [1]Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) [1]Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) [1]Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen. [2]Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde.

[3]Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) [1]Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. [2]Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

## § 42 Datenschutzbeauftragter der Deutschen Welle

(1) [1]Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit tritt. [2]Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. [3]Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) [1]Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. [2]Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. [3]Im Übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) [1]Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) [1]Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. [2]Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organes der Deutschen Welle. [3]Die Tätigkeitsberichte übermittelt der Beauftragte auch der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

(5) [1]Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. [2]Die §§ 4f und 4g bleiben unberührt.

## § 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

(1) [1]Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. [2]Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. [3]Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen

zur Minderung möglicher nachteiliger Folgen enthalten. [4]Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. [5]Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. [6]Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

# Fünfter Abschnitt: Schlussvorschriften

## § 43 Bußgeldvorschriften

(1) [1]Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,

7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) [1]Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder
7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) [1]Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. [2]Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. [3]Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

## § 44 Strafvorschriften

(1) [1]Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) [1]Die Tat wird nur auf Antrag verfolgt. [2]Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

# Sechster Abschnitt: Übergangsvorschriften

## § 45 Laufende Verwendungen

[1]Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. [2]Soweit Vorschriften dieses Gesetzes in Rechtsvorschriften außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zur Anwendung gelangen, sind Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.

## § 46 Weitergeltung von Begriffsbestimmungen

(1) [1]Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei).

[2]Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(2) [1]Wird in besonderen Rechtsvorschriften des Bundes der Begriff Akte verwendet, ist Akte jede amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht dem Dateibegriff des Absatzes 1 unterfällt; dazu zählen auch Bild- und Tonträger. [2]Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(3) [1]Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. [2]Empfänger sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

## § 47 Übergangsregelung

[1]Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 in der bis dahin geltenden Fassung weiter anzuwenden

1. für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,
2. für Zwecke der Werbung bis zum 31. August 2012.

## § 48 Bericht der Bundesregierung

[1]Die Bundesregierung berichtet dem Bundestag

1. bis zum 31. Dezember 2012 über die Auswirkungen der §§ 30a und 42a,
2. bis zum 31. Dezember 2014 über die Auswirkungen der Änderungen der §§ 28 und 29.

[2]Sofern sich aus Sicht der Bundesregierung gesetzgeberische Maßnahmen empfehlen, soll der Bericht einen Vorschlag enthalten.

## Anlage
## (zu § 9 Satz 1)

[1]Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

[2]Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

# Landesdatenschutzgesetz (LDSG)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz) |
| **Amtliche Abkürzung:** | LDSG |
| **Ausfertigung:** | 09.02.2000, GVOBl. 2000 S. 169 |
| **Inkrafttreten:** | 01.07.2000 |
| **Letzte Änderung:** | 16.03.2015, GVOBl. 2015 S. 69 |

## Inhaltsübersicht


**Abschnitt I: Allgemeine Grundsätze** **62**

§ 1 Gesetzeszweck 62
§ 2 Begriffsbestimmungen 63
§ 3 Anwendungsbereich 64
§ 4 Datenvermeidung und Datensparsamkeit, Datenschutzaudit 64
§ 5 Allgemeine Maßnahmen zur Datensicherheit 64
§ 6 Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren 65
§ 7 Verfahrensverzeichnis, Meldung 66
§ 8 Gemeinsame Verfahren und Abrufverfahren 67
§ 9 Vorabkontrolle 68
§ 10 Behördliche Datenschutzbeauftragte 68

**Abschnitt II: Zulässigkeit** **69**

§ 11 Zulässigkeit der Datenverarbeitung 69
§ 12 Form der Einwilligung 71
§ 13 Erhebung, Zweckbindung 71
§ 14 Datenübermittlung an andere öffentliche Stellen 72
§ 15 Datenübermittlung an nicht-öffentliche Stellen 73
§ 16 Datenübermittlung an ausländische Stellen 73

**Abschnitt III: Besondere Formen der Datenverarbeitung** **74**

§ 17 Verarbeitung personenbezogener Daten im Auftrag, Wartung 74
§ 18 Mobile personenbezogene Datenverarbeitungssysteme 75
§ 19 Automatisierte Einzelentscheidungen 75

§ 20 Video-Überwachung und -Aufzeichnung 75
§ 21 Veröffentlichung von Daten im Internet 76
**Abschnitt IV: Besondere Zwecke der Datenverarbeitung 77**
§ 22 Datenverarbeitung für wissenschaftliche Zwecke 77
§ 23 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen 78
§ 24 Öffentliche Auszeichnungen 78
§ 25 weggefallen 79
**Abschnitt V: Rechte der Betroffenen 79**
§ 26 Aufklärung, Benachrichtigung 79
§ 27 Auskunft an Betroffene 80
§ 27a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten 81
§ 28 Berichtigung, Löschung, Sperrung 81
§ 29 Einwand gegen die Verarbeitung 82
§ 30 Schadensersatz 82
§ 31 Unabdingbarkeit 83
**Abschnitt VI: Das Unabhängige Landeszentrum für Datenschutz 83**
§ 32 Errichtung und Rechtsform 83
§ 33 Trägerschaft, Anstaltslast und Gewährträgerhaftung 83
§ 34 Organ 83
§ 35 Wahl und Amtszeit der oder des Landesbeauftragten für Datenschutz 84
§ 36 Rechtsstellung der oder des Landesbeauftragten für Datenschutz 84
§ 37 Satzung 85
§ 38 Beirat 85
§ 39 Aufgaben des Unabhängigen Landeszentrums für Datenschutz 85
§ 40 Anrufung des Unabhängigen Landeszentrums für Datenschutz 86
§ 41 Kontrollaufgaben 86
§ 42 Beanstandungen 86
§ 43 Serviceaufgaben 87
**Abschnitt VII: Schlussvorschriften 87**
§ 44 Ordnungswidrigkeiten 87
§ 45 Übergangsregelungen 88
§ 46 Inkrafttreten, Außerkrafttreten 88

# Abschnitt I: Allgemeine Grundsätze

## § 1 Gesetzeszweck

[1]Zweck dieses Gesetzes ist es, bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen das Recht auf informationelle Selbstbestimmung zu wahren.

## § 2 Begriffsbestimmungen

(1) [1]Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene oder Betroffener).

(2) [1]Datenverarbeitung ist die Verwendung personenbezogener Daten. [2]Dabei ist

1. Erheben das Beschaffen von Daten,
2. Speichern das Aufbewahren von Daten auf Datenträgern,
3. Übermitteln das Weitergeben von Daten an Dritte oder der Abruf von zum Abruf bereitgehaltenen Daten durch Dritte,
4. Sperren das Untersagen weiterer Verarbeitung gespeicherter Daten,
5. Löschen das Unkenntlichmachen gespeicherter Daten,
6. Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,
7. Pseudonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,
8. Verschlüsseln das Verändern personenbezogener Daten derart, dass ohne Nutzung des Geheimnisses die Kenntnisnahme vom Inhalt der Daten nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist.

(3) [1]Datenverarbeitende Stelle ist jede öffentliche Stelle im Sinne von § 3 Abs. 1, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

(4) [1]Empfänger ist jede natürliche oder juristische Person, öffentliche oder nicht-öffentliche Stelle, die Daten erhält.

(5) [1]Dritte oder Dritter ist jede natürliche oder juristische Person und öffentliche oder nicht-öffentliche Stelle außer

1. der datenverarbeitenden Stelle selbst,
2. der betroffenen Person,
3. der Auftragsdatenverarbeiterin oder dem Auftragsdatenverarbeiter und
4. den Personen, die unter der unmittelbaren Verantwortung der datenverarbeitenden Stelle oder der Auftragsdatenverarbeiterin oder des Auftragsdatenverarbeiters befugt sind, die Daten zu verarbeiten.

## § 3 Anwendungsbereich

(1) [1]Dieses Gesetz gilt für öffentliche Stellen. [2]Öffentliche Stellen im Sinne dieses Gesetzes sind Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung.

(2) [1]Abweichend von Absatz 1 gelten nur die Vorschriften der §§ 23 und 39 bis 43, soweit

1. wirtschaftliche Unternehmen der Gemeinden oder Gemeindeverbände ohne eigene Rechtspersönlichkeit (Eigenbetriebe),
2. öffentliche Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden,
3. Landesbetriebe oder
4. der Aufsicht des Landes oder der Gemeinden unterstehende juristische Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen,

personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. [2]Im Übrigen sind die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme seines § 38 anzuwenden.

(3) [1]Soweit besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor.

(4) [1]Der Landtag, seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie die Landtagsverwaltung unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten. Der Landtag erlässt insoweit unter Berücksichtigung seiner verfassungsrechtlichen Stellung und der Grundsätze dieses Gesetzes eine Datenschutzordnung.

## § 4 Datenvermeidung und Datensparsamkeit, Datenschutzaudit

(1) [1]Die datenverarbeitende Stelle hat den Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten.

(2) [1]Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden. [2]Die Landesregierung regelt durch Verordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.

## § 5 Allgemeine Maßnahmen zur Datensicherheit

(1) [1]Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz im Sinne von § 3 Abs. 3 ist durch technische und

organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. [2]Sie müssen gewährleisten, dass

1. Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit),
2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (Integrität),
3. nur befugt auf Verfahren und Daten zugegriffen werden kann (Vertraulichkeit),
4. die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (Transparenz),
5. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (Nicht-Verkettbarkeit) und
6. Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 26 bis 30 wirksam ermöglichen (Intervenierbarkeit).

(2) [1]Automatisierte Verfahren sind vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen hinsichtlich einer wirksamen Umsetzung der getroffenen Maßnahmen nach Absatz 1 zu testen und durch die Leiterin oder den Leiter der datenverarbeitenden Stelle oder eine befugte Person freizugeben.

(3) [1]Die Landesregierung regelt durch Verordnung die Anforderungen an das Sicherheitskonzept sowie die Freigabe automatisierter Verfahren und weitere Einzelheiten einer ordnungsgemäßen Datenverarbeitung der öffentlichen Stellen. [2]Das Unabhängige Landeszentrum für Datenschutz ist anzuhören.

## § 6 Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

(1) [1]Automatisierte Verfahren sind so zu gestalten, dass eine Verarbeitung personenbezogener Daten erst möglich ist, nachdem die Berechtigung der Benutzerin oder des Benutzers festgestellt worden ist.

(2) [1]Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. [2]Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.

(3) [1]Werden personenbezogene Daten mit Hilfe informationstechnischer Geräte von der datenverarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. [2]Die datenverarbeitende Stelle hat sicherzustellen, dass sie die Daten entschlüsseln kann. [3]In Fällen, in denen eine Verschlüsselung aus technischen Gründen nicht möglich ist, ist die Verarbeitung personenbezogener Daten ohne Verschlüsselung nach konkreten, dem Schutzbedarf der personenbezogenen Daten angemessenen Verfahrensregelungen zulässig.

(4) [1]Werden personenbezogene Daten ausschließlich automatisiert gespeichert, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. [2]Entsprechendes gilt für die Veränderung und Übermittlung der Daten. [3]Die Protokolldaten müssen zusammen mit den gespeicherten personenbezogenen Daten sichtbar gemacht werden können und für den gleichen Zeitraum aufbewahrt werden.

(5) [1]Die datenverarbeitenden Stellen haben die ordnungsgemäße Anwendung der automatisierten Verfahren zu überwachen.

## § 7 Verfahrensverzeichnis, Meldung

(1) [1]Die datenverarbeitende Stelle erstellt für jedes von ihr betriebene automatisierte Verfahren ein Verfahrensverzeichnis. [2]Dieses Verzeichnis kann auch von einer Stelle für andere geführt werden. [3]Es enthält Angaben über

1. Name und Anschrift der datenverarbeitenden Stelle,
2. Zweckbestimmung und Rechtsgrundlage des Verfahrens,
3. den Kreis der Betroffenen,
4. die Kategorien der verarbeiteten Daten und deren Aufbewahrungs- oder Löschfristen,
5. die Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich der Auftragnehmenden,
6. geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union,
7. die datenschutzrechtliche Beurteilung der oder des behördlichen Datenschutzbeauftragten, soweit eine solche vorliegt,
8. eine allgemeine Beschreibung der nach den §§ 5 und 6 zur Einhaltung der Datensicherheit getroffenen Maßnahmen.

(2) [1]Absatz 1 gilt nicht für Register, die zur Information der Öffentlichkeit bestimmt sind oder die allen Personen, die mindestens ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen stehen, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

(3) [1]Die datenverarbeitenden Stellen, die keine behördliche Datenschutzbeauftragte oder keinen behördlichen Datenschutzbeauftragten nach § 10 bestellt haben, melden dem Unabhängigen Landeszentrum für Datenschutz den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens. [2]Ausgenommen sind die in den Absätzen 2 und 4 genannten Verfahren. [3]Die meldepflichtigen Stellen haben spätestens bei der ersten Einspeicherung die Angaben nach Absatz 1 mitzuteilen. [4]Bei Verfahren, die von öffentlichen Stellen entwickelt worden sind, können diese Stellen mit der Abgabe der Meldung beauftragt werden.

(4) [1]Das Unabhängige Landeszentrum für Datenschutz führt ein Verzeichnis der Meldungen nach Absatz 3. [2]Es enthält die Angaben nach Absatz 1. [3]Das Verzeichnis kann von jeder Person eingesehen werden. [4]Das Unabhängige Landeszentrum für Datenschutz veröffentlicht das Verzeichnis auf seiner Internetseite. [5]Die Sätze 3 und 4 gelten nicht für Verfahren, die

1. nach dem Landesverfassungsschutzgesetz geführt werden,
2. der Gefahrenabwehr dienen,
3. der Strafverfolgung dienen oder
4. der Steuerfahndung dienen.

(5) [1]Bei Bestellung einer oder eines behördlichen Datenschutzbeauftragten nach § 10 kann das Verfahrensverzeichnis von jeder Person bei der datenverarbeitenden Stelle eingesehen werden. [2]Die datenverarbeitende Stelle kann das Verfahrensverzeichnis auf ihrer Internetseite veröffentlichen. [3]Die Ausnahmen von der Einsichtnahme und Veröffentlichung nach Absatz 4 Satz 5 gelten entsprechend.

## § 8 Gemeinsame Verfahren und Abrufverfahren

(1) [1]Ein automatisiertes Verfahren, das mehreren datenverarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten (gemeinsames Verfahren) oder die Übermittlung personenbezogener Daten durch Abruf (Abrufverfahren) ermöglicht, darf nur eingerichtet werden, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) [1]Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Verfahrens kontrolliert werden kann. [2]Hierzu kann die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit des automatisierten Verfahrens von der Verantwortung für die gespeicherten Daten abgetrennt und auf eine zentrale Stelle übertragen werden. [3]Die zentrale Stelle sowie Einzelheiten über Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung werden durch Verordnung der für das Verfahren zuständigen obersten Landesbehörde bestimmt.

(3) [1]Bei Verfahren nach Absatz 1 ist das Verfahrensverzeichnis nach § 7 Abs. 1 um die Feststellung zu ergänzen, für welchen Bereich der Datenverarbeitung jede der beteiligten Stellen verantwortlich ist. [2]Die Betroffenen können die ihnen nach Abschnitt V dieses Gesetzes zustehenden Rechte gegenüber jeder der beteiligten Stellen geltend machen. [3]Diese leiten die Anliegen der Betroffenen an die nach Satz 1 als verantwortlich festgestellte Stelle weiter.

(4) [1]Werden bei gemeinsamen Verfahren personenbezogene Daten übermittelt, sind die Empfänger, der Zeitpunkt der Übermittlung, die jeweils übermittelten Daten und der Zweck der Übermittlung zu protokollieren. [2]Die Protokolldatenbestände sind ein Jahr zu speichern.

(5) [1]Bei Abrufverfahren trägt die Verantwortung für die Zulässigkeit des einzelnen Abrufs die abrufende Stelle. [2]Die speichernde Stelle prüft die Zulässigkeit

des Abrufs nur, wenn dazu Anlass besteht. [3]Die speichernde Stelle hat zu gewährleisten, dass die Zulässigkeit der Übermittlung personenbezogener Daten festgestellt und überprüft werden kann.

(6) [1]Die Absätze 1 bis 5 gelten nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

## § 9 Vorabkontrolle

(1) [1]Vor der Einrichtung oder wesentlichen Änderung

1. eines Verfahrens nach § 8 Abs. 1 oder
2. eines automatisierten Verfahrens, in dem Daten im Sinne des § 11 Abs. 3 verarbeitet werden,

ist der oder dem behördlichen Datenschutzbeauftragten oder, wenn eine solche oder ein solcher nicht bestellt ist, dem Unabhängigen Landeszentrum für Datenschutz Gelegenheit zur Prüfung innerhalb einer angemessenen Frist zu geben, ob die Datenverarbeitung zulässig und die vorgesehenen Maßnahmen nach den §§ 5 und 6 ausreichend sind (Vorabkontrolle).

(2) [1]Absatz 1 gilt nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

## § 10 Behördliche Datenschutzbeauftragte

(1) [1]Die datenverarbeitende Stelle kann schriftlich eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen. [2]Mehrere datenverarbeitende Stellen können gemeinsam eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen.

(2) [1]Die oder der behördliche Datenschutzbeauftragte muss die erforderliche Sachkunde und Zuverlässigkeit besitzen. [2]Sie oder er darf durch die Bestellung keinem Konflikt mit anderen dienstlichen Aufgaben ausgesetzt sein.

(3) [1]Die oder der behördliche Datenschutzbeauftragte ist unmittelbar der Leiterin oder dem Leiter der datenverarbeitenden Stelle zu unterstellen. [2]Sie oder er ist bei der Ausübung des Amtes weisungsfrei und darf wegen der Wahrnehmung des Amtes nicht benachteiligt werden. [3]Sie oder er ist zur Erfüllung der Aufgaben des Amtes im erforderlichen Umfang freizustellen und mit den notwendigen Mitteln auszustatten. [4]Beschäftigte und Betroffene können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an sie oder ihn wenden. [5]Die oder der behördliche Datenschutzbeauftragte darf zur Aufgabenerfüllung Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen. [6]Dies gilt nicht, soweit das Steuergeheimnis dem entgegensteht. [7]Im übrigen gilt § 41 Abs. 1 entsprechend.

(4) [1]Die oder der behördliche Datenschutzbeauftragte überwacht und unterstützt die Einhaltung der datenschutzrechtlichen Vorschriften bei der datenverarbeitenden Stelle. [2]Sie oder er hat insbesondere

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken,
2. die Beschäftigten der datenverarbeitenden Stellen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
3. die datenverarbeitende Stelle bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten zu beraten und bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren auf die Einhaltung der einschlägigen Vorschriften hinzuwirken,
4. das Verzeichnis nach § 7 Abs. 1 zu führen und zur Einsicht bereitzuhalten,
5. die Vorabkontrolle nach § 9 Abs. 1 durchzuführen.

[3]In Zweifelsfällen hat sie oder er das Unabhängige Landeszentrum für Datenschutz zu hören.

# Abschnitt II: Zulässigkeit der Datenverarbeitung

## § 11 Zulässigkeit der Datenverarbeitung

(1) [1]Die Verarbeitung personenbezogener Daten ist zulässig, wenn

1. die oder der Betroffene eingewilligt hat,
2. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt,
3. sie zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der datenverarbeitenden Stelle erforderlich ist oder
4. sie zur Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist.

(2) [1]Die Verarbeitung personenbezogener Daten, die allgemein zugänglichen Quellen entnommen werden können, sowie von Daten, die die Betroffenen selbst zur Veröffentlichung bestimmt haben, ist über die Fälle von Absatz 1 hinaus zulässig, soweit schutzwürdige Belange der Betroffenen nicht beeinträchtigt sind.

(3) [1]Die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben sowie von Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, ist nur zulässig, soweit

1. die oder der Betroffene eingewilligt hat,
2. die Voraussetzungen des § 17 Abs. 5 oder der §§ 22 bis 24 vorliegen,
3. andere Rechtsvorschriften sie erlauben,
4. sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich ist, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,
5. sie sich auf Daten bezieht, die die oder der Betroffene selbst öffentlich gemacht hat,
6. sie zur Geltendmachung rechtlicher Ansprüche vor Gericht erforderlich ist oder
7. sie für die Abwehr von Gefahren für Leben, Gesundheit, persönliche Freiheit oder vergleichbare Rechtsgüter erforderlich ist. Satz 1 gilt entsprechend für Daten über strafbare Handlungen und Entscheidungen in Strafsachen.

(4) [1]Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. [2]Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so sind auch die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, zulässig, soweit nicht schutzwürdige Belange der oder des Betroffenen überwiegen. [3]Die nicht erforderlichen Daten unterliegen insoweit einem Verwertungsverbot.

(5) [1]Die Absätze 3 und 4 finden keine Anwendung, wenn die Datenverarbeitung

1. durch die Verfassungsschutzbehörde zur Erfüllung ihrer Aufgaben erfolgt,
2. der Gefahrenabwehr dient,
3. der Strafverfolgung dient oder
4. der Steuerfahndung dient.

[2]Absatz 3 Satz 1 findet keine Anwendung, wenn die Datenverarbeitung der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder der Verwaltung von Gesundheitsdiensten dient und

die Verarbeitung der Daten durch ärztliches Personal oder sonstige Personen, die einer der ärztlichen Schweigepflicht entsprechenden Geheimhaltungspflicht unterliegen, erfolgt.

(6) [1]Pseudonymisierte Daten dürfen nur von solchen Stellen verarbeitet werden, die keinen Zugriff auf die Zuordnungsfunktion haben. [2]Die Übermittlung pseudonymisierter Daten ist zulässig, wenn die Zuordnungsfunktion im alleinigen Zugriff der übermittelnden Stelle verbleibt.

## § 12 Form der Einwilligung

(1) [1]Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. [2]In den Fällen des § 11 Abs. 3 muss sich die Einwilligung ausdrücklich auf die dort aufgeführten Daten beziehen. [3]Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, ist die oder der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen.

(2) [1]Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der oder des Betroffenen beruht. [2]Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. [3]Dabei ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

(3) [1]Die Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, dass

1. sie nur durch eine eindeutige und bewusste Handlung der oder des Betroffenen erfolgen kann,
2. sie unversehrt und authentisch ist,
3. die Identität der Urheberin oder des Urhebers erkannt werden kann und
4. die Einwilligung bei der verarbeitenden Stelle protokolliert wird.

## § 13 Erhebung, Zweckbindung

(1) [1]Personenbezogene Daten sind bei den Betroffenen mit ihrer Kenntnis zu erheben. [2]Ohne Kenntnis der Betroffenen dürfen personenbezogene Daten nur erhoben werden, wenn die Voraussetzungen von Absatz 3 Nr. 1, 2 oder 4 vorliegen. [3]Die Herkunft der Daten und der Zweck der Erhebung sind zu dokumentieren.

(2) [1]Personenbezogene Daten dürfen nur für den Zweck weiterverarbeitet werden, für den sie rechtmäßig erhoben worden sind. [2]Daten, von denen die öffentliche Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für die Zwecke weiterverarbeitet werden, für die sie erstmals rechtmäßig gespeichert worden sind.

(3) [1]Die Verarbeitung für andere Zwecke ist ohne Einwilligung der oder des Betroffenen nur zulässig, wenn

1. eine Rechtsvorschrift dies erlaubt,
2. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechte einzelner dies gebietet,
3. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder
4. die Einholung der Einwilligung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre und offensichtlich ist, dass die Verarbeitung im Interesse der oder des Betroffenen liegt und sie oder er in Kenntnis des anderen Zwecks die Einwilligung erteilen würde.

(4) [1]Daten im Sinne von § 11 Abs. 3 Satz 1 dürfen ohne Einwilligung der oder des Betroffenen für andere Zwecke nur verarbeitet werden, wenn die Voraussetzungen des Absatzes 3 Nr. 1 oder 2 vorliegen. [2]Dies gilt nicht in den Fällen des § 11 Abs. 5.

(5) [1]Die Verarbeitung der Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zur Rechnungsprüfung gilt nicht als Verarbeitung für andere Zwecke. [2]Daten, die zu einem anderen Zweck erhoben oder erstmalig gespeichert wurden, sind für Ausbildungs- und Prüfungszwecke in anonymisierter oder pseudonymisierter Form zu verarbeiten. [3]Lassen sich die in Satz 2 genannten Zwecke durch anonymisierte oder pseudonymisierte Datenverarbeitung nicht erreichen, so ist die Zweckänderung zulässig, soweit berechtigte Interessen der oder des Betroffenen an der Geheimhaltung der Daten nicht überwiegen.

(6) [1]Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

(7) [1]Werden Daten innerhalb einer datenverarbeitenden Stelle zu einem anderen Zweck als dem nach Absatz 2 weiterverarbeitet, so ist dies zu dokumentieren.

## § 14 Datenübermittlung an andere öffentliche Stellen

(1) [1]Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, wenn die Voraussetzungen der §§ 11 und 13 Abs. 2 bis 6 vorliegen.

(2) [1]Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. [2]Soll die Übermittlung auf Ersuchen einer Stelle erfolgen, so hat diese die hierfür erforderlichen Angaben zu machen, insbesondere die Rechtsgrundlage für die Übermittlung anzugeben. [3]Die übermittelnde Stelle prüft die Schlüssigkeit der Anfrage. Bestehen im Einzelfall Zweifel, so prüft sie auch die Rechtmäßigkeit des Ersuchens.

(3) [1]Die übermittelnde Stelle protokolliert die Empfänger, den Zeitpunkt der Übermittlung, die jeweils übermittelten Daten und den Zweck der Übermittlung. [2]Die Protokolldatenbestände sind ein Jahr zu speichern.

## § 15 Datenübermittlung an nicht-öffentliche Stellen

(1) [1]Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. von diesen ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt sind oder

2. die Voraussetzungen der §§ 11 und 13 Abs. 2 bis 6 vorliegen.

(2) [1]Die übermittelnde Stelle hat die empfangende Stelle zu verpflichten, die Daten nur zu dem Zweck zu verwenden, zu dem sie ihr übermittelt wurden. [2]§ 14 Abs. 3 gilt entsprechend, sofern nicht durch Rechtsvorschrift Abweichendes geregelt ist.

## § 16 Datenübermittlung an ausländische Stellen

(1) [1]Die Zulässigkeit der Übermittlung an öffentliche und nicht-öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes richtet sich nach den §§ 14 und 15.

(2) [1]Die Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union ist nur zulässig, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. [2]Fehlt es an einem angemessenen Datenschutzniveau, so ist die Übermittlung nur zulässig, wenn

1. die oder der Betroffene eingewilligt hat,

2. die Übermittlung zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung eines rechtlichen Interesses erforderlich ist,

3. die Übermittlung zur Wahrung lebenswichtiger Interessen der oder des Betroffenen erforderlich ist,

4. die Übermittlung aus einem für die Öffentlichkeit bestimmten Register erfolgt oder

5. die empfangende Stelle ausreichende Garantien hinsichtlich des Schutzes der Grundrechte bietet.

(3) [1]Vor der Entscheidung über die Angemessenheit des Datenschutzniveaus und einer Entscheidung nach Absatz 2 Nr. 5 ist das Unabhängige Landeszentrum für Datenschutz zu hören.

(4) [1]Die empfangende Stelle ist darauf hinzuweisen, dass die Daten nur zu den Zwecken verarbeitet werden dürfen, für die sie übermittelt wurden.

# Abschnitt III: Besondere Formen der Datenverarbeitung

## § 17 Verarbeitung personenbezogener Daten im Auftrag, Wartung

(1) [1]Lässt eine datenverarbeitende Stelle personenbezogene Daten in ihrem Auftrag verarbeiten, bleibt sie für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. [2]Rechte der Betroffenen sind ihr gegenüber geltend zu machen. [3]Die Weitergabe der Daten von der datenverarbeitenden Stelle an die Auftragnehmenden gilt nicht als Übermittlung im Sinne von § 2 Abs. 2 Nr. 3.

(2) [1]Werden bei automatisierter Datenverarbeitung Verantwortlichkeiten auf eine zentrale Stelle übertragen, gilt § 8 Abs. 2 entsprechend. [2]Die zentrale Stelle übernimmt für das automatisierte Verfahren die Verantwortung nach Absatz 1 Satz 1.

(3) [1]Die datenverarbeitende Stelle hat dafür Sorge zu tragen, dass personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. [2]Sie hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um dies sicherzustellen. [3]Sie hat Auftragnehmende unter besonderer Berücksichtigung ihrer Eignung für die Gewährleistung der nach den §§ 5 und 6 notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [4]Aufträge, ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und die etwaige Zulässigkeit von Unterauftragsverhältnissen sind schriftlich festzulegen.

(4) [1]Sofern die Vorschriften dieses Gesetzes auf Auftragnehmende keine Anwendung finden, hat die datenverarbeitende Stelle diese zu verpflichten, jederzeit von ihr veranlasste Kontrollen zu ermöglichen.

(5) [1]Bei der Erbringung von Wartungsarbeiten oder von vergleichbaren Unterstützungstätigkeiten bei der Datenverarbeitung durch Stellen oder Personen außerhalb der datenverarbeitenden Stelle gelten die Absätze 1 bis 3 entsprechend.

(6) [1]Zur Durchführung von beratenden oder begutachtenden Tätigkeiten im Auftrag der datenverarbeitenden Stelle ist die Übermittlung personenbezogener Daten zulässig, wenn die übermittelnde Stelle die beauftragten Personen verpflichtet,

1. die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihnen überlassen worden sind und

2. nach Erledigung des Auftrags die ihnen von der datenverarbeitenden Stelle überlassenen Datenträger zurückzugeben und die bei ihnen gespeicherten Daten zu löschen, soweit nicht besondere Rechtsvorschriften entgegenstehen.

[2]Die Absätze 1 bis 4 gelten entsprechend.

## § 18 Mobile personenbezogene Datenverarbeitungssysteme

(1) [1]Mobile personenbezogene Speicher- und Verarbeitungsmedien zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten der Betroffenen automatisiert austauschen können (mobile Datenverarbeitungssysteme), dürfen nur mit der Einwilligung der oder des Betroffenen oder aufgrund einer Rechtsvorschrift eingesetzt werden.

(2) [1]Für die Betroffenen muss jederzeit erkennbar sein,

1. ob Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungssystem oder durch dieses veranlasst stattfinden,
2. welche personenbezogenen Daten der oder des Betroffenen verarbeitet werden und
3. welcher Verarbeitungsvorgang im einzelnen abläuft oder angestoßen wird.

(3) [1]Die Betroffenen sind bei der Ausgabe des mobilen Datenverarbeitungssystems über die ihnen nach den §§ 26 ff. zustehenden Rechte aufzuklären.

## § 19 Automatisierte Einzelentscheidungen

[1]Entscheidungen, die zu einer tatsächlichen oder rechtlichen Beschwer der Betroffenen führen, dürfen nicht ausschließlich auf die Ergebnisse automatisierter Verfahren, die einzelne Aspekte der Person der Betroffenen bewerten, gestützt werden. [2]Ergebnisse automatisierter Verfahren dürfen abweichend von Satz 1 für Entscheidungen verwendet werden, wenn

1. ein Gesetz dies vorsieht oder
2. der oder dem Betroffenen vor der Entscheidung ermöglicht wird, ihre oder seine besonderen persönlichen Interessen geltend zu machen.

## § 20 Video-Überwachung und -Aufzeichnung

(1) [1]Öffentliche Stellen dürfen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten (Video-Überwachung), soweit dies zur Erfüllung

ihrer Aufgaben oder zur Wahrnehmung eines Hausrechts erforderlich ist und schutzwürdige Belange Betroffener nicht überwiegen.

(2) [1]Der Umstand der Beobachtung und die dafür verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) [1]Die Speicherung oder weitere Verarbeitung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. [2]Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) [1]Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über die Speicherung oder Verarbeitung entsprechend § 26 zu unterrichten.

(5) [1]Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

## § 21 Veröffentlichung von Daten im Internet

(1) [1]Die Veröffentlichung personenbezogener Daten im Internet ist nur zulässig, wenn diese Form der Veröffentlichung durch eine Rechtsvorschrift erlaubt ist oder wenn die oder der Betroffene in diese Form der Veröffentlichung eingewilligt hat. [2]Sollen Daten nach § 11 Abs. 2 oder Daten von Mandatsträgern und öffentlich tätigen Personen im Rahmen eines Dienst- oder Arbeitsverhältnisses veröffentlicht werden, ist dies abweichend von Satz 1 zulässig, wenn sich die Daten auf das Mandat oder das Dienst- oder Arbeitsverhältnis beziehen und die schutzwürdigen Belange der oder des Betroffenen an der Geheimhaltung der Daten nicht überwiegen.

(2) [1]Die Veröffentlichung ist zu befristen; sie darf einen Zeitraum von fünf Jahren nicht überschreiten. [2]Mit Ablauf der Frist ist die Veröffentlichung aus dem Internet zu entfernen. [3]Wiederholungsveröffentlichungen sind zulässig. [4]Bei der Veröffentlichung ist ein Datum zu bestimmen, an dem die Veröffentlichung aus dem Internet entfernt wird.

# Abschnitt IV:
# Besondere Zwecke der Datenverarbeitung

## § 22 Datenverarbeitung für wissenschaftliche Zwecke

(1) [1]Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken durch öffentliche Stellen und die Übermittlung personenbezogener Daten durch öffentliche Stellen an Dritte, die die Daten zu wissenschaftlichen Zwecken verarbeiten wollen (Datenverarbeitung für wissenschaftliche Zwecke), soll in anonymisierter Form erfolgen. [2]Ist eine Anonymisierung nicht möglich, sollen die Daten pseudonymisiert werden. [3]§ 11 Abs. 6 gilt entsprechend.

(2) [1]Steht bei der übermittelnden Stelle zur Erfassung der Daten, zur Anonymisierung oder Pseudonymisierung nicht ausreichend Personal zur Verfügung, so können die mit der Forschung befassten Personen diese Aufgaben wahrnehmen, wenn sie zuvor zur Verschwiegenheit verpflichtet worden sind.

(3) [1]Ist weder eine Anonymisierung noch eine Pseudonymisierung möglich, ist die Datenverarbeitung für wissenschaftliche Zwecke zulässig, wenn

1. die oder der Betroffene in die Datenverarbeitung eingewilligt hat,
2. es sich nicht um Daten nach § 11 Abs. 3 handelt und schutzwürdige Belange der oder des Betroffenen wegen der Art der Daten oder wegen der Art der Verwendung für das jeweilige Forschungsvorhaben nicht beeinträchtigt sind oder
3. die Genehmigung der für die datenverarbeitende Stelle zuständigen obersten Aufsichtsbehörde vorliegt.

(4) [1]Die Genehmigung nach Absatz 3 Nr. 3 wird erteilt, wenn das öffentliche Interesse an der Durchführung des jeweiligen Forschungsvorhabens die schutzwürdigen Belange der oder des Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. [2]Die Genehmigung muss den Forschungszweck, die Art der zu verarbeitenden Daten, den Kreis der Betroffenen sowie bei Übermittlungen den Empfängerkreis bezeichnen und ist dem Unabhängigen Landeszentrum für Datenschutz mitzuteilen.

(5) [1]Sobald der Forschungszweck es gestattet, sind die Daten zu anonymisieren, hilfsweise zu pseudonymisieren. [2]Nach Maßgabe der Absätze 1 bis 3 dürfen die personenbezogenen Daten auch für einen anderen als den ursprünglichen Forschungszweck weiterverarbeitet werden.

(6) [1]Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. die oder der Betroffene eingewilligt hat oder

2. dies für die Darstellung von Forschungsergebnissen über Personen der Zeitgeschichte unerlässlich ist.

(7) [1]Die übermittelnde Stelle hat empfangende Stellen, auf die dieses Gesetz keine Anwendung findet, zu verpflichten, die Vorschriften der Absätze 5 und 6 einzuhalten und jederzeit Kontrollen durch das Unabhängige Landeszentrum für Datenschutz zu ermöglichen.

## § 23 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) [1]Öffentliche Stellen dürfen Daten der Beschäftigten vorbehaltlich besonderer gesetzlicher oder tarifvertraglicher Regelungen nur nach Maßgabe der §§ 85 bis 92 des Landesbeamtengesetzes verarbeiten.

(2) [1]Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 5 und 6 gespeichert oder in einem automatisierten Verfahren gewonnen werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

## § 24 Öffentliche Auszeichnungen

(1) [1]Zur Vorbereitung öffentlicher Auszeichnungen dürfen die Ministerpräsidentin oder der Ministerpräsident, das Ministerium für Inneres und für Bundesangelegenheiten sowie die von der Ministerpräsidentin oder dem Ministerpräsidenten besonders beauftragten Stellen die dazu erforderlichen personenbezogenen Daten auch ohne Kenntnis der Betroffenen erheben und weiterverarbeiten. [2]Eine Verarbeitung dieser Daten für andere Zwecke ist nur mit Einwilligung der Betroffenen zulässig.

(2) [1]Auf Anforderung der in Absatz 1 Satz 1 genannten Stellen dürfen andere öffentliche Stellen die zur Vorbereitung der Auszeichnung erforderlichen Daten übermitteln.

(3) [1]§ 27 findet keine Anwendung.

## § 25 weggefallen

# Abschnitt V:
# Rechte der Betroffenen

## § 26 Aufklärung, Benachrichtigung

(1) [1]Werden personenbezogene Daten bei den Betroffenen mit ihrer Kenntnis erhoben, so sind sie in geeigneter Weise aufzuklären über

1. die datenverarbeitende Stelle,
2. den Zweck der Datenverarbeitung,
3. die Rechtsvorschrift, die die Datenverarbeitung gestattet; liegt eine solche nicht vor, die Freiwilligkeit der Datenangabe,
4. die Folgen einer Nichtbeantwortung, wenn die Angaben für die Gewährung einer Leistung erforderlich sind,
5. ihre Rechte nach diesem Gesetz,
6. den Empfängerkreis bei beabsichtigten Übermittlungen sowie
7. die Auftragnehmenden bei beabsichtigter Datenverarbeitung im Auftrag.

[2]Die Pflicht zur Aufklärung nach Satz 1 entfällt, wenn den Betroffenen die Informationen bereits vorliegen.

(2) [1]Absatz 1 gilt nicht für

1. die Verfassungsschutzbehörden,
2. die Behörden der Staatsanwaltschaft,
3. die Behörden der Polizei,
4. die Gefahrenabwehrbehörden und
5. die Landesfinanzverwaltungen.

(3) [1]Werden die Daten ohne Kenntnis der Betroffenen erhoben, so sind diese in angemessener Weise über die verarbeiteten Daten und über die in Absatz 1 Satz 1 und Satz 2 Nr. 1 und 3 bis 5 genannten Umstände zu unterrichten. [2]Eine Pflicht zur Aufklärung besteht nicht, wenn die Benachrichtigung der Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. [3]Sollen

die Daten übermittelt werden, so hat die Benachrichtigung spätestens zeitgleich mit der Übermittlung zu erfolgen. [4]Satz 1 und 3 finden keine Anwendung, wenn die Betroffenen auf andere Weise Kenntnis von der Verarbeitung ihrer Daten erlangt haben.

## § 27 Auskunft an Betroffene

(1) [1]Den Betroffenen ist von der datenverarbeitenden Stelle auf Antrag Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Speicherung,
3. die Herkunft der Daten (§ 13 Abs. 1 Satz 3) und die Empfänger von Übermittlungen (§ 14 Abs. 3, § 15 Abs. 2 Satz 2),
4. die Auftragnehmenden bei Datenverarbeitung im Auftrag,
5. die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den gesetzlichen Bestimmungen entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind, sowie
6. die Funktionsweise von automatisierten Verfahren.

[2]Die Betroffenen sollen die Art der personenbezogenen Daten, über die Auskunft verlangt wird, näher bezeichnen.

(2) [1]Den Betroffenen kann statt der Auskunft Einsicht in die zu ihrer Person gespeicherten Daten gewährt werden. [2]Die Einsicht wird nicht gewährt, soweit diese mit personenbezogenen Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. [3]Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(3) [1]Die Auskunftserteilung oder die Gewährung von Einsicht unterbleibt, soweit eine Prüfung ergibt, dass

1. dadurch die Erfüllung der Aufgaben der datenverarbeitenden Stelle, einer übermittelnden Stelle oder einer empfangenden Stelle gefährdet würde,
2. dadurch die öffentliche Sicherheit gefährdet würde oder sonst dem Wohle des Bundes oder eines Landes schwere Nachteile entstehen würden oder
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen einer dritten Person geheimgehalten werden müssen.

(4) [1]Werden Auskunft oder Einsicht nicht gewährt, ist die oder der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, dass sie oder er sich an das Unabhängige Landeszentrum für Datenschutz wenden kann. [2]Eine

Begründung für die Auskunftsverweigerung erfolgt nicht, soweit dadurch der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

## § 27a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

[1]Stellt eine datenverarbeitende Stelle fest, dass bei ihr gespeicherte personenbezogene Daten im Sinne von § 11 Abs. 3 Satz 1 unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies unverzüglich den Betroffenen sowie dem Unabhängigen Landeszentrum für Datenschutz mitzuteilen. § 42 a Satz 2 bis 4 und 6 des Bundesdatenschutzgesetzes gilt entsprechend. [2]Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle eine Veröffentlichung auf der Internetseite des Unabhängigen Landeszentrums für Datenschutz.

## § 28 Berichtigung, Löschung, Sperrung

(1) [1]Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) [1]Personenbezogene Daten sind zu löschen, wenn

1. ihre Verarbeitung unzulässig ist oder
2. ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

(3) [1]Die datenverarbeitende Stelle legt in allgemeinen Regelungen über die Aufbewahrung von Daten den Zeitraum fest, innerhalb dessen die Daten als zur Aufgabenerfüllung erforderlich gelten. [2]Sind personenbezogene Daten in Akten untrennbar im Sinne von § 11 Abs. 4 Satz 2 gespeichert, ist die Löschung nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist.

(4) [1]Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit von der oder dem Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit nachweisen lässt,
2. sie zur Aufgabenerfüllung nicht mehr erforderlich sind, Rechtsvorschriften jedoch die weitere Aufbewahrung anordnen,
3. die oder der Betroffene anstelle der Löschung die Sperrung verlangt,
4. die Löschung die Betroffene oder den Betroffenen in der Verfolgung ihrer oder seiner Rechte oder in sonstigen schutzwürdigen Belangen beeinträchtigen würde oder

5. eine Löschung gemäß Absatz 2 Satz 3 nicht erfolgt.

(5) [1]Gesperrte Daten dürfen über die Speicherung hinaus ohne Einwilligung der oder des Betroffenen nicht mehr weiterverarbeitet werden, es sei denn, dass Rechtsvorschriften die Verarbeitung zulassen oder die Verarbeitung durch die datenverarbeitende Stelle zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der datenverarbeitenden Stelle oder von Dritten liegenden Gründen unerlässlich ist. [2]Die Gründe für die Verarbeitung gesperrter Daten sind zu dokumentieren.

(6) [1]Von der Berichtigung, Sperrung oder Löschung nach Absatz 2 Nr. 1 sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt wurden. [2]Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt werden.

## § 29 Einwand gegen die Verarbeitung

(1) [1]Die Betroffenen haben das Recht, schriftlich unter Hinweis auf besondere persönliche Gründe Einwand gegen die Verarbeitung ihrer Daten allgemein oder gegen bestimmte Formen der Verarbeitung zu erheben. [2]Der Einwand ist begründet, wenn ein schutzwürdiges Interesse der oder des Betroffenen das öffentliche Interesse an der Datenverarbeitung im Einzelfall überwiegt. [3]In diesem Fall ist die Datenverarbeitung insgesamt oder in bestimmten Formen unzulässig.

(2) [1]Absatz 1 findet keine Anwendung bei Verfahren, die

1. nach dem Landesverfassungsschutzgesetz geführt werden,
2. der Gefahrenabwehr dienen,
3. der Strafverfolgung dienen oder
4. der Steuerfahndung dienen.

## § 30 Schadensersatz

(1) [1]Entsteht der oder dem Betroffenen durch eine unzulässige oder unrichtige Verarbeitung ihrer oder seiner personenbezogenen Daten in einem automatisierten Verfahren ein Schaden, so ist ihr oder ihm der Träger jeder für die Verarbeitung verantwortlichen Stelle unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) [1]In Fällen einer schweren Verletzung des Persönlichkeitsrechts kann die oder der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen.

(3) [1]Die ersatzpflichtige Stelle haftet jeder oder jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 125.000 Euro. [2]Mehrere Ersatzpflichtige haften gesamtschuldnerisch.

(4) [1]Auf das Mitverschulden der oder des Betroffenen und die Verjährung des Entschädigungsanspruchs sind die §§ 254, 839 Abs. 3, §§ 195 und 199 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(5) [1]Die Geltendmachung weitergehender Schadensersatzansprüche aufgrund anderer Vorschriften bleibt unberührt.

### § 31 Unabdingbarkeit

[1]Die Rechte der Betroffenen aus diesem Gesetz können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

## Abschnitt VI:
## Das Unabhängige Landeszentrum für Datenschutz

### § 32 Errichtung und Rechtsform

(1) [1]Das Land Schleswig-Holstein errichtet unter dem Namen "Unabhängiges Landeszentrum für Datenschutz" eine rechtsfähige Anstalt des öffentlichen Rechts. Sitz der Anstalt ist die Landeshauptstadt Kiel.

(2) [1]Die Anstalt besitzt Dienstherrnfähigkeit und führt das Landessiegel.

### § 33 Trägerschaft, Anstaltslast und Gewährträgerhaftung

(1) [1]Träger der Anstalt ist das Land Schleswig-Holstein.

(2) [1]Für Verbindlichkeiten der Anstalt haftet der Anstaltsträger Dritten gegenüber, soweit nicht eine Befriedigung aus dem Vermögen der Anstalt möglich ist.

(3) [1]Der Anstaltsträger stellt sicher, dass die Anstalt ihre gesetzlichen Aufgaben erfüllen kann.

### § 34 Organ

(1) [1]Organ der Anstalt ist der Vorstand.

(2) [1]Der Vorstand besteht aus der Leiterin oder dem Leiter der Anstalt. Sie oder er führt die Bezeichnung “Landesbeauftragte für Datenschutz“ oder “Landesbeauftragter für Datenschutz“.

(3) [1]Die Landesbeauftragte oder der Landesbeauftragte für Datenschutz führt die Geschäfte der Anstalt und vertritt sie gerichtlich und außergerichtlich. [2]In ihrem oder seinem Verhinderungsfalle vertritt die oder der stellvertretende Landesbeauftragte für Datenschutz die Anstalt und führt deren Geschäfte.

## § 35 Wahl und Amtszeit der oder des Landesbeauftragten für Datenschutz

(1) [1]Der Landtag wählt ohne Aussprache die Landesbeauftragte oder den Landesbeauftragten für Datenschutz mit mehr als der Hälfte seiner Mitglieder für die Dauer von fünf Jahren. [2]Die Wiederwahl ist zulässig.

(2) [1]Vorschlagsberechtigt sind die Fraktionen des Schleswig-Holsteinischen Landtages. [2]Kommt vor Ablauf der Amtszeit eine Neuwahl nicht zustande, führt die oder der Landesbeauftragte für Datenschutz das Amt bis zur Neuwahl weiter.

(3) [1]Der Landtag kann die Landesbeauftragte oder den Landesbeauftragten für Datenschutz mit einer Mehrheit von zwei Dritteln seiner Mitglieder abwählen.

## § 36 Rechtsstellung der oder des Landesbeauftragten für Datenschutz

(1) [1]Die Ministerpräsidentin oder der Ministerpräsident ernennt die Landesbeauftragte oder den Landesbeauftragten zur Beamtin oder zum Beamten auf Zeit. [2]Die oder der Landesbeauftragte für Datenschutz kann jederzeit die Entlassung verlangen. [3]Die Ministerpräsidentin oder der Ministerpräsident ist Dienstvorgesetzte oder Dienstvorgesetzter der oder des Landesbeauftragten für Datenschutz. [4]Die oder der Landesbeauftragte für Datenschutz untersteht der Dienstaufsicht nur, soweit nicht seine Unabhängigkeit bei der Aufgabenwahrnehmung beeinträchtigt wird.

(2) [1]Der Landtag und seine Ausschüsse können die Anwesenheit der oder des Landesbeauftragten für Datenschutz in ihren Sitzungen verlangen.

(3) [1]Die oder der Landesbeauftragte für Datenschutz ist Dienstvorgesetzte oder Dienstvorgesetzter und oberste Dienstbehörde der in der Anstalt beschäftigten Beamtinnen und Beamten.

(4) [1]Die oder der Landesbeauftragte für Datenschutz bestellt eine Mitarbeiterin zur Stellvertreterin oder einen Mitarbeiter zum Stellvertreter und ernennt die Beamtinnen oder Beamten der Anstalt.

## § 37 Satzung

[1]Der Vorstand ist zum Erlass und zur Änderung der Satzung befugt.

## § 38 Beirat

[1]Der Vorstand kann einen Beirat berufen, der den Vorstand der Anstalt berät. [2]Das Nähere regelt die Satzung.

## § 39 Aufgaben des Unabhängigen Landeszentrums für Datenschutz

(1) [1]Das Unabhängige Landeszentrum für Datenschutz nimmt die ihm zugewiesenen Aufgaben in Unabhängigkeit wahr und ist nur dem Gesetz unterworfen. [2]Die §§ 50 bis 52 des Landesverwaltungsgesetzes sind nicht anzuwenden; im Übrigen sind die Rechtsvorschriften, die für die der Aufsicht des Landes unterstehenden rechtsfähigen Anstalten des öffentlichen Rechts gelten, anzuwenden.

(2) [1]Das Unabhängige Landeszentrum für Datenschutz überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen, auf die dieses Gesetz Anwendung findet. [2]Die Gerichte und der Landesrechnungshof unterliegen seiner Kontrolle, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

(3) [1]Das Unabhängige Landeszentrum für Datenschutz ist die zuständige Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes über nicht-öffentliche Stellen im Anwendungsbereich des Dritten Abschnitts des Bundesdatenschutzgesetzes.

(4) [1]Das Unabhängige Landeszentrum für Datenschutz berät die obersten Landesbehörden sowie die sonstigen öffentlichen Stellen in Fragen des Datenschutzes, der Datensicherheit und der damit zusammenhängenden Datenverarbeitungstechniken sowie deren Sozialverträglichkeit. [2]Zu diesem Zweck können Empfehlungen zur Verbesserung des Datenschutzes gegeben werden. [3]Auf Anforderungen des Landtages, des Petitionsausschusses des Landtages oder einer obersten Landesbehörde soll das Unabhängige Landeszentrum für Datenschutz ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nachgehen.

(5) [1]Auf Anforderung des Landtages, einzelner Fraktionen des Landtages oder der Landesregierung hat das Unabhängige Landeszentrum für Datenschutz Gutachten zu erstellen und Berichte zu erstatten. [2]Es legt dem Landtag alle zwei Jahre einen Tätigkeitsbericht vor.

(6) [1]Für die Erfüllung der Aufgaben ist die notwendige Personal- und Sachausstattung zur Verfügung zu stellen; die Mittel sind im Einzelplan des Landtages in einem gesonderten Kapitel auszuweisen.

## § 40 Anrufung des Unabhängigen Landeszentrums für Datenschutz

[1]Jede oder jeder hat das Recht, sich unmittelbar an das Unabhängige Landeszentrum für Datenschutz zu wenden, wenn sie oder er annimmt, dass bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen datenschutzrechtliche Vorschriften verletzt wurden. [2]Dies gilt auch für Beschäftigte der öffentlichen Stellen, ohne dass der Dienstweg einzuhalten ist.

## § 41 Kontrollaufgaben

(1) [1]Die öffentlichen Stellen sind verpflichtet, das Unabhängige Landeszentrum für Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. [2]Ihm ist dabei insbesondere

1. Auskunft zu erteilen sowie Einsicht in Unterlagen und Dateien zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen; besondere Amts- und Berufsgeheimnisse stehen dem nicht entgegen;
2. Zutritt zu Diensträumen zu gewähren.

[3]Das Unabhängige Landeszentrum für Datenschutz darf im Rahmen von Kontrollen personenbezogene Daten auch ohne Kenntnis der Betroffenen erheben. [4]Die Benachrichtigung der Betroffenen richtet sich nach § 42 Abs. 4.

(2) [1]Stellt die jeweils zuständige oberste Landesbehörde im Einzelfall fest, dass durch eine mit der Einsicht verbundene Bekanntgabe personenbezogener Daten die Sicherheit des Bundes oder eines Landes gefährdet wird, dürfen die Rechte nach Absatz 1 nur von der oder dem Landesbeauftragten für Datenschutz persönlich oder den von ihr oder ihm schriftlich besonders damit betrauten Beauftragten ausgeübt werden.

## § 42 Beanstandungen

(1) [1]Stellt das Unabhängige Landeszentrum für Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten bei öffentlichen Stellen fest, so fordert es diese zur Mängelbeseitigung auf.

(2) [1]Bei erheblichen Verstößen oder sonstigen erheblichen Mängeln spricht das Unabhängige Landeszentrum für Datenschutz gegenüber der öffentlichen Stelle eine Beanstandung aus.[2]Es soll zuvor die öffentliche Stelle zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auffordern und die zuständige Aufsichtsbehörde über die Beanstandung unterrichten.

(3) [1]Mit der Feststellung von Mängeln und der Beanstandung sollen Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbunden werden.

(4) [1]Die Betroffenen können mit Kenntnis der datenverarbeitenden Stelle nach pflichtgemäßem Ermessen von Verstößen gegen die Vorschriften dieses Gesetzes oder andere Datenschutzvorschriften unterrichtet werden.

## § 43 Serviceaufgaben

(1) [1]Das Unabhängige Landeszentrum für Datenschutz berät und informiert die Bürgerinnen und Bürger über alle Fragen des Datenschutzes und der Datensicherheit, insbesondere über die ihnen bei der Verarbeitung ihrer Daten zustehenden Rechte sowie über geeignete technische Maßnahmen zum Selbstdatenschutz.

(2) [1]Öffentliche Stellen können ihre technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten sowie die datenschutzrechtliche Zulässigkeit der Datenverarbeitung durch das Unabhängige Landeszentrum für Datenschutz prüfen und beurteilen lassen.

(3) [1]Das Unabhängige Landeszentrum für Datenschutz führt Fortbildungsveranstaltungen zu den Themen Datenschutz und Datensicherheit durch. [2]Es berät nicht-öffentliche Stellen auf Anfrage in Fragen von Datenschutz und Datensicherheit.

(4) [1]Das Unabhängige Landeszentrum für Datenschutz kann für die Wahrnehmung der Aufgaben nach den Absätzen 1 bis 3 sowie nach § 9 Abs. 1 Entgelte erheben.

# Abschnitt VII: Schlussvorschriften

## § 44 Ordnungswidrigkeiten

(1) [1]Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verarbeitet, verändert, übermittelt, zum Abruf bereithält oder löscht,

2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung an sich oder andere veranlasst.

(2) [1]Ordnungswidrig handelt auch,

1. wer anonymisierte oder pseudonymisierte Daten mit anderen Informationen zusammenführt und dadurch die Betroffene oder den Betroffenen wieder bestimmbar macht,

2. wer sich bei pseudonymisierten Daten entgegen den Vorschriften dieses Gesetzes Zugriff auf die Zuordnungsfunktion verschafft oder

3. wer es vollständig unterlässt, technischorganisatorische Maßnahmen nach § 5 Abs. 1 zu treffen.

(3) [1]Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 Euro geahndet werden.

## § 45 Übergangsregelungen

[1]Am 26. Januar 2012 eingesetzte automatisierte Verfahren müssen bis zum Ablauf des 31. Dezember 2013 den § 6 Abs. 4 Satz 3, § 8 Abs. 4 und §§ 14 und 15 entsprechen.

## § 46 Inkrafttreten, Außerkrafttreten

(1) [1]Dieses Gesetz tritt am 1. Juli 2000 in Kraft.

(2) [1]Gleichzeitig treten

1. das Landesdatenschutzgesetz vom 30. Oktober 1991 (GVOBl. Schl.-H. S. 555), zuletzt geändert durch Gesetz vom 25. November 1999 (GVOBl. Schl.-H. S. 414),

2. das Gesetz zur Errichtung des Unabhängigen Landeszentrums für Datenschutz vom 25. November 1999 (GVOBl. Schl.-H. S. 414) und

3. die Landesverordnung über die zuständige Aufsichtsbehörde nach dem Bundesdatenschutzgesetz vom 8. Dezember 1992 (GVOBl. Schl.-H. S 533), geändert gemäß Verordnung vom 24. Oktober 1996 (GVOBl. Schl.-H. S. 652), außer Kraft.

# Datenschutzverordnung (DSVO)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung) |
| **Amtliche Abkürzung:** | DSVO |
| **Ausfertigung:** | 05.12.2013, GVOBl. 2013 S. 554 |
| **Inkrafttreten:** | 01.01.2014 |
| **Außerkrafttreten:** | 31.12.2018 |

## Inhaltsübersicht


| | | |
|---|---|---|
| § 1 | Anwendungsbereich | 89 |
| § 2 | Begriffsbestimmungen | 90 |
| § 3 | Verfahrensdokumentation | 90 |
| § 4 | Dokumentation der Sicherheitsmaßnahmen | 91 |
| § 5 | Dokumentation des Tests und der Freigabe | 92 |
| § 6 | Übergangsregelung | 93 |
| § 7 | Inkrafttreten, Außerkrafttreten | 93 |


Aufgrund des § 5 Abs. 3 des Landesdatenschutzgesetzes (LDSG) vom 9. Februar 2000 (GVOBl. Schl.-H. S. 169), zuletzt geändert durch Gesetz vom 6. April 2013 (GVOBl. Schl.-H. S. 125), verordnet die Landesregierung:

## § 1 Anwendungsbereich

(1) [1]Diese Verordnung regelt die Dokumentation automatisierter Verfahren bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 3 Abs. 1 LDSG) sowie deren Tests und die Freigabe dieser Verfahren.

(2) [1]Soweit besondere Rechtsvorschriften die Einzelheiten der Dokumentation automatisierter Verarbeitung personenbezogener Daten regeln, finden die Vorschriften dieser Verordnung keine Anwendung.

## § 2 Begriffsbestimmungen

[1]Im Sinne dieser Verordnung sind

| | |
|---|---|
| automatisierte Verfahren | Arbeitsabläufe mit Hilfe von informationstechnischen Geräten, Programmen und automatisierten Dateien, |
| informationstechnische Geräte | die apparative Ausstattung von automatisierten Verfahren (Hardware), |
| Programme | Arbeitsanweisungen an informationstechnische Geräte (Software), |
| Informationstechnik | ein Sammelbegriff für informationstechnische Geräte und Programme. |

## § 3 Verfahrensdokumentation

(1) [1]Automatisierte Verfahren sind zu dokumentieren. [2]Die Dokumentation muss eine schriftliche, verfahrensbezogene Darstellung

1. des Einsatzes von Informationstechnik (Absatz 2),
2. der Sicherheitsmaßnahmen (§ 4) und
3. des Vorgehens bei Test und Freigabe (§ 5)

enthalten. [3]Von der Dokumentation kann ausnahmsweise abgesehen werden, wenn durch automatisierte Verfahren die Rechte der Betroffenen nur geringfügig berührt werden. [4]In diesem Fall ist eine entsprechende Begründung schriftlich niederzulegen.

(2) [1]Zur Darstellung des ordnungsgemäßen Einsatzes von Informationstechnik sind zu dokumentieren:

1. Die Rechtsgrundlage, der Verfahrenszweck (§ 7 Abs. 1 Satz 3 Nr. 2 LDSG), eine Datenfeldbeschreibung und die Maßnahmen zur Datenvermeidung und Datensparsamkeit nach § 4 Abs. 1 LDSG sowie zur Datentrennung nach § 11 Abs. 4 LDSG,
2. die für das Verfahren verwendeten informationstechnischen Geräte einschließlich des Standorts,
3. die für das Verfahren verwendeten Programme, die zur Inbetriebnahme getätigten Schritte und die für die Inbetriebnahme verantwortlichen Personen,
4. bei vernetzten informationstechnischen Geräten die physikalischen und logischen Verbindungen zu anderen informationstechnischen Geräten (Netzplan) sowie eine Darstellung, an welche Systeme welche personenbezogenen Daten innerhalb der Organisation übertragen werden, inklusive der Schnittstellen zu anderen Organisationen (Datenflussdiagramm),

5. die technischen und organisatorischen Vorgaben für die Datenverarbeitung einschließlich der Darstellung, welche Personen für welche Aspekte der Datenverarbeitung verantwortlich und berechtigt sind,

6. die vorgesehenen und durchgeführten Datenübermittlungen einschließlich der Empfängerinnen und Empfänger der Daten,

7. das Vorliegen einer Datenverarbeitung im Auftrag einschließlich der schriftlichen Vereinbarungen gemäß § 17 Abs. 3 LDSG,

8. die Maßnahmen zum Erfüllen von Auskunftsansprüchen von Betroffenen (§ 27 LDSG) und

9. die Maßnahmen für die Berichtigung, die Löschung und die Sperrung personenbezogener Daten (§ 28 LDSG).

(3) [1]Die Dokumentation muss für sachkundige Personen in angemessener Zeit nachvollziehbar sein. [2]Sie ist nach jeder Änderung des automatisierten Verfahrens fortzuschreiben und mindestens fünf Jahre nach der letzten automatisierten Verarbeitung personenbezogener Daten aufzubewahren.

(4) [1]Jede Änderung an informationstechnischen Geräten, Programmen oder Verfahren einschließlich der Personen, die die Veränderungen vorgenommen haben, ist entsprechend Absatz 2 zu dokumentieren.

(5) [1]Die Dokumentation mehrerer automatisierter Verfahren oder die Dokumentation von Teilbereichen eines automatisierten Verfahrens (Absatz 2) kann zusammengefasst werden.

## § 4 Dokumentation der Sicherheitsmaßnahmen

(1) [1]Die technischen und organisatorischen Maßnahmen, die gemäß der §§ 5, 6 und 8 LDSG getroffen wurden, sind zu dokumentieren. [2]Dabei kann auf die Darstellung nach § 3 Abs. 2 Bezug genommen werden.

(2) [1]Die Erforderlichkeit und Angemessenheit der Sicherheitsmaßnahmen ist durch eine Analyse möglicher Gefährdungen für die Betroffenen unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten zu dokumentieren (Risikoanalyse). Es ist darzulegen, welche Gefährdungen aus welchen Gründen nicht oder nur zum Teil durch die getroffenen Maßnahmen ausgeschlossen werden können (Restrisiko-Dokumentation).

(3) [1]Die Dokumentation der technischen und organisatorischen Maßnahmen (Absatz 1) und die Analyse möglicher Gefährdungen (Absatz 2) müssen

1. Personal,

2. Räume und Gebäude,

3. informationstechnische Geräte und Programme und

4. die interne und externe Vernetzung der informationstechnischen Geräte behandeln.

(4) [1]Werden Daten verschlüsselt oder erfolgt eine elektronische Signierung, müssen die technischen und organisatorischen Maßnahmen zur Vergabe und zum Entzug von Schlüsseln sowie zur Schlüsselhinterlegung dokumentiert werden.

(5) [1]Für die bei der Datenverarbeitung zu erzeugenden Protokolldaten gemäß der §§ 6 Abs. 2 und 4 sowie § 8 Abs. 4 LDSG ist unter Berücksichtigung von § 23 Abs. 2 LDSG zu dokumentieren, welche technischen und organisatorischen Maßnahmen hinsichtlich des Zugriffs, der Auswertung und der Löschung der Protokolldaten getroffen wurden.

(6) [1]Das Datenschutzmanagement ist zu dokumentieren. Dies betrifft die getroffenen technischen und organisatorischen Maßnahmen, um die Tätigkeiten gemäß § 6 Abs. 5, § 8 Abs. 5 und § 10 Abs. 4 LDSG zu ermöglichen und zu unterstützen. Dazu gehören Aussagen zur Einbindung der oder des behördlichen Datenschutzbeauftragten in geplante Verfahren, zur Prüfung von Verfahren, zur Bearbeitung der Eingaben von Betroffenen und zu Kontrollen der technischen und organisatorischen Maßnahmen.

(7) [1]Liegt eine Verarbeitung personenbezogener Daten im Auftrag gemäß § 17 LDSG vor, sind die beim Auftragnehmer getroffenen technischen und organisatorischen Sicherheitsmaßnahmen im Sinne von § 4 Abs. 1 und 2 von der Daten verarbeitenden Stelle zu dokumentieren.

## § 5 Dokumentation des Tests und der Freigabe

(1) [1]Die in automatisierten Verfahren eingesetzten informationstechnischen Geräte und Programme sowie die in der Dokumentation festgelegten Sicherheitsmaßnahmen (§ 4) sind vor der Aufnahme der Verarbeitung personenbezogener Daten zu testen. [2]Die Testmaßnahmen und die dabei erzielten Ergebnisse sind zu dokumentieren. [3]Die Dokumentation soll durch eine Darstellung der einzelnen Prüfschritte erfolgen und die verwendeten Ein- und erhaltenen Ausgabedaten beinhalten, soweit dies technisch möglich ist. [4]Festgestellte Mängel sind durch die Leiterin oder den Leiter der Daten verarbeitenden Stelle oder eine befugte Person nach ihrer Bedeutung zu gewichten.

(2) [1]Die nach § 5 Abs. 2 LDSG vorzunehmende Freigabe automatisierter Verfahren hat schriftlich zu erfolgen. [2]Sie ist nur zulässig, soweit bei den Tests keine wesentlichen Mängel festgestellt wurden. [3]Die Beseitigung geringfügiger Mängel muss in angemessener Zeit vorgenommen werden.

(3) [1]Test und Freigabe können in einem gestuften Verfahren erfolgen. [2]In jeder Stufe können der Test und die Freigabe auf die geplante Verarbeitung personenbezogener Daten begrenzt werden.

(4) [1]Soweit ein Verfahren von mehreren Behörden eingesetzt werden soll, können eigene Tests der Daten verarbeitenden Behörde mit anderen Testergebnissen von Behörden oder Stellen kombiniert oder ergänzt werden. [2]Die kombinierten oder ergänzten Tests sind gemäß Absatz 1 zu dokumentieren.

## § 6 Übergangsregelung

(1) [1]Bereits eingesetzte automatisierte Verfahren müssen den Regelungen dieser Verordnung spätestens drei Jahre nach ihrem Inkrafttreten entsprechen.[2]Nach Inkrafttreten dieser Verordnung neu eingeführte automatisierte Verfahren müssen spätestens sechs Monate nach ihrer Einführung den Regelungen dieser Verordnung entsprechen.

(2) [1]Bei einer wesentlichen Änderung eines automatisierten Verfahrens gemäß § 8 Abs. 1 LDSG oder wenn Daten im Sinne des § 11 Abs. 3 LDSG verarbeitet werden, ist die Anpassung bereits vor Ablauf der Übergangsfrist im Rahmen der notwendigen Vorabkontrolle gemäß § 9 LDSG durchzuführen.

## § 7 Inkrafttreten, Außerkrafttreten

[1]Diese Verordnung tritt am 1. Januar 2014 in Kraft. Sie tritt mit Ablauf des 31. Dezember 2018 außer Kraft.

# Informationszugangsgesetz (IZG-SH)

**Vollständige Bezeichnung:** Informationszugangsgesetz für das Land Schleswig-Holstein
**Amtliche Abkürzung:** IZG-SH
**Ausfertigung:** 19.01.2012, GVOBl. 2012 S. 89
**Inkrafttreten:** 27.01.2012

## Inhaltsübersicht


| | | |
|---|---|---|
| § 1 | Zweck des Gesetzes, Anwendungsbereich | 95 |
| § 2 | Begriffsbestimmungen | 96 |
| § 3 | Anspruch auf Zugang zu Informationen | 98 |
| § 4 | Antragstellung | 98 |
| § 5 | Verfahren, Frist | 98 |
| § 6 | Ablehnung des Antrags | 99 |
| § 7 | Rechtsschutz | 99 |
| § 8 | Unterstützung des Zugangs zu Umweltinformationen | 100 |
| § 9 | Schutz öffentlicher Belange | 100 |
| § 10 | Schutz privater Belange | 101 |
| § 11 | Unterrichtung der Öffentlichkeit | 101 |
| § 12 | Kosten | 103 |
| § 13 | Anrufung der oder des Landesbeauftragten für den Datenschutz | 103 |
| § 14 | Übergangsvorschrift | 103 |


## § 1 Zweck des Gesetzes, Anwendungsbereich

(1) [1]Zweck dieses Gesetzes ist es, den rechtlichen Rahmen für den freien Zugang zu Informationen bei informationspflichtigen Stellen sowie für die Verbreitung dieser Informationen zu schaffen.

(2) [1]Dieses Gesetz gilt für den Zugang zu Informationen, über die die in § 2 Abs. 3 bestimmten informationspflichtigen Stellen verfügen.

## § 2 Begriffsbestimmungen

(1) [1]Im Sinne dieses Gesetzes sind

1. Informationen alle in Schrift-, Bild-, Ton- oder Datenverarbeitungsform oder auf sonstigen Informationsträgern bei informationspflichtigen Stellen vorhandene Zahlen, Daten, Fakten, Erkenntnisse oder sonstige Auskünfte;

2. Informationsträger alle Medien, die Informationen in Schrift-, Bild-, Ton- oder Datenverarbeitungsform oder in sonstiger Form speichern können.

(2) [1]Umweltinformationen sind alle Daten über

1. den Zustand von Umweltbestandteilen wie Luft und Atmosphäre, Wasser, Boden, Land, Landschaft und natürliche Lebensräume einschließlich Feuchtgebiete, Küsten- und Meeresgebiete, die Artenvielfalt und ihre Bestandteile, einschließlich gentechnisch veränderter Organismen, sowie die Wechselwirkungen zwischen diesen Bestandteilen,

2. Faktoren, die sich auf die Umweltbestandteile im Sinne der Nummer 1 auswirken oder wahrscheinlich auswirken; hierzu gehören insbesondere Stoffe, Energie, Lärm und Strahlung, Abfälle aller Art sowie Emissionen, Ableitungen und sonstige Freisetzungen von Stoffen in die Umwelt,

3. Maßnahmen oder Tätigkeiten, die

   (a) sich auf die Umweltbestandteile im Sinne der Nummer 1 oder auf Faktoren im Sinne der Nummer 2 auswirken oder wahrscheinlich auswirken oder

   (b) den Schutz von Umweltbestandteilen im Sinne der Nummer 1 bezwecken;

   dazu gehören auch politische Konzepte, Rechts- und Verwaltungsvorschriften, Abkommen, Vereinbarungen, Pläne und Programme,

4. Berichte über die Umsetzung des Umweltrechts,

5. Kosten-Nutzen-Analysen oder sonstige wirtschaftliche Analysen und Annahmen, die zur Vorbereitung oder Durchführung von Maßnahmen oder Tätigkeiten im Sinne der Nummer 3 verwendet werden, und

6. den Zustand der menschlichen Gesundheit und Sicherheit, die Lebensbedingungen des Menschen sowie Kulturstätten und Bauwerke, soweit sie jeweils vom Zustand der Umweltbestandteile im Sinne der Nummer 1, von Faktoren im Sinne der Nummer 2 oder Maßnahmen oder Tätigkeiten im Sinne der Nummer 3 betroffen sind oder sein können; hierzu gehört auch die Kontamination der Lebensmittelkette.

(3) [1]Informationspflichtige Stellen sind

1. Behörden des Landes, der Gemeinden, Kreise und Ämter sowie die sonstigen juristischen Personen des öffentlichen Rechts, einschließlich der sie beratenden satzungsmäßigen Gremien,

2. natürliche und juristische Personen des Privatrechts sowie nichtrechtsfähige Vereinigungen, soweit ihnen Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handlungsformen des öffentlichen Rechts übertragen wurden,

3. bei Umweltinformationen darüber hinaus natürliche oder juristische Personen des Privatrechts, soweit sie im Zusammenhang mit der Umwelt öffentliche Aufgaben wahrnehmen und dabei der Kontrolle des Landes oder einer unter Aufsicht des Landes stehenden juristischen Person des öffentlichen Rechts unterliegen.

(4) [1]Zu den informationspflichtigen Stellen gehören nicht:

1. Der Landtag im Rahmen seiner Gesetzgebungstätigkeit,

2. die obersten Landesbehörden, soweit sie im Rahmen der Gesetzgebungsverfahren oder beim Erlass von Rechtsverordnungen tätig werden,

3. die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden, soweit sie als Organe der Rechtspflege tätig werden,

4. der Landesrechnungshof, soweit er in richterlicher Unabhängigkeit tätig wird und es sich nicht um Umweltinformationen handelt.

(5) [1]Eine informationspflichtige Stelle verfügt über Informationen, wenn diese bei ihr vorhanden sind oder an anderer Stelle für sie bereitgehalten werden. [2]Ein Bereithalten liegt vor, wenn eine natürliche oder juristische Person, die selbst nicht informationspflichtige Stelle ist, Informationen für eine informationspflichtige Stelle aufbewahrt, auf die diese Stelle einen Übermittlungsanspruch hat.

(6) [1]Kontrolle im Sinne des Absatzes 3 Nr. 3 liegt vor, wenn

1. die Person des Privatrechts bei der Wahrnehmung der öffentlichen Aufgabe gegenüber Dritten besonderen Pflichten unterliegt oder über besondere Rechte verfügt, insbesondere ein Kontrahierungszwang oder ein Anschluss- und Benutzungszwang besteht, oder

2. ein oder mehrere Träger der öffentlichen Verwaltung alleine oder zusammen, unmittelbar oder mittelbar

   (a) die Mehrheit des gezeichneten Kapitals des Unternehmens besitzen,

   (b) über die Mehrheit der mit den Anteilen des Unternehmens verbundenen Stimmrechte verfügen oder

   (c) mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans des Unternehmens bestellen können.

## § 3 Anspruch auf Zugang zu Informationen

[1]Jede natürliche oder juristische Person hat ein Recht auf freien Zugang zu den Informationen, über die eine informationspflichtige Stelle verfügt. [2]Rechte auf Zugang zu Informationen, die andere Gesetze einräumen, bleiben unberührt.

## § 4 Antragstellung

(1) [1]Informationen werden von der informationspflichtigen Stelle auf Antrag zugänglich gemacht.

(2) [1]Der Antrag muss erkennen lassen, zu welchen Informationen der Zugang begehrt wird. [2]Ist der Antrag zu unbestimmt, so ist die antragstellende Person so bald wie möglich, spätestens innerhalb eines Monats aufzufordern, den Antrag zu präzisieren. [3]Nach Eingang des präzisierten Antrags bei der informationspflichtigen Stelle beginnt die Frist zur Beantwortung des Antrags erneut. [4]Die informationspflichtigen Stellen haben die antragstellende Person bei der Stellung und Präzisierung von Anträgen zu unterstützen.

(3) [1]Wird der Antrag bei einer informationspflichtigen Stelle gestellt, die nicht über die begehrten Informationen verfügt, leitet sie den Antrag so bald wie möglich an die über die Informationen verfügende Stelle weiter, wenn ihr diese bekannt ist, und unterrichtet die antragstellende Person hierüber. [2]Anstelle der Weiterleitung des Antrags kann sie die antragstellende Person auch auf andere ihr bekannte informationspflichtige Stellen hinweisen, die über die Informationen verfügen.

## § 5 Verfahren, Frist

(1) [1]Die in Anspruch genommene Stelle hat der antragstellenden Person Auskunft zu erteilen, Akteneinsicht zu gewähren, Kopien, auch durch Versendung, zur Verfügung zu stellen oder die Informationsträger zugänglich zu machen, die die begehrten Informationen enthalten. [2]Wird eine bestimmte Art des Informationszugangs beantragt, so entspricht die in Anspruch genommene Stelle diesem Antrag, es sei denn, die in Anspruch genommene Stelle hat wichtige Gründe, die Informationen auf andere Art zugänglich zu machen. [3]Soweit Informationen der antragstellenden Person bereits auf andere, leicht zugängliche Art, insbesondere durch Verbreitung nach § 11, zur Verfügung stehen, kann die in Anspruch genommene Stelle die Person auf diese Art des Informationszugangs verweisen.

(2) [1]Soweit ein Anspruch nach § 3 besteht, sind die Informationen der antragstellenden Person unter Berücksichtigung etwaiger von ihr angegebener Zeitpunkte sobald wie möglich, spätestens jedoch mit Ablauf eines Monats nach Eingang des Antrags bei der informationspflichtigen Stelle zugänglich zu machen. [2]Sind die Informationen derart umfangreich und komplex, dass die Frist nicht eingehalten werden kann, so kann die informationspflichtige Stelle die Frist auf höchstens zwei Monate verlängern. [3]Wird von der Fristverlängerung nach Satz 2 Gebrauch gemacht, ist dies der antragstellenden Person so bald wie

möglich, spätestens innerhalb eines Monats nach Antragseingang unter Angabe der Gründe mitzuteilen.

## § 6 Ablehnung des Antrags

(1) [1]Wird der Antrag ganz oder teilweise abgelehnt, ist dies der antragstellenden Person innerhalb der Fristen nach § 5 Abs. 2 mitzuteilen. [2]Eine Ablehnung liegt auch dann vor, wenn nach § 5 Abs. 1 der Informationszugang auf andere Art gewährt oder die antragstellende Person auf eine andere Art des Informationszugangs verwiesen wird. [3]Der antragstellenden Person sind die Gründe für die Ablehnung mitzuteilen; in den Fällen des § 9 Abs. 2 Nr. 3 ist darüber hinaus die Stelle, die das Material aufbereitet sowie der voraussichtliche Zeitpunkt der Fertigstellung mitzuteilen. [4]§ 109 Abs. 3 des Landesverwaltungsgesetzes findet keine Anwendung.

(2) [1]Wenn der Antrag schriftlich gestellt worden ist oder die antragstellende Person dies wünscht, hat die Ablehnung schriftlich zu erfolgen. [2]Sie ist auf Verlangen der antragstellenden Person in elektronischer Form mitzuteilen, wenn der Zugang hierfür eröffnet ist.

(3) [1]Liegt ein Ablehnungsgrund nach den §§ 9 oder 10 vor, sind die hiervon nicht betroffenen Informationen zugänglich zu machen, soweit sie ausgesondert werden können.

(4) [1]Die antragstellende Person ist im Falle der vollständigen oder teilweisen Ablehnung eines Antrags auch über die Rechtsschutzmöglichkeiten gegen die Entscheidung sowie darüber zu belehren, bei welcher Stelle und innerhalb welcher Frist um Rechtsschutz nachgesucht werden kann.

## § 7 Rechtsschutz

(1) [1]Für Streitigkeiten nach diesem Gesetz ist der Verwaltungsrechtsweg gegeben.

(2) [1]Gegen die Entscheidung durch eine informationspflichtige Stelle im Sinne des § 2 Abs. 3 Nr. 1 ist ein Widerspruchsverfahren nach den §§ 68 bis 73 der Verwaltungsgerichtsordnung auch dann durchzuführen, wenn die Entscheidung von einer obersten Landesbehörde getroffen worden ist.

(3) [1]Ist die antragstellende Person der Auffassung, dass eine informationspflichtige Stelle im Sinne des § 2 Abs. 3 Nr. 3 den Antrag nicht vollständig erfüllt hat, kann sie diese Entscheidung nach Absatz 4 überprüfen lassen. [2]Die Überprüfung ist nicht Voraussetzung für die Erhebung der Klage nach Absatz 1.

(4) [1]Der Anspruch auf nochmalige Prüfung ist gegenüber der informationspflichtigen Stelle im Sinne des § 2 Abs. 3 Nr. 3 innerhalb eines Monats, nachdem diese Stelle mitgeteilt hat, dass der Anspruch nicht oder nicht vollständig erfüllt werden kann, schriftlich geltend zu machen. [2]Die informationspflichtige Stelle hat der antragstellenden Person das Ergebnis ihrer nochmaligen Prüfung innerhalb eines Monats zu übermitteln.

## § 8 Unterstützung des Zugangs zu Umweltinformationen

(1) [1]Die informationspflichtigen Stellen erleichtern den Zugang zu den bei ihnen verfügbaren Umweltinformationen insbesondere durch Benennung von Auskunftspersonen oder Informationsstellen, Veröffentlichung von Verzeichnissen über verfügbare Umweltinformationen, Einrichtung öffentlich zugänglicher Informationsnetze und Datenbanken sowie Veröffentlichung von Informationen über behördliche Zuständigkeiten. [2]Sie wirken darauf hin, dass die bei ihnen verfügbaren Umweltinformationen zunehmend in elektronischen Datenbanken oder sonstigen Formaten gespeichert werden, die über Mittel der elektronischen Kommunikation abrufbar sind.

(2) [1]Soweit möglich, gewährleisten die informationspflichtigen Stellen, dass die Umweltinformationen, die von ihnen oder für sie zusammengestellt werden, auf dem gegenwärtigen Stand, exakt und vergleichbar sind.

## § 9 Schutz öffentlicher Belange

(1) [1]Soweit die Bekanntgabe der Informationen nachteilige Auswirkungen hätte auf

1. die internationalen Beziehungen, die Verteidigung oder bedeutsame Schutzgüter der öffentlichen Sicherheit,
2. die Beziehungen zum Bund oder einem anderen Land,
3. die Vertraulichkeit der Beratungen von informationspflichtigen Stellen,
4. die Durchführung eines laufenden Gerichtsverfahrens, den Anspruch einer Person auf ein faires Verfahren oder die Durchführung strafrechtlicher, ordnungswidrigkeitenrechtlicher oder disziplinarrechtlicher Ermittlungen oder
5. den Zustand der Umwelt und ihrer Bestandteile im Sinne des § 2 Abs. 2 Nr. 1 oder Schutzgüter im Sinne des § 2 Abs. 2 Nr. 6,

ist der Antrag abzulehnen, es sei denn, das öffentliche Interesse an der Bekanntgabe überwiegt. [2]Der Zugang zu Umweltinformationen kann nicht unter Berufung auf die in der Nummer 2, der Zugang zu Informationen über Emissionen nicht unter Berufung auf die in den Nummern 3 und 5 genannten Gründe abgelehnt werden.

(2) [1]Soweit ein Antrag

1. offensichtlich missbräuchlich gestellt wurde,
2. sich auf interne Mitteilungen der informationspflichtigen Stelle, die zum Schutz des behördlichen Entscheidungsprozesses erforderlich sind, bezieht,

3. bei einer Stelle, die nicht über die gewünschten Informationen verfügt, gestellt wird, sofern er nicht nach § 4 Abs. 3 weitergeleitet werden kann,

4. sich auf die Zugänglichmachung noch nicht abgeschlossener Schriftstücke oder noch nicht aufbereiteter Daten bezieht oder

5. zu unbestimmt ist und auf Aufforderung der informationspflichtigen Stelle nach § 4 Abs. 2 nicht innerhalb einer angemessenen Frist präzisiert wird,

ist er abzulehnen, es sei denn, das öffentliche Interesse an der Bekanntgabe überwiegt.

## § 10 Schutz privater Belange

[1]Soweit durch die Bekanntgabe der Informationen

1. personenbezogene Daten offenbart würden, deren Vertraulichkeit durch Rechtsvorschrift vorgesehen ist,

2. Rechte am geistigen Eigentum, insbesondere Urheberrechte, verletzt würden,

3. Betriebs- oder Geschäftsgeheimnisse zugänglich gemacht würden oder die Informationen dem Steuer- oder Statistikgeheimnis unterliegen oder

4. die Interessen einer Person beeinträchtigt würden, die die beantragte Information, ohne rechtlich dazu verpflichtet zu sein oder rechtlich verpflichtet werden zu können, der informationspflichtigen Stelle freiwillig zur Verfügung gestellt hat,

ist der Antrag abzulehnen, es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse an der Bekanntgabe überwiegt. [2]Der Zugang zu Informationen über Emissionen kann nicht unter Berufung auf die in Satz 1 Nr. 1, 3 und 4 genannten Gründe abgelehnt werden. [3]Vor der Entscheidung über die Offenbarung der durch Satz 1 Nr. 1 bis 4 geschützten Informationen sind die Betroffenen anzuhören. [4]Die informationspflichtige Stelle hat in der Regel von einer Betroffenheit im Sinne des Satzes 1 Nr. 3 auszugehen, soweit übermittelte Informationen als Betriebs- und Geschäftsgeheimnisse gekennzeichnet sind. [5]Soweit die informationspflichtige Stelle dies verlangt, haben mögliche Betroffene im Einzelnen darzulegen, dass ein Betriebs- oder Geschäftsgeheimnis vorliegt.

## § 11 Unterrichtung der Öffentlichkeit

(1) [1]Die informationspflichtigen Stellen unterrichten die Öffentlichkeit in angemessenem Umfang aktiv und systematisch über den Zustand der Umwelt. [2]Zu diesem Zweck verbreiten sie Umweltinformationen, die für ihre Aufgaben von Bedeutung sind und über die sie verfügen, oder richten Verknüpfungen zu Internet-Seiten ein, auf denen die Informationen zu finden sind.

(2) [1]Zu den zu verbreitenden Umweltinformationen gehören:

1. Der Wortlaut von völkerrechtlichen Verträgen, Übereinkünften und Vereinbarungen, Rechtsvorschriften der Europäischen Gemeinschaften, des Bundes, der Länder, der Gemeinden, Kreise und Ämter über die Umwelt oder mit Bezug zur Umwelt,

2. politische Konzepte sowie Pläne und Programme mit Bezug zur Umwelt,

3. Berichte über den Stand der Umsetzung von Rechtsvorschriften sowie von Konzepten, Plänen und Programmen nach den Nummern 1 und 2, sofern solche Berichte von den informationspflichtigen Stellen in elektronischer Form ausgearbeitet worden sind oder bereitgehalten werden,

4. Daten oder Zusammenfassungen von Daten aus der Überwachung von Tätigkeiten, die sich auf die Umwelt auswirken oder wahrscheinlich auswirken,

5. Entscheidungen über die Zulässigkeit von Vorhaben, die erhebliche Auswirkungen auf die Umwelt haben,

6. Umweltvereinbarungen sowie

7. zusammenfassende Darstellungen und Bewertungen der Umweltauswirkungen nach §§ 11 und 12 des Gesetzes über die Umweltverträglichkeitsprüfung in der Fassung der Bekanntmachung vom 24. Februar 2010 (BGBl. I S. 94), geändert durch Artikel 11 des Gesetzes vom 11. August 2010 (BGBl. I S. 1163), und Risikobewertungen im Hinblick auf Umweltbestandteile nach § 2 Abs. 2 Nr. 1.

[2]In den Fällen der Nummern 5 bis 7 genügt zur Verbreitung die Angabe, wo solche Informationen zugänglich sind oder gefunden werden können. [3]Die veröffentlichten Umweltinformationen sind in angemessenen Abständen zu aktualisieren.

(3) [1]Die Verbreitung von Umweltinformationen soll in für die Öffentlichkeit verständlicher Darstellung und leicht zugänglichen Formaten erfolgen. [2]Hierzu sollen, soweit vorhanden, elektronische Kommunikationsmittel verwendet werden. [3]Satz 2 gilt nicht für Umweltinformationen, die vor Inkrafttreten dieses Gesetzes angefallen sind, es sei denn, sie liegen bereits in elektronischer Form vor.

(4) [1]Im Fall einer unmittelbaren Bedrohung der menschlichen Gesundheit oder der Umwelt haben die informationspflichtigen Stellen sämtliche Informationen, über die sie verfügen und die es der eventuell betroffenen Öffentlichkeit ermöglichen könnten, Maßnahmen zur Abwendung oder Begrenzung von Schäden infolge dieser Bedrohung zu ergreifen, unmittelbar und unverzüglich zu verbreiten. [2]Dies gilt unabhängig davon, ob die Bedrohung Folge menschlicher Tätigkeit ist oder eine natürliche Ursache hat. [3]Verfügen mehrere informationspflichtige Stellen über solche Informationen, stimmen sie sich bei deren Verbreitung ab.

(5) [1]Die §§ 9 bis 10 sowie § 8 Abs. 2 sind entsprechend anzuwenden.

## § 12 Kosten

(1) [1]Für die Bereitstellung von Informationen aufgrund dieses Gesetzes werden Kosten (Gebühren und Auslagen) erhoben. Gebühren werden nicht erhoben für

1. die Erteilung mündlicher und einfacher schriftlicher Auskünfte,
2. die Einsichtnahme vor Ort,
3. Maßnahmen und Vorkehrungen nach § 8,
4. die Unterrichtung der Öffentlichkeit nach § 11.

(2) [1]Die Gebühren sind auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen, dass das Recht auf Zugang zu Informationen nach § 3 wirksam in Anspruch genommen werden kann.

(3) [1]Das Innenministerium wird ermächtigt, im Einvernehmen mit dem für Umwelt zuständigen Ministerium für die Bereitstellung von Informationen durch informationspflichtige Stellen nach § 2 Abs. 3 Nr. 1 die Höhe der Kosten durch Verordnung zu bestimmen. [2]Die §§ 9, 10 und 15 Abs. 2 des Verwaltungskostengesetzes des Lande Schleswig-Holstein vom 17. Januar 1974 (GVOBl. Schl.-H. S. 37), zuletzt geändert durch Artikel 7 des Gesetzes vom 9. März 2010 (GVOBl. Schl.-H. S. 356), Ressortbezeichnung ersetzt durch Artikel 49 der Verordnung vom 8. September 2010 (GVOBl. Schl.-H. S. 575), finden keine Anwendung.

(4) [1]Informationspflichtige Stellen nach § 2 Abs. 3 Nr. 2 oder 3 können für die Bereitstellung von Informationen von der antragstellenden Person Kostenerstattung entsprechend den Grundsätzen nach den Absätzen 1 und 2 verlangen. [2]Die Höhe der erstattungsfähigen Kosten bemisst sich nach den in der Rechtsverordnung nach Abs. 3 festgelegten Kostensätzen für Amtshandlungen von informationspflichtigen Stellen nach § 2 Absatz 3 Nr. 1.

## § 13 Anrufung der oder des Landesbeauftragten für den Datenschutz

[1]Eine Person, die der Ansicht ist, dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass sie von einer informationspflichtigen Stelle eine unzulängliche Antwort erhalten hat, kann die oder den Landesbeauftragten für den Datenschutz anrufen. [2]Die Regelungen des Landesdatenschutzgesetzes über die Aufgaben und die Befugnisse der oder des Landesbeauftragten für den Datenschutz finden entsprechend Anwendung. [3]Die Vorschriften über den gerichtlichen Rechtsschutz bleiben unberührt.

## § 14 Übergangsvorschrift

[1]Anträge auf Zugang zu Informationen, die vor dem Inkrafttreten dieses Gesetzes gestellt worden sind, sind nach den Vorschriften dieses Gesetzes zu Ende zu führen.

# Geodatenzugangsgesetz (GeoZG)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Gesetz über den Zugang zu digitalen Geodaten (Geodatenzugangsgesetz) |
| **Amtliche Abkürzung:** | GeoZG |
| **Ausfertigung:** | 10.02.2009, BGBl. I S. 278 |
| **Inkrafttreten:** | 11.02.2009 |
| **Letzte Änderung:** | 07.11.2012, BGBl. I S. 2289 |

## Inhaltsübersicht


| | | |
|---|---|---|
| **Abschnitt 1: Ziel und Anwendungsbereich** | | **106** |
| § 1 | Ziel des Gesetzes | 106 |
| § 2 | Anwendungsbereich | 106 |
| **Abschnitt 2: Begriffsbestimmungen** | | **106** |
| § 3 | Allgemeine Begriffe | 106 |
| § 4 | Betroffene Geodaten und Geodatendienste | 107 |
| **Abschnitt 3: Anforderungen** | | **111** |
| § 5 | Bereitstellung von Geodaten | 111 |
| § 6 | Bereitstellung der Geodatendienste und Netzdienste | 112 |
| § 7 | Bereitstellung von Metadaten | 113 |
| § 8 | Interoperabilität | 113 |
| **Abschnitt 4: Elektronisches Netzwerk** | | **114** |
| § 9 | Geodateninfrastruktur und Geoportal | 114 |
| § 10 | Nationale Anlaufstelle | 114 |
| **Abschnitt 5: Nutzung von Geodaten** | | **114** |
| § 11 | Allgemeine Nutzung | 114 |
| § 12 | Schutz öffentlicher und sonstiger Belange | 115 |
| § 13 | (weggefallen) | 116 |
| **Abschnitt 6: Schlussbestimmungen** | | **116** |
| § 14 | Verordnungsermächtigung | 116 |
| § 15 | Inkrafttreten | 116 |

# Abschnitt 1:
# Ziel und Anwendungsbereich

## § 1 Ziel des Gesetzes

[1]Dieses Gesetz dient dem Aufbau einer nationalen Geodateninfrastruktur. Es schafft den rechtlichen Rahmen für

1. den Zugang zu Geodaten, Geodatendiensten und Metadaten von geodatenhaltenden Stellen sowie
2. die Nutzung dieser Daten und Dienste, insbesondere für Maßnahmen, die Auswirkungen auf die Umwelt haben können.

## § 2 Anwendungsbereich

(1) [1]Dieses Gesetz gilt für geodatenhaltende Stellen des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts.

(2) [1]Natürliche und juristische Personen des Privatrechts können Geodaten und Metadaten über das Geoportal nach § 9 Absatz 2 bereitstellen, wenn sie sich verpflichten, diese Daten nach den Bestimmungen dieses Gesetzes bereitzustellen und hierfür die technischen Voraussetzungen zu schaffen.

(3) [1]Dieses Gesetz gilt auch für Geodatendienste, die sich auf Daten beziehen, die in den Geodaten enthalten sind, auf die dieses Gesetz Anwendung findet.

(4) [1]Dieses Gesetz gilt nach Maßgabe des Seerechtsübereinkommens der Vereinten Nationen vom 10. Dezember 1982 (BGBl. 1994 II S. 1798; 1995 II S. 602) auch im Bereich der ausschließlichen Wirtschaftszone und des Festlandsockels.

# Abschnitt 2:
# Begriffsbestimmungen

## § 3 Allgemeine Begriffe

(1) [1]Geodaten sind alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet.

(2) [1]Metadaten sind Informationen, die Geodaten oder Geodatendienste beschreiben und es ermöglichen, Geodaten und Geodatendienste zu ermitteln, in Verzeichnisse aufzunehmen und zu nutzen.

(3) [1]Geodatendienste sind vernetzbare Anwendungen, welche Geodaten und Metadaten in strukturierter Form zugänglich machen. Dies sind im Einzelnen:

1. Suchdienste, die es ermöglichen, auf der Grundlage des Inhalts entsprechender Metadaten nach Geodaten und Geodatendiensten zu suchen und den Inhalt der Metadaten anzuzeigen,

2. Darstellungsdienste, die es zumindest ermöglichen, darstellbare Geodaten anzuzeigen, in ihnen zu navigieren, sie zu vergrößern oder zu verkleinern, zu verschieben, Daten zu überlagern sowie Informationen aus Legenden und sonstige relevante Inhalte von Metadaten anzuzeigen,

3. Dienste, die das Herunterladen und, wenn durchführbar, den direkten Zugriff auf Kopien von Geodaten ermöglichen (Downloaddienste),

4. Transformationsdienste zur geodätischen Umwandlung von Geodaten.

(4) [1]Interoperabilität ist die Kombinierbarkeit von Daten beziehungsweise die Kombinierbarkeit und Interaktionsfähigkeit verschiedener Systeme und Techniken unter Einhaltung gemeinsamer Standards.

(5) [1]Geodateninfrastruktur ist eine Infrastruktur bestehend aus Geodaten, Metadaten und Geodatendiensten, Netzdiensten und -technologien, Vereinbarungen über gemeinsame Nutzung, über Zugang und Verwendung sowie Koordinierungs- und Überwachungsmechanismen, -prozesse und -verfahren mit dem Ziel, Geodaten verschiedener Herkunft interoperabel verfügbar zu machen.

(6) [1]Geoportal ist eine elektronische Kommunikations-, Transaktions- und Interaktionsplattform, die über Geodatendienste und weitere Netzdienste den Zugang zu den Geodaten ermöglicht.

(7) [1]Netzdienste sind netzbasierte Anwendungen zur Kommunikation, Transaktion und Interaktion.

(8) [1]Geodatenhaltende Stellen im Sinne dieses Gesetzes sind die informationspflichtigen Stellen im Sinne von § 2 Absatz 1 des Umweltinformationsgesetzes vom 22. Dezember 2004 (BGBl. I S. 3704).

## § 4 Betroffene Geodaten und Geodatendienste

(1) [1]Dieses Gesetz gilt für Geodaten, die noch in Verwendung stehen und die folgenden Bedingungen erfüllen:

1. Sie beziehen sich auf das Hoheitsgebiet der Bundesrepublik Deutschland oder auf die ausschließliche Wirtschaftszone der Bundesrepublik Deutschland gemäß Seerechtsübereinkommen der Vereinten Nationen;

2. sie liegen in elektronischer Form vor;

3. sie sind vorhanden bei

   (a) einer geodatenhaltenden Stelle, fallen unter ihren öffentlichen Auftrag und

      aa) wurden von einer geodatenhaltenden Stelle erstellt oder

      bb) sind bei einer solchen eingegangen oder

      cc) werden von dieser geodatenhaltenden Stelle verwaltet oder aktualisiert,

   (b) Dritten, denen nach § 2 Absatz 2 Anschluss an die nationale Geodateninfrastruktur gewährt wird,

   oder werden für diese bereitgehalten;

4. sie betreffen eines oder mehrere der folgenden Themen:

   (a) Koordinatenreferenzsysteme (Systeme zur eindeutigen räumlichen Referenzierung von Geodaten anhand eines Koordinatensatzes (x, y, z) oder Angaben zu Breite, Länge und Höhe auf der Grundlage eines geodätischen horizontalen und vertikalen Datums),

   (b) geografische Gittersysteme (harmonisiertes Gittersystem mit Mehrfachauflösung, gemeinsamem Ursprungspunkt und standardisierter Lokalisierung und Größe der Gitterzellen),

   (c) geografische Bezeichnungen (Namen von Gebieten, Regionen, Orten, Großstädten, Vororten, Städten oder Siedlungen sowie jedes geografische oder topografische Merkmal von öffentlichem oder historischem Interesse),

   (d) Verwaltungseinheiten (lokale, regionale und nationale Verwaltungseinheiten, die die Gebiete abgrenzen, in denen die Bundesrepublik Deutschland Hoheitsbefugnisse hat oder ausübt und die durch Verwaltungsgrenzen voneinander getrennt sind),

   (e) Adressen (Lokalisierung von Grundstücken anhand von Adressdaten, in der Regel Straßenname, Hausnummer und Postleitzahl),

   (f) Flurstücke oder Grundstücke (Gebiete, die anhand des Grundbuchs oder gleichwertiger Verzeichnisse bestimmt werden),

   (g) Verkehrsnetze (Verkehrsnetze und zugehörige Infrastruktureinrichtungen für Straßen-, Schienen- und Luftverkehr sowie Schifffahrt; dies umfasst auch die Verbindungen zwischen den verschiedenen Netzen und das transeuropäische Verkehrsnetz im Sinne der Entscheidung Nr. 1692/96/EG des Europäischen Parlaments und des Rates vom 23. Juli 1996 über gemeinschaftliche Leitlinien für den Aufbau eines transeuropäischen Verkehrsnetzes (ABl. L 228 vom 9.9.1996, S. 1), zuletzt geändert durch die Verordnung (EG)
   Nr. 1791/2006 des Rates (ABl. L 363 vom 20.12.2006, S. 1), und künftige Überarbeitungen dieser Entscheidung),

   (h) Gewässernetz (Elemente des Gewässernetzes, einschließlich Meeresgebiete und aller sonstigen Wasserkörper und hiermit verbundener Teilsysteme, darunter Einzugsgebiete und Teileinzugsgebiete;

gegebenenfalls gemäß den Definitionen der Richtlinie 2000/60/EG des Europäischen Parlaments und des Rates vom 23. Oktober 2000 zur Schaffung eines Ordnungsrahmens für Maßnahmen der Gemeinschaft im Bereich der Wasserpolitik (ABl. L 327 vom 22.12.2000, S. 1), die zuletzt durch die Richtlinie 2009/31/EG(ABl. L 140 vom 5.6.2009, S. 114) geändert worden ist, und in Form von Netzen),

(i) Schutzgebiete (Gebiete, die im Rahmen des internationalen und des gemeinschaftlichen Rechts der Mitgliedstaaten ausgewiesen sind oder verwaltet werden, um spezifische Erhaltungsziele zu erreichen),

(j) Höhe (digitale Höhenmodelle für Land-, Eis- und Wasserflächen inklusive Tiefenmessung bei Gewässern und Mächtigkeit bei Eisflächen, sowie Uferlinien; (Geländemodelle)),

(k) Bodenbedeckung (physische und biologische Bedeckung der Erdoberfläche, einschließlich künstlicher Flächen, landwirtschaftlicher Flächen, Wälder, natürlicher (naturnaher) Gebiete, Feuchtgebiete und Wasserkörper),

(l) Orthofotografie (georeferenzierte Bilddaten der Erdoberfläche von satelliten- oder luftfahrzeuggestützten Sensoren),

(m) Geologie (geologische Beschreibung anhand von Zusammensetzung und Struktur des Untergrundes; dies umfasst auch Grundgebirgs- und Sedimentgesteine, Lockersedimente, Grundwasserleiter und -stauer, Störungen, Geomorphologie und anderes),

(n) statistische Einheiten (Einheiten für die Verbreitung oder Verwendung statistischer Daten),

(o) Gebäude (geografischer Standort von Gebäuden),

(p) Boden (Beschreibung von Boden und Unterboden anhand von Tiefe, Textur, Struktur und Gehalt an Teilchen sowie organischem Material, Steinigkeit, Erosion, gegebenenfalls durchschnittliches Gefälle und erwartete Wasserspeicherkapazität),

(q) Bodennutzung (Beschreibung von Gebieten anhand ihrer derzeitigen und geplanten künftigen Funktion oder ihres sozioökonomischen Zwecks wie zum Beispiel Wohn-, Industrie- oder Gewerbegebiete, land- oder forstwirtschaftliche Flächen, Freizeitgebiete),

(r) Gesundheit und Sicherheit (geografische Verteilung verstärkt auftretender pathologischer Befunde (zum Beispiel Allergien, Krebserkrankungen, Erkrankungen der Atemwege), Informationen über Auswirkungen auf die Gesundheit (zum Beispiel Biomarker, Rückgang der Fruchtbarkeit, Epidemien) oder auf das Wohlbefinden (zum Beispiel Ermüdung, Stress) der Menschen in unmittelbarem Zusammenhang mit der Umweltqualität (zum Beispiel Luftverschmutzung, Chemikalien, Abbau der Ozonschicht, Lärm) oder in mittelbarem Zusammenhang mit der Umweltqualität (zum Beispiel Nahrung, genetisch veränderte Organismen)),

(s) Versorgungswirtschaft und staatliche Dienste (Versorgungseinrichtungen wie Abwasser- und Abfallentsorgung, Energieversorgung und Wasserversorgung; staatliche Verwaltungs- und Sozialdienste wie öffentliche Verwaltung, Katastrophenschutz, Schulen und Krankenhäuser),

(t) Umweltüberwachung (Standort und Betrieb von Umweltüberwachungseinrichtungen einschließlich Beobachtung und Messung von Schadstoffen, des Zustands von Umweltmedien und anderen Parametern des Ökosystems wie zum Beispiel Artenvielfalt, ökologischer Zustand der Vegetation durch oder im Auftrag von öffentlichen Behörden),

(u) Produktions- und Industrieanlagen (Standorte für industrielle Produktion, einschließlich durch die Richtlinie 2010/75/EU des Europäischen Parlaments und des Rates vom 24. November 2010 über Industrieemissionen (integrierte Vermeidung und Verminderung der Umweltverschmutzung) (Neufassung)(ABl. L 334 vom 17.12.2010, S. 17) erfasste Anlagen und Einrichtungen zur Wasserentnahme sowie Bergbau- und Lagerstandorte),

(v) landwirtschaftliche Anlagen und Aquakulturanlagen (landwirtschaftliche Anlagen und Produktionsstätten einschließlich Bewässerungssysteme, Gewächshäuser und Ställe),

(w) Verteilung der Bevölkerung – Demografie (geografische Verteilung der Bevölkerung, einschließlich Bevölkerungsmerkmale und Tätigkeitsebenen, zusammengefasst nach Gitter, Region, Verwaltungseinheit oder sonstigen analytischen Einheiten),

(x) Bewirtschaftungsgebiete, Schutzgebiete, geregelte Gebiete und Berichterstattungseinheiten (auf internationaler, europäischer, nationaler, regionaler und lokaler Ebene bewirtschaftete, geregelte oder zu Zwecken der Berichterstattung herangezogene Gebiete, dazu zählen Deponien, Trinkwasserschutzgebiete, nitratempfindliche Gebiete, geregelte Fahrwasser auf Binnen- und Seewasserstraßen, Gebiete für die Abfallverklappung, Lärmschutzgebiete, für Exploration und Bergbau ausgewiesene Gebiete, Flussgebietseinheiten, entsprechende Berichterstattungseinheiten und Gebiete des Küstenzonenmanagements),

(y) Gebiete mit naturbedingten Risiken (gefährdete Gebiete, eingestuft nach naturbedingten Risiken (sämtliche atmosphärischen, hydrologischen, seismischen, vulkanischen Phänomene sowie Naturfeuer, die auf Grund ihres örtlichen Auftretens sowie ihrer Schwere und Häufigkeit signifikante Auswirkungen auf die Gesellschaft haben können), zum Beispiel Überschwemmungen, Erdrutsche und Bodensenkungen, Lawinen, Waldbrände, Erdbeben oder Vulkanausbrüche),

(z) atmosphärische Bedingungen (physikalische Bedingungen in der Atmosphäre, dazu zählen Geodaten auf der Grundlage von Messungen, Modellen oder einer Kombination aus beiden sowie Angabe der Messstandorte),

(z1) meteorologische Objekte (Witterungsbedingungen und deren Messung: Niederschlag, Temperatur, Gesamtverdunstung (Evapotranspiration), Windgeschwindigkeit und Windrichtung),

(z2) ozeanografische Objekte (physikalische Bedingungen der Ozeane wie zum Beispiel Strömungsverhältnisse, Salinität, Wellenhöhe),

(z3) Meeresregionen (physikalische Bedingungen von Meeren und salzhaltigen Gewässern, aufgeteilt nach Regionen und Teilregionen mit gemeinsamen Merkmalen),

(z4) biogeografische Regionen (Gebiete mit relativ homogenen ökologischen Bedingungen und gemeinsamen Merkmalen),

(z5) Lebensräume und Biotope (geografische Gebiete mit spezifischen ökologischen Bedingungen, Prozessen, Strukturen und (lebensunterstützenden) Funktionen als physische Grundlage für dort lebende Organismen; dies umfasst auch durch geografische, abiotische und biotische Merkmale gekennzeichnete natürliche oder naturnahe terrestrische und aquatische Gebiete),

(z6) Verteilung der Arten (geografische Verteilung des Auftretens von Tier- und Pflanzenarten, zusammengefasst in Gittern, Region, Verwaltungseinheit oder sonstigen analytischen Einheiten),

(z7) Energiequellen (Energiequellen wie zum Beispiel Kohlenwasserstofflagerstätten, Wasserkraft, Bioenergie, Sonnen- und Windenergie, gegebenenfalls mit Tiefen- beziehungsweise Höhenangaben zur Ausdehnung der Energiequelle),

(z8) mineralische Bodenschätze (mineralische Rohstofflagerstätten wie zum Beispiel Metallerze, Industrieminerale, gegebenenfalls mit Tiefen- beziehungsweise Höhenangaben zur Ausdehnung der Lagerstätten).

(2) [1]Einzelheiten zur Spezifikation der den Themen zugeordneten Geodaten werden durch Rechtsverordnung nach § 14 geregelt.

(3) [1]Sind neben einer Referenzversion mehrere identische Kopien der gleichen Geodaten bei verschiedenen geodatenhaltenden Stellen vorhanden oder werden sie für diese bereitgehalten, so gilt dieses Gesetz nur für die Referenzversion, von der die Kopien abgeleitet sind.

(4) [1]Verfügt die geodatenhaltende Stelle bezogen auf Geodaten und Geodatendienste nicht selbst über die Rechte an geistigem Eigentum, so bleiben diese Rechte von den Vorschriften dieses Gesetzes unberührt.

## Abschnitt 3: Anforderungen

### § 5 Bereitstellung von Geodaten

(1) [1]Die amtlichen Daten des Liegenschaftskatasters, der Geotopografie und des geodätischen Raumbezugs sind die fachneutralen Kernkomponenten der

nationalen Geodateninfrastruktur. [2]Sie werden für Zwecke dieses Gesetzes durch die hierfür zuständigen Stellen des Bundes und der Länder bereitgestellt.

(2) [1]Die Geodaten nach § 4 Absatz 1 Nummer 4 sind Bestandteil der Datengrundlage der nationalen Geodateninfrastruktur. [2]Sie werden durch die hierfür jeweils ursprünglich zuständigen Stellen bereitgestellt.

(3) [1]Die geodatenhaltenden Stellen haben ihre Geodaten auf der Grundlage der Daten nach Absatz 1 zu erfassen und zu führen.

(4) [1]Soweit Geodaten sich auf einen Standort oder ein geografisches Gebiet beziehen, dessen Lage sich auf das Hoheitsgebiet mehrerer Mitgliedstaaten der Europäischen Gemeinschaft erstreckt, stimmen die zuständigen geodatenhaltenden Stellen mit den jeweils zuständigen Stellen in dem Mitgliedstaat beziehungsweise in den Mitgliedstaaten die Darstellung und die Position des Standorts beziehungsweise des geografischen Gebiets ab.

## § 6 Bereitstellung der Geodatendienste und Netzdienste

(1) [1]Die geodatenhaltenden Stellen stellen sicher, dass für die von ihnen erhobenen, geführten oder bereitgestellten Geodaten und Metadaten mindestens die nachfolgenden Dienste bereitstehen:

1. Suchdienste,
2. Darstellungsdienste,
3. Downloaddienste,
4. Transformationsdienste,
5. Dienste zur Abwicklung eines elektronischen Geschäftsverkehrs.

(2) [1]Die Dienste nach Absatz 1 sollen Nutzeranforderungen berücksichtigen und müssen über elektronische Netzwerke öffentlich verfügbar sein.

(3) [1]Transformationsdienste sind mit den anderen Diensten nach Absatz 1 so zu kombinieren, dass die Geodatendienste und Netzdienste im Einklang mit diesem Gesetz betrieben werden können.

(4) [1]Für Suchdienste sind zumindest folgende Suchkriterien zu gewährleisten:

1. Schlüsselwörter,
2. Klassifizierung von Geodaten und Geodatendiensten,
3. geografischer Standort,
4. Qualitätsmerkmale,
5. Bedingungen für den Zugang zu und die Nutzung von Geodaten und Geodatendiensten,

6. für die Erfassung, Führung und Bereitstellung von Geodaten und Geodatendiensten zuständige geodatenhaltende Stelle.

(5) [1]Einzelheiten zur Spezifikation der Geodatendienste und Netzdienste werden durch Rechtsverordnung nach § 14 geregelt.

## § 7 Bereitstellung von Metadaten

(1) [1]Die geodatenhaltenden Stellen, welche Geodaten und Geodatendienste als Referenzversion im Sinne von § 4 Absatz 3 bereitstellen, haben die zugehörigen Metadaten zu erstellen, zu führen und bereitzustellen sowie in Übereinstimmung mit den Geodaten und Geodatendiensten zu halten.

(2) [1]Als Metadaten zu Geodaten sind mindestens nachstehende Inhalte oder Angaben zu folgenden Aspekten zu führen:

1. Schlüsselwörter,
2. Klassifizierung,
3. geografischer Standort,
4. Qualitätsmerkmale,
5. bestehende Beschränkungen des Zugangs der Öffentlichkeit nach § 12 sowie die Gründe für solche Beschränkungen,
6. Bedingungen für den Zugang und die Nutzung sowie gegebenenfalls entsprechende Geldleistungen,
7. für die Erfassung, Führung und Bereitstellung zuständige geodatenhaltende Stelle.

(3) [1]Als Metadaten zu Geodatendiensten und Netzdiensten sind mindestens Angaben zu folgenden Aspekten zu führen:

1. Qualitätsmerkmale,
2. Bedingungen für den Zugang und die Nutzung sowie gegebenenfalls hiermit verbundene Geldleistungen,
3. für die Erfassung, Führung und Bereitstellung zuständige geodatenhaltende Stelle.

(4) [1]Einzelheiten zur Spezifikation der Metadaten werden durch Rechtsverordnung nach § 14 geregelt.

## § 8 Interoperabilität

(1) [1]Geodaten und Geodatendienste sowie Metadaten sind interoperabel bereitzustellen.

(2) [1]Einzelheiten werden durch Rechtsverordnung nach § 14 geregelt.

## Abschnitt 4:
## Elektronisches Netzwerk

### § 9 Geodateninfrastruktur und Geoportal

(1) [1]Metadaten, Geodaten, Geodatendienste und Netzdienste werden als Bestandteile der nationalen Geodateninfrastruktur über ein elektronisches Netzwerk verknüpft.

(2) [1]Der Zugang zum elektronischen Netzwerk nach Absatz 1 erfolgt auf der Ebene des Bundes durch ein Geoportal.

### § 10 Nationale Anlaufstelle

(1) [1]Die Organisation der nationalen Geodateninfrastruktur erfolgt in der Verantwortung eines nationalen Lenkungsgremiums des Bundes und der Länder.

(2) [1]Das nationale Lenkungsgremium nimmt die Aufgaben der nationalen Anlaufstelle im Sinne des Artikels 19 Absatz 2 der Richtlinie 2007/2/EG wahr.

(3) [1]Die Einzelheiten regeln Bund und Länder in einer Verwaltungsvereinbarung.

## Abschnitt 5:
## Nutzung von Geodaten

### § 11 Allgemeine Nutzung

(1) [1]Geodaten und Geodatendienste, einschließlich zugehöriger Metadaten, sind vorbehaltlich der Vorschrift des § 12 Absatz 1 und 2 öffentlich zur Verfügung zu stellen.

(2) [1]Geodaten und Metadaten sind über Geodatendienste für die kommerzielle und nicht kommerzielle Nutzung geldleistungsfrei zur Verfügung zu stellen, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist oder vertragliche oder gesetzliche Rechte Dritter dem nicht entgegenstehen. [2]Geodatenhaltende

Stellen des Bundes stellen einander ihre Geodaten und Geodatendienste, einschließlich zugehöriger Metadaten, geldleistungsfrei zur Verfügung, soweit deren Nutzung zur Wahrnehmung öffentlicher Aufgaben erfolgt.

(3) [1]Die Einzelheiten zur Nutzung von Geodaten und Geodatendiensten, einschließlich zugehöriger Metadaten, werden in einer Rechtsverordnung nach § 14 geregelt.

## § 12 Schutz öffentlicher und sonstiger Belange

(1) [1]Der Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten über Suchdienste im Sinne des § 6 Absatz 1 Nummer 1 kann beschränkt werden, wenn er nachteilige Auswirkungen auf die internationalen Beziehungen, bedeutsame Schutzgüter der öffentlichen Sicherheit oder die Verteidigung haben kann.

(2) [1]Für den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten über die Dienste nach § 6 Absatz 1 Nummer 2 bis 5 gelten die Zugangsbeschränkungen nach § 8 Absatz 1 sowie § 9 des Umweltinformationsgesetzes vom 22. Dezember 2004 (BGBl. I S. 3704) entsprechend.

(3) [1]Gegenüber geodatenhaltenden Stellen mit Ausnahme derjenigen Stellen im Sinne von § 2 Absatz 1 Nummer 2 des Umweltinformationsgesetzes vom 22. Dezember 2004 sowie gegenüber entsprechenden Stellen der Länder, der Kommunen und anderer Mitgliedstaaten der Europäischen Gemeinschaft sowie gegenüber Organen und Einrichtungen der Europäischen Gemeinschaft sowie auf der Grundlage von Gegenseitigkeit und Gleichwertigkeit auch gegenüber Einrichtungen, die durch internationale Übereinkünfte geschaffen wurden, soweit die Europäische Gemeinschaft und ihre Mitgliedstaaten zu deren Vertragsparteien gehören, können der Zugang zu Geodaten und Geodatendiensten sowie der Austausch und die Nutzung von Geodaten beschränkt werden, wenn hierdurch

1. die Durchführung eines laufenden Gerichtsverfahrens,
2. der Anspruch einer Person auf ein faires Verfahren,
3. die Durchführung strafrechtlicher, ordnungswidrigkeitenrechtlicher oder disziplinarrechtlicher Ermittlungen,
4. bedeutsame Schutzgüter der öffentlichen Sicherheit,
5. die Verteidigung oder
6. die internationalen Beziehungen

gefährdet werden können.

## § 13 (weggefallen)

# Abschnitt 6:
# Schlussbestimmungen

## § 14 Verordnungsermächtigung

[1]Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf,

1. die Verpflichtungen aus den Durchführungsbestimmungen nach Artikel 5 Absatz 4, Artikel 7 Absatz 1, Artikel 16, 17 Absatz 8 sowie Artikel 21 Absatz 4 der Richtlinie 2007/2/EG zu erfüllen, soweit diese den Anwendungsbereich dieses Gesetzes betreffen, und

2. die Nutzungsbedingungen nach § 11 Absatz 3, insbesondere zu den Nutzungsrechten, zur Gewährleistung und zum Haftungsausschluss, festzulegen.

## § 15 Inkrafttreten

[1]Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

# Geodateninfrastrukturgesetz Schleswig-Holstein (GDIG)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Geodateninfrastrukturgesetz für das Land Schleswig-Holstein |
| **Amtliche Abkürzung:** | GDIG |
| **Ausfertigung:** | 15.12.2010, GVOBl. 2010 S. 717 |
| **Inkrafttreten:** | 16.12.2010 |
| **Letzte Änderung:** | 19.01.2012, GVOBl. 2012 S. 279 |

## Inhaltsübersicht


| | | |
|---|---|---|
| **Abschnitt I: Allgemeine Vorschriften** | | **118** |
| § 1 | Ziel des Gesetzes | 118 |
| § 2 | Anwendungsbereich | 118 |
| § 3 | Allgemeine Begriffe | 118 |
| § 4 | Betroffene Geodaten und Geodatendienste | 120 |
| **Abschnitt II: Anforderungen an die Geodateninfrastruktur** | | **122** |
| § 5 | Geodaten | 122 |
| § 6 | Geodatendienste und Netzdienste | 122 |
| § 7 | Metadaten | 123 |
| § 8 | Interoperabilität und Geoportal | 123 |
| § 9 | Lenkungsgremium und Koordinierungsstelle Geodateninfrastruktur | 124 |
| § 10 | Allgemeine Nutzung | 124 |
| § 11 | Schutz öffentlicher und sonstiger Belange | 125 |
| § 12 | Kosten und Lizenzen | 125 |
| **Abschnitt III: Schlussbestimmungen** | | **127** |
| § 13 | Verordnungsermächtigung | 127 |
| § 14 | Inkrafttreten | 127 |

# Abschnitt I:
# Allgemeine Vorschriften

## § 1 Ziel des Gesetzes

[1]Dieses Gesetz schafft den rechtlichen Rahmen für den Ausbau und den Betrieb der Geodateninfrastruktur Schleswig-Holstein als Bestandteil der nationalen Geodateninfrastruktur. [2]Es dient der Umsetzung der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft - INSPIRE - (ABl. EU Nr. L 108 S. 1).

## § 2 Anwendungsbereich

(1) [1]Dieses Gesetz gilt für geodatenhaltende Stellen.

(2) [1]Geodatenhaltende Stellen nach Absatz 1 sind die Stellen gemäß § 2 Abs. 3 des Informationszugangsgesetzes für das Land Schleswig-Holstein (IZG-SH) vom 19. Januar 2012 (GVOBl. Schl.-H. S. 89).

(3) [1]Dieses Gesetz gilt auch für natürliche und juristische Personen des privaten Rechts, denen nach § 8 Abs. 3 Anschluss an die Geodateninfrastruktur gewährt wird, soweit diese über die Geodateninfrastruktur Geodaten und Geodatendienste sowie Metadaten bereitstellen.

(4) [1]Dieses Gesetz gilt nicht für

1. den Landtag im Rahmen seiner Gesetzgebungstätigkeit;
2. die obersten Landesbehörden, soweit sie im Rahmen der Gesetzgebungsverfahren oder beim Erlass von Rechtsverordnungen tätig werden;
3. die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden, soweit sie als Organe der Rechtspflege tätig werden.

(5) [1]Dieses Gesetz gilt nach Maßgabe des Seerechtsübereinkommens der Vereinten Nationen vom 10. Dezember 1982 (BGBl. 1994 II S. 1798, 1799, 1995 II S. 602) auch im Bereich der ausschließlichen Wirtschaftszone und des Festlandsockels.

## § 3 Allgemeine Begriffe

(1) [1]Geodaten sind Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet.

(2) [1]Metadaten sind Informationen, die Geodaten, Geodatendienste oder Netzdienste beschreiben und es ermöglichen, diese zu ermitteln, in Verzeichnisse aufzunehmen und zu nutzen.

(3) [1]Geodatendienste sind vernetzbare Anwendungen, die Geodaten und Metadaten in strukturierter Form zugänglich machen. Dies sind im Einzelnen:

1. Suchdienste, die es ermöglichen, auf der Grundlage des Inhalts entsprechender Metadaten nach Geodaten und Geodatendiensten zu suchen und den Inhalt der Metadaten anzuzeigen,

2. Darstellungsdienste, die es ermöglichen, darstellbare Geodaten anzuzeigen, in ihnen zu navigieren, sie zu vergrößern oder sie zu verkleinern, zu verschieben, Daten zu überlagern sowie Informationen aus Legenden und sonstige relevante Inhalte von Metadaten anzuzeigen,

3. Downloaddienste, die das Herunterladen und, wenn durchführbar, den direkten Zugriff auf Kopien von Geodaten ermöglichen,

4. Transformationsdienste zur Umwandlung von Geodaten,

5. Dienste zum Abrufen von Geodatendiensten, die es erlauben, Anforderungen an Geodaten zu definieren und verschiedene Geodatendienste zu kombinieren.

(4) [1]Interoperabilität ist die Fähigkeit zur Kombination und Interaktion verschiedener Systeme, Techniken oder Daten unter Einhaltung gemeinsamer Standards.

(5) [1]Geodateninfrastruktur ist eine Infrastruktur bestehend aus Geodaten, Metadaten und Geodatendiensten, Netzdiensten und -technologien, Vereinbarungen über gemeinsame Nutzung, Zugang und Verwendung sowie Koordinierungs- und Überwachungsmechanismen, Überwachungsprozesse und -verfahren, in Verbindung mit der Aufgabe, Geodaten verschiedener Herkunft interoperabel verfügbar zu machen.

(6) [1]Netzdienste sind netzbasierte Anwendungen zur Kommunikation, Transaktion und Interaktion.

(7) [1]Geoportal ist eine Kommunikations-, Transaktions- und Interaktionsplattform, die über Geodatendienste und weitere Netzdienste den Zugang zu den Geodaten ermöglicht.

(8) [1]Zugang ist die Weitergabe von gespeicherten oder durch Datenverarbeitung gewonnenen Geodaten und das Einräumen der Möglichkeit, diese Daten einzusehen oder abzurufen.

(9) [1]Verarbeitung ist neben den in § 2 Abs. 2 des Landesdatenschutzgesetzes (LDSG) vom 9. Februar 2000 (GVOBl. Schl.-H. S. 169), zuletzt geändert durch Artikel 12 des Gesetzes vom 26. März 2009 (GVOBl. Schl.-H. S. 93), genannten Tätigkeiten auch das Verschneiden von Geodaten und Geodatendiensten.

## § 4 Betroffene Geodaten und Geodatendienste

(1) [1]Dieses Gesetz gilt für Geodaten, die die folgenden Voraussetzungen erfüllen:

1. Sie beziehen sich auf das Hoheitsgebiet des Landes Schleswig-Holstein,
2. sie liegen in elektronischer Form vor,
3. sie sind vorhanden bei
   (a) einer geodatenhaltenden Stelle, fallen unter ihren öffentlichen Auftrag und
      aa) wurden von einer geodatenhaltenden Stelle erstellt,
      bb) sind bei einer solchen eingegangen oder
      cc) werden von dieser geodatenhaltenden Stelle verwaltet oder aktualisiert, oder
   (b) Stellen, denen gemäß § 8 Abs. 3 Anschluss an die Geodateninfrastruktur gewährt wird,

   oder werden für diese bereitgehalten und
4. sie betreffen eines oder mehrere der folgenden Themen:
   (a) Themen nach Anhang I der Richtlinie 2007/2/EG
      aa) Koordinatenreferenzsysteme,
      bb) Geografische Gittersysteme,
      cc) Geografische Bezeichnungen,
      dd) Verwaltungseinheiten,
      ee) Adressen,
      ff) Flurstücke oder Grundstücke,
      gg) Verkehrsnetze,
      hh) Gewässernetz,
      ii) Schutzgebiete,
   (b) Themen nach Anhang II der Richtlinie 2007/2/EG
      aa) Höhe, digitale Höhen- und Geländemodelle,
      bb) Bodenbedeckung,
      cc) Orthofotografie,
      dd) Geologie,
   (c) Themen nach Anhang III der Richtlinie 2007/2/EG
      aa) Statistische Einheiten,
      bb) Gebäude,
      cc) Boden,
      dd) Bodennutzung,
      ee) Gesundheit und Sicherheit,

ff) Versorgungswirtschaft und staatliche Dienste,
gg) Umweltüberwachung,
hh) Produktions- und Industrieanlagen,
ii) Landwirtschaftliche Anlagen und Aquakulturanlagen,
jj) Verteilung der Bevölkerung - Demografie,
kk) Bewirtschaftungsgebiete/Schutzgebiete/geregelte Gebiete und Berichterstattungseinheiten,
ll) Gebiete mit naturbedingten Risiken,
mm) Atmosphärische Bedingungen,
nn) Meteorologisch-geografische Objekte,
oo) Ozeanografisch-geografische Objekte,
pp) Meeresregionen,
qq) Biogeografische Regionen,
rr) Lebensräume und Biotope,
ss) Verteilung der Arten,
tt) Energiequellen,
uu) Mineralische Bodenschätze.

(2) [1]Sind identische Kopien derselben Geodaten bei verschiedenen geodatenhaltenden Stellen vorhanden oder werden sie für diese bereitgehalten, so gilt dieses Gesetz nur für die Referenzversion, von der die Kopien abgeleitet sind. [2]Die Bestimmungen zum Schutz öffentlicher und sonstiger Belange nach § 11 bleiben unberührt.

(3) [1]Dieses Gesetz gilt auch für Geodatendienste, die sich auf die Daten beziehen, die in den in Absatz 1 genannten Geodaten enthalten sind.

(4) [1]Verfügen die geodatenhaltenden Stellen nicht selbst über die Urheberrechte oder verwandte Schutzrechte an den Geodaten nach Absatz 1,so bleiben diese Rechte von den Vorschriften dieses Gesetzes unberührt.

(5) [1]Geodaten nach Absatz 1, die bei den der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts oder bei Stellen im Sinne des § 2 Abs. 3 Nr. 3 IZG-SH vorhanden sind oder für diese bereitgehalten werden, unterliegen diesem Gesetz nur, wenn ihre Sammlung oder Verbreitung durch Rechtsvorschrift vorgeschrieben ist.

(6) [1]Die in den Grundbüchern enthaltenen Daten werden von den Regelungen dieses Gesetzes nicht erfasst.

## Abschnitt II:
## Anforderungen an die Geodateninfrastruktur

### § 5 Geodaten

(1) [1]Die amtlichen Geodaten des Liegenschaftskatasters und der Landesvermessung sind die fachneutralen Kernkomponenten der Geodateninfrastruktur Schleswig-Holstein.

(2) [1]Die Geodaten sind auf der Basis der amtlichen Geodaten des Liegenschaftskatasters und der Landesvermessung bzw. der amtlichen Geodaten der Geotopographie des Bundes zu erfassen und zu führen.

(3) [1]Soweit Geodaten sich auf einen Standort oder ein geografisches Gebiet beziehen, dessen Lage sich auf das Hoheitsgebiet eines weiteren Landes oder mehrerer Länder oder auf andere Mitgliedstaaten der Europäischen Gemeinschaft erstreckt, stimmen die zuständigen geodatenhaltenden Stellen mit den jeweils zuständigen Stellen dieser Länder, des Bundes oder der anderen Mitgliedstaaten der Europäischen Gemeinschaft die Darstellung und die Position des Standorts oder des geografischen Gebiets ab.

### § 6 Geodatendienste und Netzdienste

(1) [1]Die geodatenhaltenden Stellen gewährleisten, dass für die bei ihnen vorgehaltenen aktuellen Geodaten und Metadaten Geodatendienste bereitstehen. Soweit für Geodatendienste Geldleistungen gefordert werden, sollen Netzdienste zur Abwicklung eines elektronischen Geschäftsverkehrs und zur Sicherstellung des Betriebs von Geodatendiensten zur Verfügung gestellt werden.

(2) [1]Geodatendienste und Netzdienste sollen Nutzeranforderungen berücksichtigen und müssen über computergestützte Netzwerke öffentlich verfügbar sein.

(3) [1]Für Suchdienste ist zumindest folgende Kombination von Suchkriterien zu gewährleisten:

1. Schlüsselwörter,
2. Klassifizierung von Geodaten und Geodatendiensten,
3. Qualitätsmerkmale,
4. geografischer Standort,
5. Bedingungen für den Zugang zu und die Nutzung von Geodaten und Geodatendiensten,

6. die für die Erfassung, Führung und Bereitstellung der Geodaten zuständigen geodatenhaltenden Stellen.

## § 7 Metadaten

(1) [1]Die geodatenhaltenden Stellen, die Geodaten und Geodatendienste bereitstellen, haben die zugehörigen Metadaten zu erstellen, zu führen und bereitzustellen, sowie in Übereinstimmung mit den Geodaten und Geodatendiensten zu halten.

(2) [1]Als Metadaten zu Geodaten sind mindestens nachstehende Inhalte oder Angaben zu folgenden Aspekten zu führen:

1. Schlüsselwörter,
2. Klassifizierung,
3. geografischer Standort,
4. Qualitätsmerkmale,
5. für die Erfassung, Führung und Bereitstellung zuständige geodatenhaltende Stelle,
6. Bedingungen für den Zugang einschließlich bestehender Beschränkungen und deren Gründe, Bedingungen für die Nutzung sowie gegebenenfalls anfallende Geldleistungen.

(3) [1]Als Metadaten zu Geodatendiensten und Netzdiensten sind mindestens Angaben zu folgenden Aspekten zu führen:

1. Bedingungen für den Zugang und die Nutzung einschließlich bestehender Beschränkungen und deren Gründe sowie gegebenenfalls anfallende Geldleistungen,
2. Qualitätsmerkmale,
3. für die Erfassung, Führung und Bereitstellung zuständige geodatenhaltende Stelle.

## § 8 Interoperabilität und Geoportal

(1) [1]Geodaten, Metadaten, Netzdienste und Geodatendienste sind als Bestandteile der Geodateninfrastruktur interoperabel bereitzustellen.

(2) [1]Der Zugang zu Geodaten, Metadaten, Netzdiensten und Geodatendiensten erfolgt für das Land durch ein Geoportal. [2]Diese Nutzung des Geoportals ist kostenfrei. [3]Dieses Geoportal kann auch von den übrigen geodatenhaltenden

Stellen als Zugang zu ihren Geodaten, Metadaten, Netzdiensten und Geodatendiensten kostenfrei genutzt werden.

(3) [1]Das Geoportal nach Absatz 2 Satz 1 kann auch von den Stellen nach § 2 Abs. 3 als Zugang zu ihren Geodaten, Geodatendienste und Metadaten, und damit als Anschluss an die Geodateninfrastruktur, genutzt werden, sofern diese Stellen sich verpflichten, die Daten gemäß den Bestimmungen dieses Gesetzes bereitzustellen, hierfür die technischen Voraussetzungen zu schaffen und die Metadaten in Übereinstimmung mit den Geodaten und Geodatendiensten zu halten.

(4) [1]Die Bereitstellung von Geodaten und Geodatendiensten nach § 4 über ein Geoportal hat vorbehaltlich der §§ 10 und 11 unter Beachtung der im Landes- und im Bundesdatenschutzgesetz festgelegten Grundsätze des Schutzes personenbezogener Daten zu erfolgen. [2]Die Daten unterliegen den Regelungen des Gesetzes über Urheberrecht und verwandte Schutzrechte.

## § 9 Lenkungsgremium und Koordinierungsstelle Geodateninfrastruktur

(1) [1]Für Organisation, Ausbau und Betrieb der Geodateninfrastruktur Schleswig-Holstein wird ein Lenkungsgremium Geodateninfrastruktur Schleswig-Holstein (LG GDI-SH) des Landes und der Kommunen eingerichtet.

(2) [1]Das LG GDI-SH unterstützt das nationale Lenkungsgremium, das nach § 10 des Gesetzes über den Zugang zu digitalen Geodaten (Geodatenzugangsgesetz) vom 10. Februar 2009 (BGBl. I S. 278) die Aufgaben der nationalen Anlaufstelle im Sinne des Artikels 19 Abs. 2 der Richtlinie 2007/2/EG wahrnimmt.

(3) [1]Zur Koordinierung der Ausführung der Beschlüsse des LG GDI-SH und für operative Aufgaben beim Ausbau und Betrieb der Geodateninfrastruktur Schleswig-Holstein wird im Geschäftsbereich der für die Landesvermessung und das Liegenschaftskataster zuständigen obersten Landesbehörde eine Koordinierungsstelle Geodateninfrastruktur eingerichtet.

(4) [1]Die geodatenhaltenden Stellen sind verpflichtet, der Koordinierungsstelle Geodateninfrastruktur auf Anforderung alle Informationen zur Verfügung zu stellen, die sie zur Erfüllung ihrer Aufgaben benötigt.

## § 10 Allgemeine Nutzung

[1]Zu Geodaten und Geodatendiensten ist vorbehaltlich des § 11 sowie nach Maßgabe des § 12 ein Zugang für die Öffentlichkeit und andere geodatenhaltende Stellen bereitzustellen. [2]Werden Geodaten über Darstellungsdienste bereitgestellt, kann dies in einer Form geschehen, die eine Weiterverwendung, insbesondere zu kommerziellen Zwecken, ausschließt.

## § 11 Schutz öffentlicher und sonstiger Belange

(1) [1]Der Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten über einen Suchdienst nach § 3 Abs. 3 Nr. 1 kann beschränkt werden, wenn dieser Zugang nachteilige Auswirkungen auf die internationalen Beziehungen, bedeutsame Schutzgüter der öffentlichen Sicherheit oder die Verteidigung haben kann, es sei denn, das öffentliche Interesse am Zugang überwiegt.

(2) [1]Für den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten nach § 3 Abs. 3 Nr. 2 bis 5 gelten die Zugangsbeschränkungen nach § 9 sowie § 10 IZG-SH entsprechend.

(3) [1]Die für eine Offenbarung von personenbezogenen Daten notwendige einzelfallbezogene Abwägung des öffentlichen Interesses gemäß § 10 Satz 1 IZG-SH an der Bekanntgabe von Geodaten gegen den Schutz privater Belange kann durch eine daten- und nutzungsspezifische Kategorisierung von Geodaten ersetzt werden, wenn schutzwürdige private Belange nur geringfügig beeinträchtigt werden. [2]Die Kategorisierung ist von der jeweiligen geodatenhaltenden Stelle im Einvernehmen mit dem Unabhängigen Landeszentrum für Datenschutz durchzuführen und von der Koordinierungsstelle nach § 9 öffentlich verfügbar bereitzustellen.

(4) [1]Gegenüber geodatenhaltenden Stellen mit Ausnahme derjenigen Stellen im Sinne des § 2 Abs. 3 Nr. 3 IZG-SH sowie gegenüber entsprechenden Stellen der Länder und deren Kommunen, des Bundes und anderer Mitgliedstaaten der Europäischen Gemeinschaft sowie gegenüber Organen und Einrichtungen der Europäischen Gemeinschaft sowie auf der Grundlage von Gegenseitigkeit und Gleichwertigkeit auch gegenüber Einrichtungen, die durch internationale Übereinkünfte geschaffen wurden, soweit die Europäische Gemeinschaft und ihre Mitgliedstaaten zu deren Vertragsparteien gehören, können der Zugang zu Geodaten und Geodatendiensten sowie der Austausch und die Nutzung von Geodaten beschränkt werden, wenn hierdurch

1. die Durchführung eines laufenden Gerichtsverfahrens,
2. der Anspruch einer Person auf ein faires Verfahren,
3. die Durchführung strafrechtlicher, ordnungswidrigkeitenrechtlicher oder disziplinarrechtlicher Ermittlungen,
4. bedeutsame Schutzgüter der öffentlichen Sicherheit,
5. die Verteidigung oder
6. die internationalen Beziehungen

gefährdet werden.

## § 12 Kosten und Lizenzen

(1) [1]Die fachneutralen Kernkomponenten der Geodateninfrastruktur Schleswig-Holstein nach § 5 Abs. 1 werden den geodatenhaltenden Stellen für Zwecke

dieses Gesetzes kostenfrei zur Verfügung gestellt. [2]Die Kostenfreiheit erstreckt sich nicht auf eine kommerzielle Weiterverwendung.

(2) [1]Geodatenhaltende Stellen, die Geodaten nach § 4 Abs. 1 Nr. 4 und Geodatendienste nach § 3 Abs. 3 anbieten, können für deren Nutzung Haftungsausschlüsse, elektronische Lizenzvereinbarungen oder, wenn notwendig, Lizenzen in sonstiger Form festsetzen.

(3) [1]Geodatenhaltende Stellen, die Geodaten nach § 4 Abs. 1 Nr. 4 und Dienste nach § 3 Abs. 3 Nr. 3 bis 5 anbieten, können für deren Nutzung Geldleistungen fordern.

(4) [1]Suchdienste nach § 3 Abs. 3 Nr. 1 stehen der Öffentlichkeit kostenfrei zur Verfügung.

(5) [1]Darstellungsdienste nach § 3 Abs. 3 Nr. 2 stehen der Öffentlichkeit kostenfrei zur Verfügung, soweit sie nicht über eine netzgebundene Bildschirmdarstellung hinausgehen. [2]Die geodatenhaltende Stelle kann unterbinden, dass Geodaten, die über Darstellungsdienste bereitgestellt werden, ausgedruckt oder für einen wirtschaftlichen Zweck weiterverwendet werden. [3]Abweichend von Satz 1 können für die Nutzung von Darstellungsdiensten Geldleistungen gefordert werden, wenn die Geldleistung die Pflege der Geodaten und der entsprechenden Geodatendienste sichert, insbesondere in Fällen, in denen große Datenmengen häufig aktualisiert werden.

(6) [1]Soweit von geodatenhaltenden Stellen oder von Organen und Einrichtungen der Europäischen Gemeinschaft gemäß Absätze 2 und 3 Geldleistungen gefordert oder diesen Lizenzen erteilt werden, müssen sie mit dem allgemeinen Ziel des Austauschs von Geodaten und Geodatendiensten zwischen diesen Stellen vereinbar sein. [2]Die von geodatenhaltenden Stellen oder Organen oder Einrichtungen der Europäischen Gemeinschaft geforderten Geldleistungen übersteigen nicht das zur Gewährleistung der nötigen Qualität und des Angebots von Geodaten und Geodatendiensten notwendige Minimum zuzüglich einer angemessenen Rendite, wobei die Selbstfinanzierungserfordernisse der geodatenhaltenden Stellen, die Geodaten und Geodatendienste anbieten, zu beachten sind. Werden Geodaten oder Geodatendienste Organen oder Einrichtungen der Europäischen Gemeinschaft zur Erfüllung von aus dem Gemeinschaftsumweltrecht erwachsenden Berichtspflichten zur Verfügung gestellt, werden keine Geldleistungen gefordert.

(7) [1]Soweit Stellen anderer Mitgliedstaaten der Europäischen Gemeinschaft öffentliche Aufgaben wahrnehmen, die Auswirkungen auf die Umwelt haben können, finden die Regelungen des Absatzes 6 auch auf diese Anwendung. [2]Satz 1 gilt auf der Grundlage von Gegenseitigkeit und Gleichwertigkeit auch für durch internationale Übereinkünfte geschaffene Einrichtungen, soweit die Europäische Gemeinschaft und ihre Mitgliedstaaten zu deren Vertragsparteien gehören.

(8) [1]Bedingungen für den Zugang und die Nutzung durch Organe und Einrichtungen der Europäischen Gemeinschaft sind einheitlich zu gestalten.

# Abschnitt III: Schlussbestimmungen

## § 13 Verordnungsermächtigung

[1]Die Landesregierung wird ermächtigt, durch Verordnung

1. die zur Erfüllung der Verpflichtungen aus den Durchführungsbestimmungen nach Artikel 5 Abs. 4, Artikel 7 Abs. 1, Artikel 16, Artikel 17 Abs. 8 und Artikel 21 Abs. 4 der Richtlinie 2007/2/EG erforderlichen Regelungen zu erlassen und

2. Einzelheiten zur Nutzung des Geoportals nach § 8 Abs. 2 und 3 sowie zur Spezifikation

   (a) der Geodaten nach § 4,

   (b) der Suchdienste nach § 6,

   (c) der Metadaten nach § 7,

   (d) der Organisation und der Aufgaben des Lenkungsgremiums und der Koordinierungsstelle Geodateninfrastruktur nach § 9 und

   (e) der Bedingungen für den Zugang und die Nutzung durch Organe und Einrichtungen der Europäischen Gemeinschaft nach § 12 Abs. 8

   zu regeln.

## § 14 Inkrafttreten

[1]Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

# Telemediengesetz (TMG)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Telemediengesetz |
| **Amtliche Abkürzung:** | TMG |
| **Ausfertigung:** | 26.02.2007, BGBl. I S. 179 |
| **Inkrafttreten:** | 01.03.2007 |
| **Letzte Änderung:** | 21.07.2016, BGBl. I S. 1766 |

## Inhaltsübersicht


**Abschnitt 1: Allgemeine Bestimmungen** **130**
§ 1 Anwendungsbereich 130
§ 2 Begriffsbestimmungen 130
§ 2a Europäisches Sitzland 132
§ 3 Herkunftslandprinzip 133
**Abschnitt 2: Zulassungsfreiheit und Informationspflichten** **135**
§ 4 Zulassungsfreiheit 135
§ 5 Allgemeine Informationspflichten 135
§ 6 Besondere Informationspflichten bei kommerziellen Kommunikationen 136
**Abschnitt 3: Verantwortlichkeit** **137**
§ 7 Allgemeine Grundsätze 137
§ 8 Durchleitung von Informationen 137
§ 9 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen 138
§ 10 Speicherung von Informationen 138
**Abschnitt 4: Datenschutz** **139**
§ 11 Anbieter-Nutzer-Verhältnis 139
§ 12 Grundsätze 139
§ 13 Pflichten des Diensteanbieters 140
§ 14 Bestandsdaten 141
§ 15 Nutzungsdaten 142
§ 15a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten 143
**Abschnitt 5: Bußgeldvorschriften** **143**
§ 16 Bußgeldvorschriften 143

# Abschnitt 1:
# Allgemeine Bestimmungen

## § 1 Anwendungsbereich

(1) [1]Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien). [2]Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

(2) [1]Dieses Gesetz gilt nicht für den Bereich der Besteuerung.

(3) [1]Das Telekommunikationsgesetz und die Pressegesetze bleiben unberührt.

(4) [1]Die an die Inhalte von Telemedien zu richtenden besonderen Anforderungen ergeben sich aus dem Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag).

(5) [1]Dieses Gesetz trifft weder Regelungen im Bereich des internationalen Privatrechts noch regelt es die Zuständigkeit der Gerichte.

(6) [1]Die besonderen Bestimmungen dieses Gesetzes für audiovisuelle Mediendienste auf Abruf gelten nicht für Dienste, die

1. ausschließlich zum Empfang in Drittländern bestimmt sind und
2. nicht unmittelbar oder mittelbar von der Allgemeinheit mit handelsüblichen Verbraucherendgeräten in einem Staat innerhalb des Geltungsbereichs der Richtlinie 89/552/EWG des Rates vom 3. Oktober 1989 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit (ABl. L 298 vom 17.10.1989, S. 23), die zuletzt durch die Richtlinie 2007/65/EG (ABl. L 332 vom 18.12.2007, S. 27) geändert worden ist, empfangen werden.

## § 2 Begriffsbestimmungen

[1]Im Sinne dieses Gesetzes

1. ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert,

2. ist niedergelassener Diensteanbieter jeder Anbieter, der mittels einer festen Einrichtung auf unbestimmte Zeit Telemedien geschäftsmäßig anbietet oder erbringt; der Standort der technischen Einrichtung allein begründet keine Niederlassung des Anbieters,

2a. ist drahtloses lokales Netzwerk ein Drahtloszugangssystem mit geringer Leistung und geringer Reichweite sowie mit geringem Störungsrisiko für weitere, von anderen Nutzern in unmittelbarer Nähe installierte Systeme dieser Art, welches nicht exklusive Grundfrequenzen nutzt,

3. ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen,

4. sind Verteildienste Telemedien, die im Wege einer Übertragung von Daten ohne individuelle Anforderung gleichzeitig für eine unbegrenzte Anzahl von Nutzern erbracht werden,

5. ist kommerzielle Kommunikation jede Form der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren, Dienstleistungen oder des Erscheinungsbilds eines Unternehmens, einer sonstigen Organisation oder einer natürlichen Person dient, die eine Tätigkeit im Handel, Gewerbe oder Handwerk oder einen freien Beruf ausübt; die Übermittlung der folgenden Angaben stellt als solche keine Form der kommerziellen Kommunikation dar:

   a) Angaben, die unmittelbaren Zugang zur Tätigkeit des Unternehmens oder der Organisation oder Person ermöglichen, wie insbesondere ein Domain-Name oder eine Adresse der elektronischen Post,

   b) Angaben in Bezug auf Waren und Dienstleistungen oder das Erscheinungsbild eines Unternehmens, einer Organisation oder Person, die unabhängig und insbesondere ohne finanzielle Gegenleistung gemacht werden.

6. sind „audiovisuelle Mediendienste auf Abruf“ Telemedien mit Inhalten, die nach Form und Inhalt fernsehähnlich sind und die von einem Diensteanbieter zum individuellen Abruf zu einem vom Nutzer gewählten Zeitpunkt und aus einem vom Diensteanbieter festgelegten Inhaltekatalog bereitgestellt werden.

[2]Einer juristischen Person steht eine Personengesellschaft gleich, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben und Verbindlichkeiten einzugehen.

## § 2a Europäisches Sitzland [2]

(1) [1]Innerhalb des Geltungsbereichs der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") (ABl. L 178 vom 17.7.2000, S. 1) bestimmt sich das Sitzland des Diensteanbieters danach, wo dieser seine Geschäftstätigkeit tatsächlich ausübt. [2]Dies ist der Ort, an dem sich der Mittelpunkt der Tätigkeiten des Diensteanbieters im Hinblick auf ein bestimmtes Telemedienangebot befindet.

(2) [1]Abweichend von Absatz 1 gilt innerhalb des Geltungsbereichs der Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) (ABl. L 95 vom 15.4.2010, S. 1) bei audiovisuellen Mediendiensten auf Abruf Deutschland als Sitzland des Diensteanbieters, wenn

1. die Hauptverwaltung in Deutschland liegt und die redaktionellen Entscheidungen über den audiovisuellen Mediendienst dort getroffen werden,

2. die Hauptverwaltung in Deutschland liegt und die redaktionellen Entscheidungen über den audiovisuellen Mediendienst in einem anderen Mitgliedstaat der Europäischen Union getroffen werden, jedoch

   a) ein wesentlicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals in Deutschland tätig ist,

   b) ein wesentlicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals sowohl in Deutschland als auch in dem anderen Mitgliedstaat tätig ist oder

   c) ein wesentlicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals weder in Deutschland noch in dem anderen Mitgliedstaat tätig ist, aber der Diensteanbieter zuerst in Deutschland seine Tätigkeit aufgenommen hat und eine dauerhafte und tatsächliche Verbindung mit der Wirtschaft Deutschlands fortbesteht, oder

3. die Hauptverwaltung in Deutschland liegt und die redaktionellen Entscheidungen über den audiovisuellen Mediendienst in einem Drittstaat getroffen werden oder umgekehrt, aber ein wesentlicher Teil des mit der Bereitstellung des audiovisuellen Mediendienstes betrauten Personals in Deutschland tätig ist.

(3) [1]Für audiovisuelle Mediendiensteanbieter, die nicht bereits aufgrund ihrer Niederlassung der Rechtshoheit Deutschlands oder eines anderen Mitgliedstaats der Europäischen Union unterliegen, gilt Deutschland als Sitzland, wenn sie

[2] § 2a dient der Umsetzung der Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) (ABl. L 95 vom 15.4.2010, S. 1).

1. eine in Deutschland gelegene Satelliten-Bodenstation für die Aufwärtsstrecke nutzen oder

2. zwar keine in einem Mitgliedstaat der Europäischen Union gelegene Satelliten-Bodenstation für die Aufwärtsstrecke nutzen, aber eine Deutschland zugewiesene Übertragungskapazität eines Satelliten nutzen.

[2]Liegt keines dieser beiden Kriterien vor, gilt Deutschland auch als Sitzland für Diensteanbieter, die in Deutschland gemäß den Artikeln 49 bis 55 des Vertrages über die Arbeitsweise der Europäischen Union niedergelassen sind.

## § 3 Herkunftslandprinzip

(1) [1]In der Bundesrepublik Deutschland nach § 2a niedergelassene Diensteanbieter und ihre Telemedien unterliegen den Anforderungen des deutschen Rechts auch dann, wenn die Telemedien in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 89/552/EWG geschäftsmäßig angeboten oder erbracht werden.

(2) [1]Der freie Dienstleistungsverkehr von Telemedien, die in der Bundesrepublik Deutschland von Diensteanbietern geschäftsmäßig angeboten oder erbracht werden, die in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 89/552/EWG niedergelassen sind, wird nicht eingeschränkt. [2]Absatz 5 bleibt unberührt.

(3) [1]Von den Absätzen 1 und 2 bleiben unberührt

1. die Freiheit der Rechtswahl,

2. die Vorschriften für vertragliche Schuldverhältnisse in Bezug auf Verbraucherverträge,

3. gesetzliche Vorschriften über die Form des Erwerbs von Grundstücken und grundstücksgleichen Rechten sowie der Begründung, Übertragung, Änderung oder Aufhebung von dinglichen Rechten an Grundstücken und grundstücksgleichen Rechten,

4. das für den Schutz personenbezogener Daten geltende Recht.

(4) [1]Die Absätze 1 und 2 gelten nicht für

1. die Tätigkeit von Notaren sowie von Angehörigen anderer Berufe, soweit diese ebenfalls hoheitlich tätig sind,

2. die Vertretung von Mandanten und die Wahrnehmung ihrer Interessen vor Gericht,

3. die Zulässigkeit nicht angeforderter kommerzieller Kommunikationen durch elektronische Post,

4. Gewinnspiele mit einem einen Geldwert darstellenden Einsatz bei Glücksspielen, einschließlich Lotterien und Wetten,

5. die Anforderungen an Verteildienste,

6. das Urheberrecht, verwandte Schutzrechte, Rechte im Sinne der Richtlinie 87/54/EWG des Rates vom 16. Dezember 1986 über den Rechtsschutz der Topographien von Halbleitererzeugnissen (ABl. EG Nr. L 24 S. 36) und der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken (ABl. EG Nr. L 77 S. 20) sowie für gewerbliche Schutzrechte,

7. die Ausgabe elektronischen Geldes durch Institute, die gemäß Artikel 8 Abs. 1 der Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (ABl. EG Nr. L 275 S. 39) von der Anwendung einiger oder aller Vorschriften dieser Richtlinie und von der Anwendung der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates vom 20. März 2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (ABl. EG Nr. L 126 S. 1) freigestellt sind,

8. Vereinbarungen oder Verhaltensweisen, die dem Kartellrecht unterliegen,

9. die von den §§ 12, 13a bis 13c, 55a, 83, 110a bis 110d, 111b und 111c des Versicherungsaufsichtsgesetzes in der Fassung der Bekanntmachung vom 17. Dezember 1992 (BGBl. 1993 I S. 2), das zuletzt durch Artikel 2 des Gesetzes vom 29. Juli 2009 (BGBl.I S. 2305) geändert worden ist, in der am 31. Dezember 2015 geltenden Fassung und der Versicherungsberichterstattungs-Verordnung erfassten Bereiche, die Regelungen über das auf Versicherungsverträge anwendbare Recht sowie für Pflichtversicherungen.

(5) [1]Das Angebot und die Erbringung von Telemedien durch einen Diensteanbieter, der in einem anderen Staat im Geltungsbereich der Richtlinien 2000/31/EG oder 89/552/EWG niedergelassen ist, unterliegen abweichend von Absatz 2 den Einschränkungen des innerstaatlichen Rechts, soweit dieses dem Schutz

1. der öffentlichen Sicherheit und Ordnung, insbesondere im Hinblick auf die Verhütung, Ermittlung, Aufklärung, Verfolgung und Vollstreckung von Straftaten und Ordnungswidrigkeiten, einschließlich des Jugendschutzes und der Bekämpfung der Hetze aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität sowie von Verletzungen der Menschenwürde einzelner Personen sowie die Wahrung nationaler Sicherheits- und Verteidigungsinteressen,

2. der öffentlichen Gesundheit,

3. der Interessen der Verbraucher, einschließlich des Schutzes von Anlegern,

vor Beeinträchtigungen oder ernsthaften und schwerwiegenden Gefahren dient und die auf der Grundlage des innerstaatlichen Rechts in Betracht kommenden Maßnahmen in einem angemessenen Verhältnis zu diesen Schutzzielen stehen. [2]Für das Verfahren zur Einleitung von Maßnahmen nach Satz 1 – mit Ausnahme von gerichtlichen Verfahren einschließlich etwaiger Vorverfahren und

der Verfolgung von Straftaten einschließlich der Strafvollstreckung und von Ordnungswidrigkeiten – sehen Artikel 3 Abs. 4 und 5 der Richtlinie 2000/31/EG sowie Artikel 2a Absatz 4 und 5 der Richtlinie 89/552/EWG Konsultations- und Informationspflichten vor.

## Abschnitt 2: Zulassungsfreiheit und Informationspflichten

### § 4 Zulassungsfreiheit

[1]Telemedien sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

### § 5 Allgemeine Informationspflichten

(1) [1]Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen,

2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,

3. soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,

4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,

5. soweit der Dienst in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens dreijährige Berufsausbildung abschließen (ABl. EG Nr. L 19 S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung beruflicher Befähigungsnachweise in Ergänzung

zur Richtlinie 89/48/EWG (ABl. EG Nr. L 209 S. 25, 1995 Nr. L 17 S. 20), zuletzt geändert durch die Richtlinie 97/38/EG der Kommission vom 20. Juni 1997 (ABl. EG Nr. L 184 S. 31), angeboten oder erbracht wird, Angaben über

a) die Kammer, welcher die Diensteanbieter angehören,

b) die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,

c) die Bezeichnung der berufsrechtlichen Regelungen und dazu, wie diese zugänglich sind,

6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung besitzen, die Angabe dieser Nummer,

7. bei Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung, die sich in Abwicklung oder Liquidation befinden, die Angabe hierüber.

(2) [1]Weitergehende Informationspflichten nach anderen Rechtsvorschriften bleiben unberührt.

## § 6 Besondere Informationspflichten bei kommerziellen Kommunikationen

(1) [1]Diensteanbieter haben bei kommerziellen Kommunikationen, die Telemedien oder Bestandteile von Telemedien sind, mindestens die folgenden Voraussetzungen zu beachten:

1. Kommerzielle Kommunikationen müssen klar als solche zu erkennen sein.

2. Die natürliche oder juristische Person, in deren Auftrag kommerzielle Kommunikationen erfolgen, muss klar identifizierbar sein.

3. Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke müssen klar als solche erkennbar sein, und die Bedingungen für ihre Inanspruchnahme müssen leicht zugänglich sein sowie klar und unzweideutig angegeben werden.

4. Preisausschreiben oder Gewinnspiele mit Werbecharakter müssen klar als solche erkennbar und die Teilnahmebedingungen leicht zugänglich sein sowie klar und unzweideutig angegeben werden.

(2) [1]Werden kommerzielle Kommunikationen per elektronischer Post versandt, darf in der Kopf- und Betreffzeile weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. [2]Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der

Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.

(3) [1]Die Vorschriften des Gesetzes gegen den unlauteren Wettbewerb bleiben unberührt.

## Abschnitt 3: Verantwortlichkeit

### § 7 Allgemeine Grundsätze

(1) [1]Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) [1]Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. [2]Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. [3]Das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren.

### § 8 Durchleitung von Informationen

(1) [1]Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

[2]Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) [1]Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

(3) [1]Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

## § 9 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen

[1]Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie

1. die Informationen nicht verändern,
2. die Bedingungen für den Zugang zu den Informationen beachten,
3. die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,
4. die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und
5. unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

[2]§ 8 Abs. 1 Satz 2 gilt entsprechend.

## § 10 Speicherung von Informationen

[1]Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern

1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.

[2]Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

# Abschnitt 4:
# Datenschutz

## § 11 Anbieter-Nutzer-Verhältnis

(1) [1]Die Vorschriften dieses Abschnitts gelten nicht für die Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien, soweit die Bereitstellung solcher Dienste

1. im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder
2. innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

(2) [1]Nutzer im Sinne dieses Abschnitts ist jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

(3) [1]Bei Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, gelten für die Erhebung und Verwendung personenbezogener Daten der Nutzer nur § 15 Absatz 8 und § 16 Absatz 2 Nummer 4.

## § 12 Grundsätze

(1) [1]Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

(2) [1]Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

(3) [1]Soweit nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht automatisiert verarbeitet werden.

## § 13 Pflichten des Diensteanbieters

(1) [1]Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. [2]Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. [3]Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

(2) [1]Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

(3) [1]Der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Recht nach Absatz 2 Nr. 4 hinzuweisen. [2]Absatz 1 Satz 3 gilt entsprechend.

(4) [1]Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 2 gesperrt werden,
3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
5. Daten nach § 15 Abs. 2 nur für Abrechnungszwecke zusammengeführt werden können und
6. Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

[2]An die Stelle der Löschung nach Satz 1 Nr. 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

(5) [1]Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(6) [1]Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. [2]Der Nutzer ist über diese Möglichkeit zu informieren.

(7) [1]Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
2. diese
   (a) gegen Verletzungen des Schutzes personenbezogener Daten und
   (b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

[2]gesichert sind. [3]Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. [4]Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

(8) [1]Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. [2]Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.

## § 14 Bestandsdaten

(1) [1]Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten).

(2) [1]Auf Anordnung der zuständigen Stellen darf der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

## § 15 Nutzungsdaten

(1) [1]Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. Merkmale zur Identifikation 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.

(2) [1]Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemedien zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.

(3) [1]Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. [2]Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. [3]Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

(4) [1]Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). [2]Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren.

(5) [1]Der Diensteanbieter darf an andere Diensteanbieter oder Dritte Abrechnungsdaten übermitteln, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer erforderlich ist. [2]Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. [3]Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen anonymisierte Nutzungsdaten übermittelt werden. [4]§ 14 Abs. 2 findet entsprechende Anwendung.

(6) [1]Die Abrechnung über die Inanspruchnahme von Telemedien darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Telemedien nicht erkennen lassen, es sei denn, der Nutzer verlangt einen Einzelnachweis.

(7) [1]Der Diensteanbieter darf Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers verarbeitet werden, höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung speichern. [2]Werden gegen die Entgeltforderung innerhalb dieser Frist Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen, dürfen die Abrechnungsdaten weiter gespeichert werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen ist.

(8) [1]Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus nur verwenden, soweit dies für Zwecke der Rechtsverfolgung erforderlich ist. [2]Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. [3]Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.

### § 15a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

[1]Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.

## Abschnitt 5: Bußgeldvorschriften

### § 16 Bußgeldvorschriften

(1) [1]Ordnungswidrig handelt, wer absichtlich entgegen § 6 Abs. 2 Satz 1 den Absender oder den kommerziellen Charakter der Nachricht verschleiert oder verheimlicht.

(2) [1]Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 5 Abs. 1 eine Information nicht, nicht richtig oder nicht vollständig verfügbar hält,
2. entgegen § 13 Abs. 1 Satz 1 oder 2 den Nutzer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,
3. einer Vorschrift des § 13 Abs. 4 Satz 1 Nr. 1 bis 4 oder 5 oder Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a über eine dort genannte Pflicht zur Sicherstellung zuwiderhandelt,

4. entgegen § 14 Abs. 1 oder § 15 Abs. 1 Satz 1 oder Abs. 8 Satz 1 oder 2 personenbezogene Daten erhebt oder verwendet oder nicht oder nicht rechtzeitig löscht oder

5. entgegen § 15 Abs. 3 Satz 3 ein Nutzungsprofil mit Daten über den Träger des Pseudonyms zusammenführt.

(3) [1] Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

# §§ 1-3, 88-115
# Telekommunikationsgesetz (TKG)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Telekommunikationsgesetz |
| **Amtliche Abkürzung:** | TKG |
| **Ausfertigung:** | 22.06.2004, BGBl. I 2004 S. 1190 |
| **Inkrafttreten:** | 26.06.2004 |
| **Letzte Änderung:** | 26.07.2016, BGBl. I S. 1818 |

## Inhaltsübersicht


**Teil 1: Allgemeine Vorschriften** **146**
§ 1 Zweck des Gesetzes 146
§ 2 Regulierung, Ziele und Grundsätze 146
§ 3 Begriffsbestimmungen 148
**Teil 7: Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit** **156**
**Abschnitt 1: Fernmeldegeheimnis** **156**
§ 88 Fernmeldegeheimnis 156
§ 89 Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen 156
§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen 157
**Abschnitt 2: Datenschutz** **158**
§ 91 Anwendungsbereich 158
§ 92 (weggefallen) 158
§ 93 Informationspflichten 158
§ 94 Einwilligung im elektronischen Verfahren 159
§ 95 Vertragsverhältnisse 159
§ 96 Verkehrsdaten 160
§ 97 Entgeltermittlung und Entgeltabrechnung 161
§ 98 Standortdaten 162
§ 99 Einzelverbindungsnachweis 163
§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten 164
§ 101 Mitteilen ankommender Verbindungen 165
§ 102 Rufnummernanzeige und -unterdrückung 166
§ 103 Automatische Anrufweiterschaltung 167

§ 104 Teilnehmerverzeichnisse 167
§ 105 Auskunftserteilung 167
§ 106 Telegrammdienst 168
§ 107 Nachrichtenübermittlungssysteme mit Zwischenspeicherung 168
**Abschnitt 3: Öffentliche Sicherheit 169**
§ 108 Notruf 169
§ 109 Technische Schutzmaßnahmen 171
§ 109a Daten- und Informationssicherheit 174
§ 110 Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften 175
§ 111 Daten für Auskunftsersuchen der Sicherheitsbehörden 178
§ 112 Automatisiertes Auskunftsverfahren 180
§ 113 Manuelles Auskunftsverfahren 183
§ 113a Verpflichtete; Entschädigung 184
§ 113b Pflichten zur Speicherung von Verkehrsdaten 184
§ 113c Verwendung der Daten 186
§ 113d Gewährleistung der Sicherheit der Daten 187
§ 113e Protokollierung 187
§ 113f Anforderungskatalog 187
§ 113g Sicherheitskonzept 188
§ 114 Auskunftsersuchen des Bundesnachrichtendienstes 188
§ 115 Kontrolle und Durchsetzung von Verpflichtungen 189

# Teil 1: Allgemeine Vorschriften

## § 1 Zweck des Gesetzes

[1]Zweck dieses Gesetzes ist es, durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten.

## § 2 Regulierung, Ziele und Grundsätze

(1) [1]Die Regulierung der Telekommunikation ist eine hoheitliche Aufgabe des Bundes.

(2) [1]Ziele der Regulierung sind:

1. die Wahrung der Nutzer-, insbesondere der Verbraucherinteressen auf dem Gebiet der Telekommunikation und die Wahrung des Fernmeldegeheimnisses. [2]Die Bundesnetzagentur fördert die Möglichkeit der Endnutzer, Informationen abzurufen und zu verbreiten oder Anwendungen und

Dienste ihrer Wahl zu nutzen. [3]Die Bundesnetzagentur berücksichtigt die Bedürfnisse bestimmter gesellschaftlicher Gruppen, insbesondere von behinderten Nutzern, älteren Menschen und Personen mit besonderen sozialen Bedürfnissen,

2. die Sicherstellung eines chancengleichen Wettbewerbs und die Förderung nachhaltig wettbewerbsorientierter Märkte der Telekommunikation im Bereich der Telekommunikationsdienste und -netze sowie der zugehörigen Einrichtungen und Dienste, auch in der Fläche. [4]Die Bundesnetzagentur stellt insoweit auch sicher, dass für die Nutzer, einschließlich behinderter Nutzer, älterer Menschen und Personen mit besonderen sozialen Bedürfnissen, der größtmögliche Nutzen in Bezug auf Auswahl, Preise und Qualität erbracht wird. [5]Sie gewährleistet, dass es im Bereich der Telekommunikation, einschließlich der Bereitstellung von Inhalten, keine Wettbewerbsverzerrungen oder -beschränkungen gibt,

3. die Entwicklung des Binnenmarktes der Europäischen Union zu fördern,

4. die Sicherstellung einer flächendeckenden gleichartigen Grundversorgung in städtischen und ländlichen Räumen mit Telekommunikationsdiensten (Universaldienstleistungen) zu erschwinglichen Preisen,

5. die Beschleunigung des Ausbaus von hochleistungsfähigen öffentlichen Telekommunikationsnetzen der nächsten Generation,

6. die Förderung von Telekommunikationsdiensten bei öffentlichen Einrichtungen,

7. die Sicherstellung einer effizienten und störungsfreien Nutzung von Frequenzen, auch unter Berücksichtigung der Belange des Rundfunks,

8. eine effiziente Nutzung von Nummerierungsressourcen zu gewährleisten,

9. die Wahrung der Interessen der öffentlichen Sicherheit.

(3) [1]Die Bundesnetzagentur wendet bei der Verfolgung der in Absatz 2 festgelegten Ziele objektive, transparente, nicht diskriminierende und verhältnismäßige Regulierungsgrundsätze an, indem sie unter anderem

1. die Vorhersehbarkeit der Regulierung dadurch fördert, dass sie über angemessene Überprüfungszeiträume ein einheitliches Regulierungskonzept beibehält,

2. gewährleistet, dass Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten unter vergleichbaren Umständen nicht diskriminiert werden,

3. den Wettbewerb zum Nutzen der Verbraucher schützt und, soweit sachgerecht, den infrastrukturbasierten Wettbewerb fördert,

4. effiziente Investitionen und Innovationen im Bereich neuer und verbesserter Infrastrukturen auch dadurch fördert, dass sie dafür sorgt, dass bei jeglicher Zugangsverpflichtung dem Risiko der investierenden Unternehmen gebührend Rechnung getragen wird, und dass sie verschiedene Kooperationsvereinbarungen zur Aufteilung des Investitionsrisikos zwischen Investoren und Zugangsbegehrenden zulässt, während sie gleichzeitig gewährleistet, dass der Wettbewerb auf dem Markt und der GrundSatz der Nichtdiskriminierung gewahrt werden,

5. die vielfältigen Bedingungen im Zusammenhang mit Wettbewerb und Verbrauchern, die in den verschiedenen geografischen Gebieten innerhalb der Bundesrepublik Deutschland herrschen, gebührend berücksichtigt und

6. regulatorische Vorabverpflichtungen nur dann auferlegt, wenn es keinen wirksamen und nachhaltigen Wettbewerb gibt, und diese Verpflichtungen lockert oder aufhebt, sobald es einen solchen Wettbewerb gibt.

(4) [1]Die Vorschriften des Gesetzes gegen Wettbewerbsbeschränkungen bleiben, soweit nicht durch dieses Gesetz ausdrücklich abschließende Regelungen getroffen werden, anwendbar. [2]Die Aufgaben und Zuständigkeiten der Kartellbehörden bleiben unberührt.

(5) [1]Die hoheitlichen Rechte des Bundesministeriums der Verteidigung bleiben unberührt.

(6) [1]Die Belange des Rundfunks und vergleichbarer Telemedien sind unabhängig von der Art der Übertragung zu berücksichtigen. [2]Die medienrechtlichen Bestimmungen der Länder bleiben unberührt.

## § 3 Begriffsbestimmungen

[1]Im Sinne dieses Gesetzes ist oder sind

1. „Anruf“ eine über einen öffentlich zugänglichen Telekommunikationsdienst aufgebaute Verbindung, die eine zweiseitige Sprachkommunikation ermöglicht;

2. „Anwendungs-Programmierschnittstelle“ die Software-Schnittstelle zwischen Anwendungen, die von Sendeanstalten oder Diensteanbietern zur Verfügung gestellt werden, und den Anschlüssen in den erweiterten digitalen Fernsehempfangsgeräten für digitale Fernseh- und Rundfunkdienste;

2a. „Auskunftsdienste“ bundesweit jederzeit telefonisch erreichbare Dienste, insbesondere des Rufnummernbereichs 118, die ausschließlich der neutralen Weitergabe von Rufnummer, Name, Anschrift sowie zusätzlichen Angaben von Telekommunikationsnutzern dienen. [2]Die Weitervermittlung zu einem erfragten Teilnehmer oder Dienst kann Bestandteil des Auskunftsdienstes sein;

3. „Bestandsdaten“ Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden;

4. „beträchtliche Marktmacht“ eines oder mehrerer Unternehmen gegeben, wenn die Voraussetzungen nach § 11 Absatz 1 Satz 3 und 4 vorliegen;

4a. „Betreiberauswahl“ der Zugang eines Teilnehmers zu den Diensten aller unmittelbar zusammengeschalteten Anbieter von öffentlich zugänglichen Telekommunikationsdiensten im Einzelwahlverfahren durch Wählen einer Kennzahl;

4b. „Betreibervorauswahl“ der Zugang eines Teilnehmers zu den Diensten aller unmittelbar zusammengeschalteten Anbieter von öffentlich zugänglichen Telekommunikationsdiensten durch festgelegte Vorauswahl, wobei der Teilnehmer unterschiedliche Voreinstellungen für Orts- und Fernverbindungen vornehmen kann und bei jedem Anruf die festgelegte Vorauswahl durch Wählen einer Betreiberkennzahl übergehen kann;

5. „Dienst mit Zusatznutzen“ jeder Dienst, der die Erhebung und Verwendung von Verkehrsdaten oder Standortdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Entgeltabrechnung dieses Vorganges erforderliche Maß hinausgeht;

6. „Diensteanbieter“ jeder, der ganz oder teilweise geschäftsmäßig

   (a) Telekommunikationsdienste erbringt oder

   (b) an der Erbringung solcher Dienste mitwirkt;

7. „digitales Fernsehempfangsgerät“ ein Fernsehgerät mit integriertem digitalem Decoder oder ein an ein Fernsehgerät anschließbarer digitaler Decoder zur Nutzung digital übertragener Fernsehsignale, die mit Zusatzsignalen, einschließlich einer Zugangsberechtigung, angereichert sein können;

7a. „Einzelrichtlinien“

   (a) die Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie) (ABl. L 108 vom 24.4.2002, S. 21), die zuletzt durch die Richtlinie 2009/140/EG (ABl. L 337 vom 18.12.2009, S. 37) geändert worden ist;

   (b) die Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie) (ABl. L 108 vom 24.4.2002, S. 7), die zuletzt durch die Richtlinie 2009/140/EG (ABl. L 337 vom 18.12.2009, S. 37) geändert worden ist;

   (c) die Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie) (ABl. L 108 vom 24.4.2002, S. 51), die zuletzt durch die Richtlinie 2009/136/EG (ABl. L 337 vom 18.12.2009, S. 11) geändert worden ist, und

(d) die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37), die zuletzt durch die Richtlinie 2009/136/EG (ABl. L 337 vom 18.12.2009, S. 11) geändert worden ist;

8. „Endnutzer“ ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt;

8a. „entgeltfreie Telefondienste“ Dienste, insbesondere des Rufnummernbereichs (0)800, bei deren Inanspruchnahme der Anrufende kein Entgelt zu entrichten hat;

8b. „Service-Dienste” Dienste, insbesondere des Rufnummernbereichs (0)180, die bundesweit zu einem einheitlichen Entgelt zu erreichen sind;

9. Frequenznutzung“ jede gewollte Aussendung oder Abstrahlung elektromagnetischer Wellen zwischen 9 kHz und 3 000 GHz zur Nutzung durch Funkdienste und andere Anwendungen elektromagnetischer Wellen;

9a. „Frequenzzuweisung“ die Benennung eines bestimmten Frequenzbereichs für die Nutzung durch einen oder mehrere Funkdienste oder durch andere Anwendungen elektromagnetischer Wellen, falls erforderlich mit weiteren Festlegungen;

9b. „gemeinsamer Zugang zum Teilnehmeranschluss“ die Bereitstellung des Zugangs zum Teilnehmeranschluss oder zum Teilabschnitt in der Weise, dass die Nutzung eines bestimmten Teils der Kapazität der Netzinfrastruktur, wie etwa eines Teils der Frequenz oder Gleichwertiges, ermöglicht wird;

9c. „GEREK“ das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation;

10. „geschäftsmäßiges Erbringen“ von Telekommunikationsdiensten das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht;

10a. (weggefallen)

11. „Kundenkarten“ Karten, mit deren Hilfe Telekommunikationsverbindungen hergestellt und personenbezogene Daten erhoben werden können;

11a. „Kurzwahl-Datendienste“ Kurzwahldienste, die der Übermittlung von nichtsprachgestützten Inhalten mittels Telekommunikation dienen und die keine Telemedien sind;

11b. „Kurzwahldienste“ Dienste, die die Merkmale eines Premium-Dienstes haben, jedoch eine spezielle Nummernart mit kurzen Nummern nutzen;

11c. „Kurzwahl-Sprachdienste“ Kurzwahldienste, bei denen die Kommunikation sprachgestützt erfolgt;

11d. „Massenverkehrs-Dienste“ Dienste, insbesondere des Rufnummernbereichs (0)137, die charakterisiert sind durch ein hohes Verkehrsaufkommen in einem oder mehreren kurzen Zeitintervallen mit kurzer Belegungsdauer zu einem Ziel mit begrenzter Abfragekapazität;

12. „nachhaltig wettbewerbsorientierter Markt“ ein Markt, auf dem der Wettbewerb so abgesichert ist, dass er ohne sektorspezifische Regulierung besteht;

12a. „Netzabschlusspunkt“ der physische Punkt, an dem einem Teilnehmer der Zugang zu einem Telekommunikationsnetz bereitgestellt wird; in Netzen, in denen eine Vermittlung oder Leitwegebestimmung erfolgt, wird der Netzabschlusspunkt anhand einer bestimmten Netzadresse bezeichnet, die mit der Nummer oder dem Namen eines Teilnehmers verknüpft sein kann;

12b. „Neuartige Dienste“ Dienste, insbesondere des Rufnummernbereichs (0)12, bei denen Nummern für einen Zweck verwendet werden, für den kein anderer Rufnummernraum zur Verfügung steht;

13. „Nummern“ Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen;

13a. „Nummernart“ die Gesamtheit aller Nummern eines Nummernraums für einen bestimmten Dienst oder eine bestimmte technische Adressierung;

13b. „Nummernbereich“ eine für eine Nummernart bereitgestellte Teilmenge des Nummernraums;

13c. „Nummernraum“ die Gesamtheit aller Nummern, die für eine bestimmte Art der Adressierung verwendet werden;

13e. „Nummernteilbereich“ eine Teilmenge eines Nummernbereichs;

14. „Nutzer“ jede natürliche oder juristische Person, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt oder beantragt, ohne notwendigerweise Teilnehmer zu sein;

15. „öffentliches Münz- und Kartentelefon“ ein der Allgemeinheit zur Verfügung stehendes Telefon, für dessen Nutzung als Zahlungsmittel unter anderem Münzen, Kredit- und Abbuchungskarten oder Guthabenkarten, auch solche mit Einwahlcode, verwendet werden können;

16. „öffentliches Telefonnetz“ ein Telekommunikationsnetz, das zur Bereitstellung des öffentlich zugänglichen Telefondienstes genutzt wird und darüber hinaus weitere Dienste wie Telefax- oder Datenfernübertragung und einen funktionalen Internetzugang ermöglicht;

16a. „öffentliches Telekommunikationsnetz“ ein Telekommunikationsnetz, das ganz oder überwiegend der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen;

17. „öffentlich zugänglicher Telefondienst“ ein der Öffentlichkeit zur Verfügung stehender Dienst, der direkt oder indirekt über eine oder mehrere Nummern eines nationalen oder internationalen Telefonnummernplans oder eines anderen Adressierungsschemas das Führen folgender Gespräche ermöglicht:

    (a) aus- und eingehende Inlandsgespräche oder

    (b) aus- und eingehende Inlands- und Auslandsgespräche;

17a. „öffentlich zugängliche Telekommunikationsdienste“ der Öffentlichkeit zur Verfügung stehende Telekommunikationsdienste;

17b. „Premium-Dienste“ Dienste, insbesondere der Rufnummernbereiche (0)190 und (0)900, bei denen über die Telekommunikationsdienstleistung hinaus eine weitere Dienstleistung erbracht wird, die gegenüber dem Anrufer gemeinsam mit der Telekommunikationsdienstleistung abgerechnet wird und die nicht einer anderen Nummernart zuzurechnen ist;

18. „Rufnummer“ eine Nummer, durch deren Wahl im öffentlich zugänglichen Telefondienst eine Verbindung zu einem bestimmten Ziel aufgebaut werden kann;

18a. „Rufnummernbereich“ eine für eine Nummernart bereitgestellte Teilmenge des Nummernraums für das öffentliche Telefonnetz;

19. „Standortdaten“ Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben;

19a. „Teilabschnitt“ eine Teilkomponente des Teilnehmeranschlusses, die den Netzabschlusspunkt am Standort des Teilnehmers mit einem Konzentrationspunkt oder einem festgelegten zwischengeschalteten Zugangspunkt des öffentlichen Festnetzes verbindet;

20. „Teilnehmer“ jede natürliche oder juristische Person, die mit einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat;

21. „Teilnehmeranschluss“ die physische Verbindung, mit dem der Netzabschlusspunkt in den Räumlichkeiten des Teilnehmers mit den Hauptverteilerknoten oder mit einer gleichwertigen Einrichtung in festen öffentlichen Telefonnetzen verbunden wird;

22. „Telekommunikation“ der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen;

23. „Telekommunikationsanlagen“ technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können;

24. „Telekommunikationsdienste“ in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen;

25. „telekommunikationsgestützte Dienste“ Dienste, die keinen räumlich und zeitlich trennbaren Leistungsfluss auslösen, sondern bei denen die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird;

26. „Telekommunikationslinien“ unter- oder oberirdisch geführte Telekommunikationskabelanlagen einschließlich ihrer zugehörigen Schalt- und Verzweigungseinrichtungen, Masten und Unterstützungen, Kabelschächte und Kabelkanalrohre;

27. „Telekommunikationsnetz“ die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen, leitungs- und paketvermittelten Netzen, einschließlich des Internets, und mobilen terrestrischen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information;

28. „Übertragungsweg“ Telekommunikationsanlagen in Form von Kabel- oder Funkverbindungen mit ihren übertragungstechnischen Einrichtungen als Punkt-zu-Punkt- oder Punkt-zu-Mehrpunktverbindungen mit einem bestimmten Informationsdurchsatzvermögen (Bandbreite oder Bitrate) einschließlich ihrer Abschlusseinrichtungen;

29. „Unternehmen“ das Unternehmen selbst oder mit ihm im Sinne des § 36 Abs. 2 und § 37 Abs. 1 und 2 des Gesetzes gegen Wettbewerbsbeschränkungen verbundene Unternehmen;

30. „Verkehrsdaten“ Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden;

30a. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Datensicherheit, die zum Verlust, zur unrechtmäßigen Löschung, Veränderung, Speicherung, Weitergabe oder sonstigen unrechtmäßigen Verwendung personenbezogener Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste verarbeitet werden sowie der unrechtmäßige Zugang zu diesen;

30b. „vollständig entbündelter Zugang zum Teilnehmeranschluss“ die Bereitstellung des Zugangs zum Teilnehmeranschluss oder zum Teilabschnitt in der Weise, dass die Nutzung der gesamten Kapazität der Netzinfrastruktur ermöglicht wird;

30c. „Warteschleife“ jede vom Nutzer eines Telekommunikationsdienstes eingesetzte Vorrichtung oder Geschäftspraxis, über die Anrufe entgegengenommen oder aufrechterhalten werden, ohne dass das Anliegen des Anrufers bearbeitet wird. [3]Dies umfasst die Zeitspanne ab Rufaufbau vom Anschluss des Anrufers bis zu dem Zeitpunkt, an dem mit der Bearbeitung des Anliegens des Anrufers begonnen wird, gleichgültig ob dies über einen automatisierten Dialog oder durch eine persönliche Bearbeitung erfolgt. [4]Ein automatisierter Dialog beginnt, sobald automatisiert Informationen abgefragt werden, die für die Bearbeitung des Anliegens erforderlich sind. [5]Eine persönliche Bearbeitung des Anliegens beginnt, sobald eine natürliche Person den Anruf entgegennimmt und bearbeitet. [6]Hierzu zählt auch die Abfrage von Informationen, die für die Bearbeitung des Anliegens erforderlich sind. [7]Als Warteschleife ist ferner die Zeitspanne anzusehen, die anlässlich einer Weiterleitung zwischen Beendigung der vorhergehenden Bearbeitung des Anliegens und der weiteren Bearbeitung vergeht, ohne dass der Anruf technisch unterbrochen wird. [8]Keine Warteschleife sind automatische Bandansagen, wenn die Dienstleistung für den Anrufer vor Herstellung der Verbindung erkennbar ausschließlich in einer Bandansage besteht;

31. „wirksamer Wettbewerb“ die Abwesenheit von beträchtlicher Marktmacht im Sinne des § 11 Absatz 1 Satz 3 und 4;

32. „Zugang“ die Bereitstellung von Einrichtungen oder Diensten für ein anderes Unternehmen unter bestimmten Bedingungen zum Zwecke der Erbringung von Telekommunikationsdiensten, auch bei deren Verwendung zur Erbringung von Diensten der Informationsgesellschaft oder Rundfunkinhaltediensten. [9]Dies umfasst unter anderem Folgendes:

    (a) Zugang zu Netzkomponenten, einschließlich nicht aktiver Netzkomponenten, und zugehörigen Einrichtungen, wozu auch der feste oder nicht feste Anschluss von Geräten gehören kann. [10]Dies beinhaltet insbesondere den Zugang zum Teilnehmeranschluss sowie zu Einrichtungen und Diensten, die erforderlich sind, um Dienste über den Teilnehmeranschluss zu erbringen, einschließlich des Zugangs zur Anschaltung und Ermöglichung des Anbieterwechsels des Teilnehmers und zu hierfür notwendigen Informationen und Daten und zur Entstörung;

    (b) Zugang zu physischen Infrastrukturen wie Gebäuden, Leitungsrohren und Masten;

    (c) Zugang zu einschlägigen Softwaresystemen, einschließlich Systemen für die Betriebsunterstützung;

    (d) Zugang zu informationstechnischen Systemen oder Datenbanken für Vorbestellung, Bereitstellung, Auftragserteilung, Anforderung von Wartungs- und Instandsetzungsarbeiten sowie Abrechnung;

    (e) Zugang zur Nummernumsetzung oder zu Systemen, die eine gleichwertige Funktion bieten;

    (f) Zugang zu Fest- und Mobilfunknetzen, insbesondere, um Roaming zu ermöglichen;

(g) Zugang zu Zugangsberechtigungssystemen für Digitalfernsehdienste und

(h) Zugang zu Diensten für virtuelle Netze;

33. „Zugangsberechtigungssysteme“ technische Verfahren oder Vorrichtungen, welche die erlaubte Nutzung geschützter Rundfunkprogramme von einem Abonnement oder einer individuellen Erlaubnis abhängig machen;

33a. „zugehörige Dienste“ diejenigen mit einem Telekommunikationsnetz oder einem Telekommunikationsdienst verbundenen Dienste, welche die Bereitstellung von Diensten über dieses Netz oder diesen Dienst ermöglichen, unterstützen oder dazu in der Lage sind. [11]Darunter fallen unter anderem Systeme zur Nummernumsetzung oder Systeme, die eine gleichwertige Funktion bieten, Zugangsberechtigungssysteme und elektronische Programmführer sowie andere Dienste wie Dienste im Zusammenhang mit Identität, Standort und Präsenz des Nutzers;

33b. „zugehörige Einrichtungen“ diejenigen mit einem Telekommunikationsnetz oder einem Telekommunikationsdienst verbundenen zugehörigen Dienste, physischen Infrastrukturen und sonstigen Einrichtungen und Komponenten, welche die Bereitstellung von Diensten über dieses Netz oder diesen Dienst ermöglichen, unterstützen oder dazu in der Lage sind. [12]Darunter fallen unter anderem Gebäude, Gebäudezugänge, Verkabelungen in Gebäuden, Antennen, Türme und andere Trägerstrukturen, Leitungsrohre, Leerrohre, Masten, Einstiegsschächte und Verteilerkästen;

34. „Zusammenschaltung“ derjenige Zugang, der die physische und logische Verbindung öffentlicher Telekommunikationsnetze herstellt, um Nutzern eines Unternehmens die Kommunikation mit Nutzern desselben oder eines anderen Unternehmens oder die Inanspruchnahme von Diensten eines anderen Unternehmens zu ermöglichen; Dienste können von den beteiligten Parteien erbracht werden oder von anderen Parteien, die Zugang zum Netz haben. [13]Zusammenschaltung ist ein Sonderfall des Zugangs und wird zwischen Betreibern öffentlicher Telekommunikationsnetze hergestellt.

# Teil 7:
# Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit

## Abschnitt 1:
## Fernmeldegeheimnis

### § 88 Fernmeldegeheimnis

(1) [1]Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. [2]Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) [1]Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. [2]Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) [1]Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. [2]Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. [3]Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. [4]Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) [1]Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

### § 89 Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen

[1]Mit einer Funkanlage dürfen nur Nachrichten, die für den Betreiber der Funkanlage, Funkamateure im Sinne des Gesetzes über den Amateurfunk vom 23. Juni 1997 (BGBl. I S. 1494), die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, abgehört werden. [2]Der Inhalt anderer als in Satz 1 genannter Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht

zur Geheimhaltung nicht schon nach § 88 besteht, anderen nicht mitgeteilt werden. [3]§ 88 Abs. 4 gilt entsprechend. [4]Das Abhören und die Weitergabe von Nachrichten auf Grund besonderer gesetzlicher Ermächtigung bleiben unberührt.

## § 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen

(1) [1]Es ist verboten, Sendeanlagen oder sonstige Telekommunikationsanlagen zu besitzen, herzustellen, zu vertreiben, einzuführen oder sonst in den Geltungsbereich dieses Gesetzes zu verbringen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und auf Grund dieser Umstände oder auf Grund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen. [2]Das Verbot, solche Anlagen zu besitzen, gilt nicht für denjenigen, der die tatsächliche Gewalt über eine solche Anlage

1. als Organ, als Mitglied eines Organs, als gesetzlicher Vertreter oder als vertretungsberechtigter Gesellschafter eines Berechtigten nach Absatz 2 erlangt,
2. von einem anderen oder für einen anderen Berechtigten nach Absatz 2 erlangt, sofern und solange er die Weisungen des anderen über die Ausübung der tatsächlichen Gewalt über die Anlage auf Grund eines Dienst- oder Arbeitsverhältnisses zu befolgen hat oder die tatsächliche Gewalt auf Grund gerichtlichen oder behördlichen Auftrags ausübt,
3. als Gerichtsvollzieher oder Vollzugsbeamter in einem Vollstreckungsverfahren erwirbt,
4. von einem Berechtigten nach Absatz 2 vorübergehend zum Zwecke der sicheren Verwahrung oder der nicht gewerbsmäßigen Beförderung zu einem Berechtigten erlangt,
5. lediglich zur gewerbsmäßigen Beförderung oder gewerbsmäßigen Lagerung erlangt,
6. durch Fund erlangt, sofern er die Anlage unverzüglich dem Verlierer, dem Eigentümer, einem sonstigen Erwerbsberechtigten oder der für die Entgegennahme der Fundanzeige zuständigen Stelle abliefert,
7. von Todes wegen erwirbt, sofern er die Anlage unverzüglich einem Berechtigten überlässt oder sie für dauernd unbrauchbar macht,
8. erlangt, die durch Entfernen eines wesentlichen Bauteils dauernd unbrauchbar gemacht worden ist, sofern er den Erwerb unverzüglich der Bundesnetzagentur schriftlich anzeigt, dabei seine Personalien, die Art der Anlage, deren Hersteller- oder Warenzeichen und, wenn die Anlage eine Herstellungsnummer hat, auch diese angibt sowie glaubhaft macht, dass er die Anlage ausschließlich zu Sammlerzwecken erworben hat.

(2) [1]Die zuständigen obersten Bundes- oder Landesbehörden lassen Ausnahmen zu, wenn es im öffentlichen Interesse, insbesondere aus Gründen der öffentlichen Sicherheit, erforderlich ist. [2]Absatz 1 Satz 1 gilt nicht, soweit das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) die Ausfuhr der Sendeanlagen oder sonstigen Telekommunikationsanlagen genehmigt hat.

(3) [1]Es ist verboten, öffentlich oder in Mitteilungen, die für einen größeren Personenkreis bestimmt sind, für Sendeanlagen oder sonstige Telekommunikationsanlagen mit dem Hinweis zu werben, dass sie geeignet sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder dessen Bild von diesem unbemerkt aufzunehmen.

## Abschnitt 2: Datenschutz

### § 91 Anwendungsbereich

(1) [1]Dieser Abschnitt regelt den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken. [2]Dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft, sofern sie mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, stehen den personenbezogenen Daten gleich.

(2) [1]Für geschlossene Benutzergruppen öffentlicher Stellen der Länder gilt dieser Abschnitt mit der Maßgabe, dass an die Stelle des Bundesdatenschutzgesetzes die jeweiligen Landesdatenschutzgesetze treten.

### § 92 (weggefallen)

### § 93 Informationspflichten

(1) [1]Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. [2]Dabei sind die Teilnehmer auch auf die zulässigen Wahl- und Gestaltungsmög-

lichkeiten hinzuweisen. [3]Die Nutzer sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten. [4]Das Auskunftsrecht nach dem Bundesdatenschutzgesetz bleibt davon unberührt.

(2) [1]Unbeschadet des Absatzes 1 hat der Diensteanbieter in den Fällen, in denen ein besonderes Risiko der Verletzung der Netzsicherheit besteht, die Teilnehmer über dieses Risiko und, wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahme liegt, über mögliche Abhilfen, einschließlich der für sie voraussichtlich entstehenden Kosten, zu unterrichten.

(3) [1]Im Fall einer Verletzung des Schutzes personenbezogener Daten haben die betroffenen Teilnehmer oder Personen die Rechte aus § 109a Absatz 1 Satz 2 in Verbindung mit Absatz 2.

## § 94 Einwilligung im elektronischen Verfahren

[1]Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. der Teilnehmer oder Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Teilnehmer oder Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Teilnehmer oder Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

## § 95 Vertragsverhältnisse

(1) [1]Der Diensteanbieter darf Bestandsdaten erheben und verwenden, soweit dieses zur Erreichung des in § 3 Nr. 3 genannten Zweckes erforderlich ist. [2]Im Rahmen eines Vertragsverhältnisses mit einem anderen Diensteanbieter darf der Diensteanbieter Bestandsdaten seiner Teilnehmer und der Teilnehmer des anderen Diensteanbieters erheben und verwenden, soweit dies zur Erfüllung des Vertrages zwischen den Diensteanbietern erforderlich ist. [3]Eine Übermittlung der Bestandsdaten an Dritte erfolgt, soweit nicht dieser Teil oder ein anderes Gesetz sie zulässt, nur mit Einwilligung des Teilnehmers.

(2) [1]Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, zur Werbung für eigene Angebote, zur Marktforschung und zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. [2]Ein Diensteanbieter, der im Rahmen einer bestehenden Kundenbeziehung rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers

erhalten hat, darf diese für die Versendung von Text- oder Bildmitteilungen an ein Telefon oder an eine Postadresse zu den in Satz 1 genannten Zwecken verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. [3]Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann.

(3) [1]Endet das Vertragsverhältnis, sind die Bestandsdaten vom Diensteanbieter mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. [2]§ 35 Abs. 3 des Bundesdatenschutzgesetzes gilt entsprechend.

(4) [1]Der Diensteanbieter kann im Zusammenhang mit dem Begründen und dem Ändern des Vertragsverhältnisses sowie dem Erbringen von Telekommunikationsdiensten die Vorlage eines amtlichen Ausweises verlangen, wenn dies zur Überprüfung der Angaben des Teilnehmers erforderlich ist. [2]Die Pflicht nach § 111 Absatz 1 Satz 3 bleibt unberührt. [3]Er kann von dem Ausweis eine Kopie erstellen. [4]Die Kopie ist vom Diensteanbieter unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Teilnehmers zu vernichten. [5]Andere als die nach Absatz 1 zulässigen Daten darf der Diensteanbieter dabei nicht verwenden.

(5) [1]Die Erbringung von Telekommunikationsdiensten darf nicht von einer Einwilligung des Teilnehmers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden, wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten ohne die Einwilligung nicht oder in nicht zumutbarer Weise möglich ist. [2]Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

## § 96 Verkehrsdaten

(1) [1]Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt genannten Zwecke erforderlich ist:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,

2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,

3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,

4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,

5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

[2]Diese Verkehrsdaten dürfen nur verwendet werden, soweit dies für die in Satz 1 genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen erforderlich ist. [3]Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.

(2) [1]Eine über Absatz 1 hinausgehende Erhebung oder Verwendung der Verkehrsdaten ist unzulässig.

(3) [1]Der Diensteanbieter darf teilnehmerbezogene Verkehrsdaten, die vom Anbieter eines öffentlich zugänglichen Telekommunikationsdienstes verwendet werden, zum Zwecke der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und im dazu erforderlichen Zeitraum nur verwenden, sofern der Betroffene in diese Verwendung eingewilligt hat. [2]Die Daten der Angerufenen sind unverzüglich zu anonymisieren. [3]Eine zielnummernbezogene Verwendung der Verkehrsdaten durch den Diensteanbieter zu den in Satz 1 genannten Zwecken ist nur mit Einwilligung der Angerufenen zulässig. [4]Hierbei sind die Daten der Anrufenden unverzüglich zu anonymisieren.

(4) [1]Bei der Einholung der Einwilligung ist dem Teilnehmer mitzuteilen, welche Datenarten für die in Absatz 3 Satz 1 genannten Zwecke verarbeitet werden sollen und wie lange sie gespeichert werden sollen. [2]Außerdem ist der Teilnehmer darauf hinzuweisen, dass er die Einwilligung jederzeit widerrufen kann.

## § 97 Entgeltermittlung und Entgeltabrechnung

(1) [1]Diensteanbieter dürfen die in § 96 Abs. 1 aufgeführten Verkehrsdaten verwenden, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Teilnehmern benötigt werden. [2]Erbringt ein Diensteanbieter seine Dienste über ein öffentliches Telekommunikationsnetz eines fremden Betreibers, darf der Betreiber des öffentlichen Telekommunikationsnetzes dem Diensteanbieter die für die Erbringung von dessen Diensten erhobenen Verkehrsdaten übermitteln. [3]Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er dem Dritten die in Absatz 2 genannten Daten übermitteln, soweit es zum Einzug des Entgelts und der Erstellung einer detaillierten Rechnung erforderlich ist. [4]Der Dritte ist vertraglich zur Wahrung des Fernmeldegeheimnisses nach § 88 und des Datenschutzes nach den §§ 93 und 95 bis 97, 99 und 100 zu verpflichten. [5]§ 11 des Bundesdatenschutzgesetzes bleibt unberührt.

(2) [1]Der Diensteanbieter darf zur ordnungsgemäßen Ermittlung und Abrechnung der Entgelte für Telekommunikationsdienste und zum Nachweis der Richtigkeit derselben folgende personenbezogene Daten nach Maßgabe der Absätze 3 bis 6 erheben und verwenden:

1. die Verkehrsdaten nach § 96 Abs. 1,

2. die Anschrift des Teilnehmers oder Rechnungsempfängers, die Art des Anschlusses, die Zahl der im Abrechnungszeitraum einer planmäßigen Entgeltabrechnung insgesamt aufgekommenen Entgelteinheiten, die übermittelten Datenmengen, das insgesamt zu entrichtende Entgelt,

3. sonstige für die Entgeltabrechnung erhebliche Umstände wie Vorschusszahlungen, Zahlungen mit Buchungsdatum, Zahlungsrückstände, Mahnungen, durchgeführte und aufgehobene Anschlusssperren, eingereichte und bearbeitete Reklamationen, beantragte und genehmigte Stundungen, Ratenzahlungen und Sicherheitsleistungen.

(3) [1]Der Diensteanbieter hat nach Beendigung der Verbindung aus den Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 3 und 5 unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. [2]Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. [3]Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen. [4]Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

(4) [1]Soweit es für die Abrechnung des Diensteanbieters mit anderen Diensteanbietern oder mit deren Teilnehmern sowie anderer Diensteanbieter mit ihren Teilnehmern erforderlich ist, darf der Diensteanbieter Verkehrsdaten verwenden.

(5) [1]Zieht der Diensteanbieter mit der Rechnung Entgelte für Leistungen eines Dritten ein, die dieser im Zusammenhang mit der Erbringung von Telekommunikationsdiensten erbracht hat, so darf er dem Dritten Bestands- und Verkehrsdaten übermitteln, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Teilnehmer erforderlich sind.

## § 98 Standortdaten

(1) [1]Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet werden, dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat. [2]In diesen Fällen hat der Anbieter des Dienstes mit Zusatznutzen bei jeder Feststellung des Standortes des Mobilfunkendgerätes den Nutzer durch eine Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurden, zu informieren. [3]Dies gilt nicht, wenn der Standort nur auf dem Endgerät angezeigt wird, dessen Standortdaten ermittelt wurden. [4]Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 seine Einwilligung ausdrücklich, gesondert und schriftlich gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilen. [5]In diesem Fall gilt die Verpflichtung nach Satz 2 entsprechend für den Anbieter des Dienstes mit Zusatznutzen. [6]Der Anbieter des Dienstes mit Zusatznutzen darf die erfor-

derlichen Bestandsdaten zur Erfüllung seiner Verpflichtung aus Satz 2 nutzen. [7]Der Teilnehmer muss Mitbenutzer über eine erteilte Einwilligung unterrichten. [8]Eine Einwilligung kann jederzeit widerrufen werden.

(2) [1]Haben die Teilnehmer ihre Einwilligung zur Verarbeitung von Standortdaten gegeben, müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen.

(3) [1]Bei Verbindungen zu Anschlüssen, die unter den Notrufnummern 112 oder 110 oder der Rufnummer 124 124 oder 116 117 erreicht werden, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Übermittlung von Standortdaten ausgeschlossen wird.

(4) [1]Die Verarbeitung von Standortdaten nach den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

## § 99 Einzelverbindungsnachweis

(1) [1]Dem Teilnehmer sind die gespeicherten Daten derjenigen Verbindungen, für die er entgeltpflichtig ist, nur dann mitzuteilen, wenn er vor dem maßgeblichen Abrechnungszeitraum in Textform einen Einzelverbindungsnachweis verlangt hat; auf Wunsch dürfen ihm auch die Daten pauschal abgegoltener Verbindungen mitgeteilt werden. [2]Dabei entscheidet der Teilnehmer, ob ihm die von ihm gewählten Rufnummern ungekürzt oder unter Kürzung um die letzten drei Ziffern mitgeteilt werden. [3]Bei Anschlüssen im Haushalt ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber informiert hat und künftige Mitbenutzer unverzüglich darüber informieren wird, dass ihm die Verkehrsdaten zur Erteilung des Nachweises bekannt gegeben werden. [4]Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. [5]Soweit die öffentlich-rechtlichen Religionsgesellschaften für ihren Bereich eigene Mitarbeitervertreterregelungen erlassen haben, findet Satz 4 mit der Maßgabe Anwendung, dass an die Stelle des Betriebsrates oder der Personalvertretung die jeweilige Mitarbeitervertretung tritt. [6]Dem Teilnehmer dürfen darüber hinaus die gespeicherten Daten mitgeteilt werden, wenn er Einwendungen gegen die Höhe der Verbindungsentgelte erhoben hat. [7]Soweit ein Teilnehmer zur vollständigen oder teilweisen Übernahme der Entgelte für Verbindungen verpflichtet ist, die bei seinem Anschluss ankommen, dürfen ihm in dem für ihn bestimmten Einzelverbindungsnachweis die Nummern der Anschlüsse, von denen die Anrufe ausgehen, nur unter Kürzung um die letzten drei Ziffern mitgeteilt werden. [8]Die Sätze 2 und 7 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

(2) [1]Der Einzelverbindungsnachweis nach Absatz 1 Satz 1 darf nicht Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen erkennen lassen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen. [2]Dies gilt nur, soweit die Bundesnetzagentur die angerufenen Anschlüsse in eine Liste aufgenommen hat. [3]Der Beratung im Sinne des Satzes 1 dienen neben den in § 203 Abs. 1 Nr. 4 und 4a des Strafgesetzbuches genannten Personengruppen insbesondere die Telefonseelsorge und die Gesundheitsberatung. [4]Die Bundesnetzagentur nimmt die Inhaber der Anschlüsse auf Antrag in die Liste auf, wenn sie ihre Aufgabenbestimmung nach Satz 1 durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts nachgewiesen haben. [5]Die Liste wird zum Abruf im automatisierten Verfahren bereitgestellt. [6]Der Diensteanbieter hat die Liste quartalsweise abzufragen und Änderungen unverzüglich in seinen Abrechnungsverfahren anzuwenden. [7]Die Sätze 1 bis 6 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

(3) [1]Bei Verwendung einer Kundenkarte muss auch auf der Karte ein deutlicher Hinweis auf die mögliche Mitteilung der gespeicherten Verkehrsdaten ersichtlich sein. [2]Sofern ein solcher Hinweis auf der Karte aus technischen Gründen nicht möglich oder für den Kartenemittenten unzumutbar ist, muss der Teilnehmer eine Erklärung nach Absatz 1 Satz 3 oder Satz 4 abgegeben haben.

## § 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) [1]Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. [2]Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können.

(2) [1]Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber der Telekommunikationsanlage oder seinem Beauftragten das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist. [2]Eventuelle bei der Aufschaltung erstellte Aufzeichnungen sind unverzüglich zu löschen. [3]Das Aufschalten muss den betroffenen Kommunikationsteilnehmern durch ein akustisches oder sonstiges Signal zeitgleich angezeigt und ausdrücklich mitgeteilt werden. [4]Sofern dies technisch nicht möglich ist, muss der betriebliche Datenschutzbeauftragte unverzüglich detailliert über die Verfahren und Umstände jeder einzelnen Maßnahme informiert werden. [5]Diese Informationen sind beim betrieblichen Datenschutzbeauftragten für zwei Jahre aufzubewahren.

(3) [1]Wenn zu dokumentierende tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme eines Telekommunikationsnetzes oder -dienstes vorlie-

gen, insbesondere für eine Leistungserschleichung oder einen Betrug, darf der Diensteanbieter zur Sicherung seines Entgeltanspruchs die Bestandsdaten und Verkehrsdaten verwenden, die erforderlich sind, um die rechtswidrige Inanspruchnahme des Telekommunikationsnetzes oder -dienstes aufzudecken und zu unterbinden. [2]Der Diensteanbieter darf die nach § 96 erhobenen Verkehrsdaten in der Weise verwenden, dass aus dem Gesamtbestand aller Verkehrsdaten, die nicht älter als sechs Monate sind, die Daten derjenigen Verbindungen des Netzes ermittelt werden, für die tatsächliche Anhaltspunkte den Verdacht der rechtswidrigen Inanspruchnahme von Telekommunikationsnetzen und -diensten begründen. [3]Der Diensteanbieter darf aus den Verkehrsdaten und Bestandsdaten nach Satz 1 einen pseudonymisierten Gesamtdatenbestand bilden, der Aufschluss über die von einzelnen Teilnehmern erzielten Umsätze gibt und unter Zugrundelegung geeigneter Kriterien das Auffinden solcher Verbindungen des Netzes ermöglicht, bei denen der Verdacht einer rechtswidrigen Inanspruchnahme besteht. [4]Die Daten anderer Verbindungen sind unverzüglich zu löschen. [5]Die Bundesnetzagentur und der Bundesbeauftragte für den Datenschutz sind über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.

(4) [1]Unter den Voraussetzungen des Absatzes 3 Satz 1 darf der Diensteanbieter im Einzelfall Steuersignale erheben und verwenden, soweit dies zum Aufklären und Unterbinden der dort genannten Handlungen unerlässlich ist. [2]Die Erhebung und Verwendung von anderen Nachrichteninhalten ist unzulässig. [3]Über Einzelmaßnahmen nach Satz 1 ist die Bundesnetzagentur in Kenntnis zu setzen. [4]Die Betroffenen sind zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahmen möglich ist.

## § 101 Mitteilen ankommender Verbindungen

(1) [1]Trägt ein Teilnehmer in einem zu dokumentierenden Verfahren schlüssig vor, dass bei seinem Anschluss bedrohende oder belästigende Anrufe ankommen, hat der Diensteanbieter auf schriftlichen Antrag auch netzübergreifend Auskunft über die Inhaber der Anschlüsse zu erteilen, von denen die Anrufe ausgehen. [2]Die Auskunft darf sich nur auf Anrufe beziehen, die nach Stellung des Antrags durchgeführt werden. [3]Der Diensteanbieter darf die Rufnummern, Namen und Anschriften der Inhaber dieser Anschlüsse sowie Datum und Uhrzeit des Beginns der Verbindungen und der Verbindungsversuche erheben und verwenden sowie diese Daten seinem Teilnehmer mitteilen. [4]Die Sätze 1 und 2 gelten nicht für Diensteanbieter, die ihre Dienste nur den Teilnehmern geschlossener Benutzergruppen anbieten.

(2) [1]Die Bekanntgabe nach Absatz 1 Satz 3 darf nur erfolgen, wenn der Teilnehmer zuvor die Verbindungen nach Datum, Uhrzeit oder anderen geeigneten Kriterien eingrenzt, soweit ein Missbrauch dieses Verfahrens nicht auf andere Weise ausgeschlossen werden kann.

(3) [1]Im Falle einer netzübergreifenden Auskunft sind die an der Verbindung mitwirkenden anderen Diensteanbieter verpflichtet, dem Diensteanbieter des bedrohten oder belästigten Teilnehmers die erforderlichen Auskünfte zu erteilen, sofern sie über diese Daten verfügen.

(4) [1]Der Inhaber des Anschlusses, von dem die festgestellten Verbindungen ausgegangen sind, ist zu unterrichten, dass über diese Auskunft erteilt wurde. [2]Davon kann abgesehen werden, wenn der Antragsteller schriftlich schlüssig vorgetragen hat, dass ihm aus dieser Mitteilung wesentliche Nachteile entstehen können, und diese Nachteile bei Abwägung mit den schutzwürdigen Interessen der Anrufenden als wesentlich schwerwiegender erscheinen. [3]Erhält der Teilnehmer, von dessen Anschluss die als bedrohend oder belästigend bezeichneten Anrufe ausgegangen sind, auf andere Weise Kenntnis von der Auskunftserteilung, so ist er auf Verlangen über die Auskunftserteilung zu unterrichten.

(5) [1]Die Bundesnetzagentur sowie der oder die Bundesbeauftragte für den Datenschutz sind über die Einführung und Änderung des Verfahrens zur Sicherstellung der Absätze 1 bis 4 unverzüglich in Kenntnis zu setzen.

## § 102 Rufnummernanzeige und -unterdrückung

(1) [1]Bietet der Diensteanbieter die Anzeige der Rufnummer der Anrufenden an, so müssen Anrufende und Angerufene die Möglichkeit haben, die Rufnummernanzeige dauernd oder für jeden Anruf einzeln auf einfache Weise und unentgeltlich zu unterdrücken. [2]Angerufene müssen die Möglichkeit haben, eingehende Anrufe, bei denen die Rufnummernanzeige durch den Anrufenden unterdrückt wurde, auf einfache Weise und unentgeltlich abzuweisen.

(2) [1]Abweichend von Absatz 1 Satz 1 dürfen Anrufende bei Werbung mit einem Telefonanruf ihre Rufnummernanzeige nicht unterdrücken oder bei dem Diensteanbieter veranlassen, dass diese unterdrückt wird; der Anrufer hat sicherzustellen, dass dem Angerufenen die dem Anrufer zugeteilte Rufnummer übermittelt wird.

(3) [1]Die Absätze 1 und 2 gelten nicht für Diensteanbieter, die ihre Dienste nur den Teilnehmern geschlossener Benutzergruppen anbieten.

(4) [1]Auf Antrag des Teilnehmers muss der Diensteanbieter Anschlüsse bereitstellen, bei denen die Übermittlung der Rufnummer des Anschlusses, von dem der Anruf ausgeht, an den angerufenen Anschluss unentgeltlich ausgeschlossen ist. [2]Die Anschlüsse sind auf Antrag des Teilnehmers in dem öffentlichen Teilnehmerverzeichnis (§ 104) seines Diensteanbieters zu kennzeichnen. [3]Ist eine Kennzeichnung nach Satz 2 erfolgt, so darf an den so gekennzeichneten Anschluss eine Übermittlung der Rufnummer des Anschlusses, von dem der Anruf ausgeht, erst dann erfolgen, wenn zuvor die Kennzeichnung in der aktualisierten Fassung des Teilnehmerverzeichnisses nicht mehr enthalten ist.

(5) [1]Hat der Teilnehmer die Eintragung in das Teilnehmerverzeichnis nicht nach § 104 beantragt, unterbleibt die Anzeige seiner Rufnummer bei dem angerufenen Anschluss, es sei denn, dass der Teilnehmer die Übermittlung seiner Rufnummer ausdrücklich wünscht.

(6) [1]Wird die Anzeige der Rufnummer von Angerufenen angeboten, so müssen Angerufene die Möglichkeit haben, die Anzeige ihrer Rufnummer beim Anrufenden auf einfache Weise und unentgeltlich zu unterdrücken. [2]Absatz 3 gilt entsprechend.

(7) [1]Die Absätze 1 bis 3 und 6 gelten auch für Anrufe in das Ausland und für

aus dem Ausland kommende Anrufe, soweit sie Anrufende oder Angerufene im Inland betreffen.

(8) [1]Bei Verbindungen zu Anschlüssen, die unter den Notrufnummern 112 oder 110 oder der Rufnummer 124 124 oder 116 117 erreicht werden, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Anzeige von Nummern der Anrufenden ausgeschlossen wird.

## § 103 Automatische Anrufweiterschaltung

[1]Der Diensteanbieter ist verpflichtet, seinen Teilnehmern die Möglichkeit einzuräumen, eine von einem Dritten veranlasste automatische Weiterschaltung auf sein Endgerät auf einfache Weise und unentgeltlich abzustellen, soweit dies technisch möglich ist. [2]Satz 1 gilt nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

## § 104 Teilnehmerverzeichnisse

[1]Teilnehmer können mit ihrem Namen, ihrer Anschrift und zusätzlichen Angaben wie Beruf, Branche und Art des Anschlusses in öffentliche gedruckte oder elektronische Verzeichnisse eingetragen werden, soweit sie dies beantragen. [2]Dabei können die Teilnehmer bestimmen, welche Angaben in den Verzeichnissen veröffentlicht werden sollen. [3]Auf Verlangen des Teilnehmers dürfen Mitbenutzer eingetragen werden, soweit diese damit einverstanden sind.

## § 105 Auskunftserteilung

(1) [1]Über die in Teilnehmerverzeichnissen enthaltenen Rufnummern dürfen Auskünfte unter Beachtung der Beschränkungen des § 104 und der Absätze 2 und 3 erteilt werden.

(2) [1]Die Telefonauskunft über Rufnummern von Teilnehmern darf nur erteilt werden, wenn diese in angemessener Weise darüber informiert worden sind, dass sie der Weitergabe ihrer Rufnummer widersprechen können und von ihrem Widerspruchsrecht keinen Gebrauch gemacht haben. [2]Über Rufnummern hinausgehende Auskünfte über nach § 104 veröffentlichte Daten dürfen nur erteilt werden, wenn der Teilnehmer in eine weitergehende Auskunftserteilung eingewilligt hat.

(3) [1]Die Telefonauskunft von Namen oder Namen und Anschrift eines Teilnehmers, von dem nur die Rufnummer bekannt ist, ist zulässig, wenn der Teilnehmer, der in ein Teilnehmerverzeichnis eingetragen ist, nach einem Hinweis seines Diensteanbieters auf seine Widerspruchsmöglichkeit nicht widersprochen hat.

(4) [1]Ein Widerspruch nach Absatz 2 Satz 1 oder Absatz 3 oder eine Einwilligung nach Absatz 2 Satz 2 sind in den Kundendateien des Diensteanbieters und des Anbieters nach Absatz 1, die den Verzeichnissen zugrunde liegen, unverzüglich

zu vermerken. [2]Sie sind auch von den anderen Diensteanbietern zu beachten, sobald diese in zumutbarer Weise Kenntnis darüber erlangen konnten, dass der Widerspruch oder die Einwilligung in den Verzeichnissen des Diensteanbieters und des Anbieters nach Absatz 1 vermerkt ist.

## § 106 Telegrammdienst

(1) [1]Daten und Belege über die betriebliche Bearbeitung und Zustellung von Telegrammen dürfen gespeichert werden, soweit es zum Nachweis einer ordnungsgemäßen Erbringung der Telegrammdienstleistung nach Maßgabe des mit dem Teilnehmer geschlossenen Vertrags erforderlich ist. [2]Die Daten und Belege sind spätestens nach sechs Monaten vom Diensteanbieter zu löschen.

(2) [1]Daten und Belege über den Inhalt von Telegrammen dürfen über den Zeitpunkt der Zustellung hinaus nur gespeichert werden, soweit der Diensteanbieter nach Maßgabe des mit dem Teilnehmer geschlossenen Vertrags für Übermittlungsfehler einzustehen hat. [2]Bei Inlandstelegrammen sind die Daten und Belege spätestens nach drei Monaten, bei Auslandstelegrammen spätestens nach sechs Monaten vom Diensteanbieter zu löschen.

(3) [1]Die Löschungsfristen beginnen mit dem ersten Tag des Monats, der auf den Monat der Telegrammaufgabe folgt. [2]Die Löschung darf unterbleiben, solange die Verfolgung von Ansprüchen oder eine internationale Vereinbarung eine längere Speicherung erfordert.

## § 107 Nachrichtenübermittlungssysteme mit Zwischenspeicherung

(1) [1]Der Diensteanbieter darf bei Diensten, für deren Durchführung eine Zwischenspeicherung erforderlich ist, Nachrichteninhalte, insbesondere Sprach-, Ton-, Text- und Grafikmitteilungen von Teilnehmern, im Rahmen eines hierauf gerichteten Diensteangebots unter folgenden Voraussetzungen verarbeiten:

1. Die Verarbeitung erfolgt ausschließlich in Telekommunikationsanlagen des zwischenspeichernden Diensteanbieters, es sei denn, die Nachrichteninhalte werden im Auftrag des Teilnehmers oder durch Eingabe des Teilnehmers in Telekommunikationsanlagen anderer Diensteanbieter weitergeleitet.

2. Ausschließlich der Teilnehmer bestimmt durch seine Eingabe Inhalt, Umfang und Art der Verarbeitung.

3. Ausschließlich der Teilnehmer bestimmt, wer Nachrichteninhalte eingeben und darauf zugreifen darf (Zugriffsberechtigter).

4. Der Diensteanbieter darf dem Teilnehmer mitteilen, dass der Empfänger auf die Nachricht zugegriffen hat.

5. Der Diensteanbieter darf Nachrichteninhalte nur entsprechend dem mit dem Teilnehmer geschlossenen Vertrag löschen.

(2) [1]Der Diensteanbieter hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten innerhalb seines Unternehmens oder an Dritte auszuschließen. [2]Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. [3]Soweit es im Hinblick auf den angestrebten Schutzzweck erforderlich ist, sind die Maßnahmen dem jeweiligen Stand der Technik anzupassen.

## Abschnitt 3: Öffentliche Sicherheit

### § 108 Notruf

(1) [1]Wer öffentlich zugängliche Telekommunikationsdienste für das Führen von ausgehenden Inlandsgesprächen zu einer oder mehreren Nummern des nationalen Telefonnummernplanes bereitstellt, hat Vorkehrungen zu treffen, damit Endnutzern unentgeltliche Verbindungen möglich sind, die entweder durch die Wahl der europaeinheitlichen Notrufnummer 112 oder der zusätzlichen nationalen Notrufnummer 110 oder durch das Aussenden entsprechender Signalisierungen eingeleitet werden (Notrufverbindungen). [2]Wer derartige öffentlich zugängliche Telekommunikationsdienste erbringt, den Zugang zu solchen Diensten ermöglicht oder Telekommunikationsnetze betreibt, die für diese Dienste einschließlich der Durchleitung von Anrufen genutzt werden, hat gemäß Satz 4 sicherzustellen oder im notwendigen Umfang daran mitzuwirken, dass Notrufverbindungen unverzüglich zu der örtlich zuständigen Notrufabfragestelle hergestellt werden, und er hat alle erforderlichen Maßnahmen zu treffen, damit Notrufverbindungen jederzeit möglich sind. [3]Die Diensteanbieter nach den Sätzen 1 und 2 haben gemäß Satz 6 sicherzustellen, dass der Notrufabfragestelle auch Folgendes mit der Notrufverbindung übermittelt wird:

1. die Rufnummer des Anschlusses, von dem die Notrufverbindung ausgeht, und

2. die Daten, die zur Ermittlung des Standortes erforderlich sind, von dem die Notrufverbindung ausgeht.

[4]Notrufverbindungen sind vorrangig vor anderen Verbindungen herzustellen, sie stehen vorrangigen Verbindungen nach dem Post- und Telekommunikationssicherstellungsgesetz gleich. [5]Daten, die nach Maßgabe der Rechtsverordnung nach Absatz 3 zur Verfolgung von Missbrauch des Notrufs erforderlich sind,

dürfen auch verzögert an die Notrufabfragestelle übermittelt werden. [6]Die Übermittlung der Daten nach den Sätzen 3 und 5 erfolgt unentgeltlich. [7]Die für Notrufverbindungen entstehenden Kosten trägt jeder Diensteanbieter selbst; die Entgeltlichkeit von Vorleistungen bleibt unberührt.

(2) [1]Im Hinblick auf Notrufverbindungen, die durch sprach- oder hörbehinderte Endnutzer unter Verwendung eines Telefaxgerätes eingeleitet werden, gilt Absatz 1 entsprechend.

(3) [1]Das Bundesministerium für Wirtschaft und Technologie wird ermächtigt, im Einvernehmen mit dem Bundesministerium des Innern und dem Bundesministerium für Arbeit und Soziales durch Rechtsverordnung mit Zustimmung des Bundesrates Regelungen zu treffen

1. zu den Grundsätzen der Festlegung von Einzugsgebieten von Notrufabfragestellen und deren Unterteilungen durch die für den Notruf zuständigen Landes- und Kommunalbehörden sowie zu den Grundsätzen des Abstimmungsverfahrens zwischen diesen Behörden und den betroffenen Teilnehmernetzbetreibern und Mobilfunknetzbetreibern, soweit diese Grundsätze für die Herstellung von Notrufverbindungen erforderlich sind,

2. zur Herstellung von Notrufverbindungen zur jeweils örtlich zuständigen Notrufabfragestelle oder Ersatznotrufabfragestelle,

3. zum Umfang der für Notrufverbindungen zu erbringenden Leistungsmerkmale, einschließlich

   (a) der Übermittlung der Daten nach Absatz 1 Satz 3 und

   (b) zulässiger Abweichungen hinsichtlich der nach Absatz 1 Satz 3 Nummer 1 zu übermittelnden Daten in unausweichlichen technisch bedingten Sonderfällen,

4. zur Bereitstellung und Übermittlung von Daten, die geeignet sind, der Notrufabfragestelle die Verfolgung von Missbrauch des Notrufs zu ermöglichen,

5. zum Herstellen von Notrufverbindungen mittels automatischer Wählgeräte und

6. zu den Aufgaben der Bundesnetzagentur auf den in den Nummern 1 bis 5 aufgeführten Gebieten, insbesondere im Hinblick auf die Festlegung von Kriterien für die Genauigkeit und Zuverlässigkeit der Daten, die zur Ermittlung des Standortes erforderlich sind, von dem die Notrufverbindung ausgeht.

[2]Landesrechtliche Regelungen über Notrufabfragestellen bleiben von den Vorschriften dieses Absatzes insofern unberührt, als sie nicht Verpflichtungen im Sinne von Absatz 1 betreffen.

(4) [1]Die technischen Einzelheiten zu den in Absatz 3 Satz 1 Nummer 1 bis 5 aufgeführten Gegenständen, insbesondere die Kriterien für die Genauigkeit und Zuverlässigkeit der Angaben zu dem Standort, von dem die Notrufverbindung ausgeht, legt die Bundesnetzagentur in einer Technischen Richtlinie fest;

dabei berücksichtigt sie die Vorschriften der Verordnung nach Absatz 3. [2]Die Bundesnetzagentur erstellt die Richtlinie unter Beteiligung

1. der Verbände der durch Absatz 1 Satz 1 und 2 und Absatz 2 betroffenen Diensteanbieter und Betreiber von Telekommunikationsnetzen,

2. der vom Bundesministerium des Innern benannten Vertreter der Betreiber von Notrufabfragestellen und

3. der Hersteller der in den Telekommunikationsnetzen und Notrufabfragestellen eingesetzten technischen Einrichtungen.

[3]Bei den Festlegungen in der Technischen Richtlinie sind internationale Standards zu berücksichtigen; Abweichungen von den Standards sind zu begründen. [4]Die Technische Richtlinie ist von der Bundesnetzagentur auf ihrer Internetseite zu veröffentlichen; die Veröffentlichung hat die Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen. [5]Die Verpflichteten nach Absatz 1 Satz 1 bis 3 und Absatz 2 haben die Anforderungen der Technischen Richtlinie spätestens ein Jahr nach deren Bekanntmachung zu erfüllen, sofern dort für bestimmte Verpflichtungen kein längerer Übergangszeitraum festgelegt ist. [6]Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.

## § 109 Technische Schutzmaßnahmen

(1) [1]Jeder Diensteanbieter hat erforderliche technische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz des Fernmeldegeheimnisses und

2. gegen die Verletzung des Schutzes personenbezogener Daten.

[2]Dabei ist der Stand der Technik zu berücksichtigen.

(2) [1]Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und

2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten.

[2]Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen

von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. [3]Bei Maßnahmen nach Satz 2 ist der Stand der Technik zu berücksichtigen. [4]Wer ein öffentliches Telekommunikationsnetz betreibt, hat Maßnahmen zu treffen, um den ordnungsgemäßen Betrieb seiner Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen. [5]Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. [6]§ 11 Absatz 1 des Bundesdatenschutzgesetzes gilt entsprechend.

(3) [1]Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Beteiligte die Verpflichtungen nach den Absätzen 1 und 2 zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Beteiligten zugeordnet werden können.

(4) [1]Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,

1. welches öffentliche Telekommunikationsnetz betrieben und welche öffentlich zugänglichen Telekommunikationsdienste erbracht werden,

2. von welchen Gefährdungen auszugehen ist und

3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind.

[2]Wer ein öffentliches Telekommunikationsnetz betreibt, hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach der Aufnahme des Netzbetriebs vorzulegen. [3]Wer öffentlich zugängliche Telekommunikationsdienste erbringt, kann nach der Bereitstellung des Telekommunikationsdienstes von der Bundesnetzagentur verpflichtet werden, das Sicherheitskonzept vorzulegen. [4]Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. [5]Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie deren unverzügliche Beseitigung verlangen. [6]Sofern sich die dem Sicherheitskonzept zugrunde liegenden Gegebenheiten ändern, hat der nach Satz 2 oder 3 Verpflichtete das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen. [7]Die Bundesnetzagentur überprüft regelmäßig die Umsetzung des Sicherheitskonzepts. [8]Die Überprüfung soll mindestens alle zwei Jahre erfolgen.

(5) [1]Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die

1. zu beträchtlichen Sicherheitsverletzungen führen oder

2. zu beträchtlichen Sicherheitsverletzungen führen können.

[2]Dies schließt Störungen ein, die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. [3]Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und zu der betroffenen Informationstechnik enthalten. [4]Kommt es zu einer beträchtlichen Sicherheitsverletzung, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. [5]Soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen, leitet die Bundesnetzagentur die eingegangenen Meldungen sowie die Informationen zu den ergriffenen Abhilfemaßnahmen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. [6]Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. [7]Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. [8]§ 8d des BSI-Gesetzes gilt entsprechend. [9]Die Bundesnetzagentur legt der Europäischen Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen vor.

(6) [1]Die Bundesnetzagentur erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach Absatz 4 und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach den Absätzen 1 und 2. [2]Sie gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme. [3]Der Katalog wird von der Bundesnetzagentur veröffentlicht.

(7) [1]Die Bundesnetzagentur kann anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird, ob die Anforderungen nach den Absätzen 1 bis 3 erfüllt sind. [2]Der nach Satz 1 Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bundesnetzagentur zu übermitteln. [3]Er trägt die Kosten dieser Überprüfung.

(8) [1]Über aufgedeckte Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik.

## § 109a Daten- und Informationssicherheit

(1) [1]Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen. [2]Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden, hat der Anbieter des Telekommunikationsdienstes zusätzlich die Betroffenen unverzüglich von dieser Verletzung zu benachrichtigen. [3]In Fällen, in denen in dem Sicherheitskonzept nachgewiesen wurde, dass die von der Verletzung betroffenen personenbezogenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden, ist eine Benachrichtigung nicht erforderlich. [4]Unabhängig von Satz 3 kann die Bundesnetzagentur den Anbieter des Telekommunikationsdienstes unter Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten zu einer Benachrichtigung der Betroffenen verpflichten. [5]Im Übrigen gilt § 42a Satz 6 des Bundesdatenschutzgesetzes entsprechend.

(2) [1]Die Benachrichtigung an die Betroffenen muss mindestens enthalten:

1. die Art der Verletzung des Schutzes personenbezogener Daten,
2. Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind, und
3. Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen.

[2]In der Benachrichtigung an die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat der Anbieter des Telekommunikationsdienstes zusätzlich zu den Angaben nach Satz 1 die Folgen der Verletzung des Schutzes personenbezogener Daten und die beabsichtigten oder ergriffenen Maßnahmen darzulegen.

(3) [1]Die Anbieter der Telekommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, das Angaben zu Folgendem enthält:

1. zu den Umständen der Verletzungen,
2. zu den Auswirkungen der Verletzungen und
3. zu den ergriffenen Abhilfemaßnahmen.

[2]Diese Angaben müssen ausreichend sein, um der Bundesnetzagentur und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Prüfung zu ermöglichen, ob die Bestimmungen der Absätze 1 und 2 eingehalten wurden. [3]Das Verzeichnis enthält nur die zu diesem Zweck erforderlichen Informationen und muss nicht Verletzungen berücksichtigen, die mehr als fünf Jahre zurückliegen.

(4) [1]Werden dem Diensteanbieter nach Absatz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. [2]Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können.

(5) [1]Vorbehaltlich technischer Durchführungsmaßnahmen der Europäischen Kommission nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG kann die Bundesnetzagentur Leitlinien vorgeben bezüglich des Formats, der Verfahrensweise und der Umstände, unter denen eine Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist.

## § 110 Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften

(1) [1]Wer eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, hat

1. ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen,

1a. in Fällen, in denen die Überwachbarkeit nur durch das Zusammenwirken von zwei oder mehreren Telekommunikationsanlagen sichergestellt werden kann, die dazu erforderlichen automatischen Steuerungsmöglichkeiten zur Erfassung und Ausleitung der zu überwachenden Telekommunikation in seiner Telekommunikationsanlage bereitzustellen sowie eine derartige Steuerung zu ermöglichen,

2. der Bundesnetzagentur unverzüglich nach der Betriebsaufnahme

   (a) zu erklären, dass er die Vorkehrungen nach Nummer 1 getroffen hat sowie

   (b) eine im Inland gelegene Stelle zu benennen, die für ihn bestimmte Anordnungen zur Überwachung der Telekommunikation entgegennimmt,

3. der Bundesnetzagentur den unentgeltlichen Nachweis zu erbringen, dass seine technischen Einrichtungen und organisatorischen Vorkehrungen nach Nummer 1 mit den Vorschriften der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 übereinstimmen; dazu hat er unverzüglich, spätestens nach einem Monat nach Betriebsaufnahme,

   (a) der Bundesnetzagentur die Unterlagen zu übersenden, die dort für die Vorbereitung der im Rahmen des Nachweises von der Bundesnetzagentur durchzuführenden Prüfungen erforderlich sind, und

   (b) mit der Bundesnetzagentur einen Prüftermin für die Erbringung dieses Nachweises zu vereinbaren;

bei den für den Nachweis erforderlichen Prüfungen hat er die Bundesnetzagentur zu unterstützen,

4. der Bundesnetzagentur auf deren besondere Aufforderung im begründeten Einzelfall eine erneute unentgeltliche Prüfung seiner technischen und organisatorischen Vorkehrungen zu gestatten sowie

5. die Aufstellung und den Betrieb von Geräten für die Durchführung von Maßnahmen nach den §§ 5 und 8 des Artikel 10-Gesetzes in seinen Räumen zu dulden und Bediensteten der für diese Maßnahmen zuständigen Stelle sowie den Mitgliedern und Mitarbeitern der G 10-Kommission (§ 1 Abs. 2 des Artikel 10-Gesetzes) Zugang zu diesen Geräten zur Erfüllung ihrer gesetzlichen Aufgaben zu gewähren.

[2]Wer öffentlich zugängliche Telekommunikationsdienste erbringt, ohne hierfür eine Telekommunikationsanlage zu betreiben, hat sich bei der Auswahl des Betreibers der dafür genutzten Telekommunikationsanlage zu vergewissern, dass dieser Anordnungen zur Überwachung der Telekommunikation unverzüglich nach Maßgabe der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 umsetzen kann und der Bundesnetzagentur unverzüglich nach Aufnahme seines Dienstes mitzuteilen, welche Telekommunikationsdienste er erbringt, durch wen Überwachungsanordnungen, die seine Teilnehmer betreffen, umgesetzt werden und an welche im Inland gelegene Stelle Anordnungen zur Überwachung der Telekommunikation zu richten sind. [3]Änderungen der den Mitteilungen nach Satz 1 Nr. 2 Buchstabe b und Satz 2 zugrunde liegenden Daten sind der Bundesnetzagentur unverzüglich mitzuteilen. [4]In Fällen, in denen noch keine Vorschriften nach Absatz 3 vorhanden sind, hat der Verpflichtete die technischen Einrichtungen nach Satz 1 Nr. 1 und 1a in Absprache mit der Bundesnetzagentur zu gestalten, die entsprechende Festlegungen im Benehmen mit den berechtigten Stellen trifft. [5]Die Sätze 1 bis 4 gelten nicht, soweit die Rechtsverordnung nach Absatz 2 Ausnahmen für die Telekommunikationsanlage vorsieht. [6]§ 100b Abs. 3 Satz 1 der Strafprozessordnung, § 2 Abs. 1 Satz 3 des Artikel 10-Gesetzes, § 20l Abs. 5 Satz 1 des Bundeskriminalamtgesetzes sowie entsprechende landesgesetzliche Regelungen zur polizeilich-präventiven Telekommunikationsüberwachung bleiben unberührt.

(2) [1]Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates

1. Regelungen zu treffen

   (a) über die grundlegenden technischen Anforderungen und die organisatorischen Eckpunkte für die Umsetzung von Überwachungsmaßnahmen und die Erteilung von Auskünften einschließlich der Umsetzung von Überwachungsmaßnahmen und der Erteilung von Auskünften durch einen von dem Verpflichteten beauftragten Erfüllungsgehilfen,

   (b) über den Regelungsrahmen für die Technische Richtlinie nach Absatz 3,

   (c) für den Nachweis nach Absatz 1 Satz 1 Nr. 3 und 4 und

   (d) für die nähere Ausgestaltung der Duldungsverpflichtung nach Absatz 1 Satz 1 Nr. 5 sowie

2. zu bestimmen,

   (a) in welchen Fällen und unter welchen Bedingungen vorübergehend auf die Einhaltung bestimmter technischer Vorgaben verzichtet werden kann,

   (b) dass die Bundesnetzagentur aus technischen Gründen Ausnahmen von der Erfüllung einzelner technischer Anforderungen zulassen kann und

   (c) bei welchen Telekommunikationsanlagen und damit erbrachten Diensteangeboten aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit abweichend von Absatz 1 Satz 1 Nr. 1 keine technischen Einrichtungen vorgehalten und keine organisatorischen Vorkehrungen getroffen werden müssen.

(3) [1]Die Bundesnetzagentur legt technische Einzelheiten, die zur Sicherstellung einer vollständigen Erfassung der zu überwachenden Telekommunikation und zur Auskunftserteilung sowie zur Gestaltung des Übergabepunktes zu den berechtigten Stellen erforderlich sind, in einer im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller zu erstellenden Technischen Richtlinie fest. [2]Dabei sind internationale technische Standards zu berücksichtigen; Abweichungen von den Standards sind zu begründen. [3]Die Technische Richtlinie ist von der Bundesnetzagentur auf ihrer Internetseite zu veröffentlichen; die Veröffentlichung hat die Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen.

(4) [1]Wer technische Einrichtungen zur Umsetzung von Überwachungsmaßnahmen herstellt oder vertreibt, kann von der Bundesnetzagentur verlangen, dass sie diese Einrichtungen im Rahmen einer Typmusterprüfung im Zusammenwirken mit bestimmten Telekommunikationsanlagen daraufhin prüft, ob die rechtlichen und technischen Vorschriften der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 erfüllt werden. [2]Die Bundesnetzagentur kann nach pflichtgemäßem Ermessen vorübergehend Abweichungen von den technischen Vorgaben zulassen, sofern die Umsetzung von Überwachungsmaßnahmen grundsätzlich sichergestellt ist und sich ein nur unwesentlicher Anpassungsbedarf bei den Einrichtungen der berechtigten Stellen ergibt. [3]Die Bundesnetzagentur hat dem Hersteller oder Vertreiber das Prüfergebnis schriftlich mitzuteilen. [4]Die Prüfergebnisse werden von der Bundesnetzagentur bei dem Nachweis der Übereinstimmung der technischen Einrichtungen mit den anzuwendenden technischen Vorschriften beachtet, den der Verpflichtete nach Absatz 1 Satz 1 Nr. 3 oder 4 zu erbringen hat. [5]Die vom Bundesministerium für Wirtschaft und Technologie vor Inkrafttreten dieser Vorschrift ausgesprochenen Zustimmungen zu den von Herstellern vorgestellten Rahmenkonzepten gelten als Mitteilungen im Sinne des Satzes 3.

(5) [1]Wer nach Absatz 1 in Verbindung mit der Rechtsverordnung nach Absatz 2 verpflichtet ist, Vorkehrungen zu treffen, hat die Anforderungen der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3 spätestens ein Jahr nach deren Bekanntmachung zu erfüllen, sofern dort für bestimmte Verpflichtungen kein längerer Zeitraum festgelegt ist. [2]Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen für bereits vom Verpflichteten angebotene Telekommunikationsdienste müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.

[3]Stellt sich bei dem Nachweis nach Absatz 1 Satz 1 Nr. 3 oder einer erneuten Prüfung nach Absatz 1 Satz 1 Nr. 4 ein Mangel bei den von dem Verpflichteten getroffenen technischen oder organisatorischen Vorkehrungen heraus, hat er diesen Mangel nach Vorgaben der Bundesnetzagentur in angemessener Frist zu beseitigen; stellt sich im Betrieb, insbesondere anlässlich durchzuführender Überwachungsmaßnahmen, ein Mangel heraus, hat er diesen unverzüglich zu beseitigen. [4]Sofern für die technische Einrichtung eine Typmusterprüfung nach Absatz 4 durchgeführt worden ist und dabei Fristen für die Beseitigung von Mängeln festgelegt worden sind, hat die Bundesnetzagentur diese Fristen bei ihren Vorgaben zur Mängelbeseitigung nach Satz 3 zu berücksichtigen.

(6) [1]Jeder Betreiber einer Telekommunikationsanlage, der anderen im Rahmen seines Angebotes für die Öffentlichkeit Netzabschlusspunkte seiner Telekommunikationsanlage überlässt, ist verpflichtet, den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf deren Anforderung Netzabschlusspunkte für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen unverzüglich und vorrangig bereitzustellen. [2]Die technische Ausgestaltung derartiger Netzabschlusspunkte kann in einer Rechtsverordnung nach Absatz 2 geregelt werden. [3]Für die Bereitstellung und Nutzung gelten mit Ausnahme besonderer Tarife oder Zuschläge für vorrangige oder vorzeitige Bereitstellung oder Entstörung die jeweils für die Allgemeinheit anzuwendenden Tarife. [4]Besondere vertraglich vereinbarte Rabatte bleiben von Satz 3 unberührt.

(7) [1]Telekommunikationsanlagen, die von den gesetzlich berechtigten Stellen betrieben werden und mittels derer in das Fernmeldegeheimnis oder in den Netzbetrieb eingegriffen werden soll, sind im Einvernehmen mit der Bundesnetzagentur technisch zu gestalten. [2]Die Bundesnetzagentur hat sich zu der technischen Gestaltung innerhalb angemessener Frist zu äußern.

(8) [1](weggefallen)

(9) [1](weggefallen)

## § 111 Daten für Auskunftsersuchen der Sicherheitsbehörden

(1) [1]Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie

6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. [2]Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. [3]Bei im Voraus bezahlten Mobilfunkdiensten ist die Richtigkeit der nach Satz 1 erhobenen Daten vor der Freischaltung zu überprüfen durch

1. Vorlage eines Ausweises im Sinne des § 2 Absatz 1 des Personalausweisgesetzes,

2. Vorlage eines Passes im Sinne des § 1 Absatz 2 des Passgesetzes,

3. Vorlage eines sonstigen gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, wozu insbesondere auch ein nach ausländerrechtlichen Bestimmungen anerkannter oder zugelassener Pass, Personalausweis oder Pass- oder AusweiserSatz zählt,

4. Vorlage eines Aufenthaltstitels,

5. Vorlage eines Ankunftsnachweises nach § 63a Absatz 1 des Asylgesetzes oder einer Bescheinigung über die Aufenthaltsgestattung nach § 63 Absatz 1 des Asylgesetzes,

6. Vorlage einer Bescheinigung über die Aussetzung der Abschiebung nach § 60a Absatz 4 des Aufenthaltsgesetzes oder

7. Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den darin enthaltenen Daten, sofern es sich bei dem Anschlussinhaber um eine juristische Person oder Personengesellschaft handelt,

soweit die Daten in den vorgelegten Dokumenten oder eingesehenen Registern oder Verzeichnissen enthalten sind. [4]Die Überprüfung kann auch durch andere geeignete Verfahren erfolgen; die Bundesnetzagentur legt nach Anhörung der betroffenen Kreise durch Verfügung im Amtsblatt fest, welche anderen Verfahren zur Überprüfung geeignet sind, wobei jeweils zum Zwecke der Identifikation vor Freischaltung der vertraglich vereinbarten Mobilfunkdienstleistung ein Dokument im Sinne des Satzes 3 genutzt werden muss. [5]Bei der Überprüfung ist die Art des eingesetzten Verfahrens zu speichern; bei Überprüfung mittels eines Dokumentes im Sinne des Satzes 3 Nummer 1 bis 6 sind ferner Angaben zu Art, Nummer und ausstellender Stelle zu speichern. [6]Für die Identifizierung anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes gilt § 8 Absatz 1 Satz 6 des Geldwäschegesetzes entsprechend. [7]Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

(2) [1]Die Verpflichtung zur unverzüglichen Speicherung nach Absatz 1 Satz 1 gilt hinsichtlich der Daten nach Absatz 1 Satz 1 Nummer 1 und 2 entsprechend

für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Absatz 1 Satz 1 Nummer 1 und 2 erhebt, wobei an die Stelle der Daten nach Absatz 1 Satz 1 Nummer 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Absatz 1 Satz 1 Nummer 2 der Inhaber des elektronischen Postfachs tritt.

(3) [1]Wird dem Verpflichteten nach Absatz 1 Satz 1 oder Absatz 2 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen. [2]In diesem Zusammenhang hat der nach Absatz 1 Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist.

(4) [1]Bedient sich ein Diensteanbieter zur Erhebung der Daten nach Absatz 1 Satz 1 und Absatz 2 eines Dritten, bleibt er für die Erfüllung der Pflichten nach Absatz 1 Satz 1 und Absatz 2 verantwortlich. [2]Werden dem Dritten im Rahmen des üblichen Geschäftsablaufes Änderungen der Daten nach Absatz 1 Satz 1 und Absatz 2 bekannt, hat er diese dem Diensteanbieter unverzüglich zu übermitteln.

(5) [1]Die Daten nach den Absätzen 1 und 2 sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(6) [1]Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

## § 112 Automatisiertes Auskunftsverfahren

(1) [1]Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat die nach § 111 Absatz 1 Satz 1, Absatz 2, 3 und 4 erhobenen Daten unverzüglich in Kundendateien zu speichern, in die auch Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere Anbieter von Telekommunikationsdiensten vergeben werden, sowie bei portierten Rufnummern die aktuelle Portierungskennung aufzunehmen sind. [2]Der Verpflichtete kann auch eine andere Stelle nach Maßgabe des § 11 des Bundesdatenschutzgesetzes beauftragen, die Kundendateien zu führen. [3]Für die Berichtigung und Löschung der in den Kundendateien gespeicherten Daten gilt § 111 Absatz 3 und 5 entsprechend. [4]In Fällen portierter Rufnummern sind die Rufnummer und die zugehörige Portierungskennung erst nach Ablauf des Jahres zu löschen, das dem Zeitpunkt folgt, zu dem die Rufnummer wieder an den Netzbetreiber zurückgegeben wurde, dem sie ursprünglich zugeteilt worden war. [5]Der Verpflichtete hat zu gewährleisten, dass

1. die Bundesnetzagentur jederzeit Daten aus den Kundendateien automatisiert im Inland abrufen kann,
2. der Abruf von Daten unter Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichenfunktion erfolgen kann.

[6]Der Verpflichtete und sein Beauftragter haben durch technische und organisatorische Maßnahmen sicherzustellen, dass ihnen Abrufe nicht zur Kenntnis gelangen können. [7]Die Bundesnetzagentur darf Daten aus den Kundendateien nur abrufen, soweit die Kenntnis der Daten erforderlich ist

1. für die Verfolgung von Ordnungswidrigkeiten nach diesem Gesetz oder nach dem Gesetz gegen den unlauteren Wettbewerb,

2. für die Erledigung von Auskunftsersuchen der in Absatz 2 genannten Stellen.

[8]Die ersuchende Stelle prüft unverzüglich, inwieweit sie die als Antwort übermittelten Daten benötigt, nicht benötigte Daten löscht sie unverzüglich; dies gilt auch für die Bundesnetzagentur für den Abruf von Daten nach Satz 7 Nummer 1.

(2) [1]Auskünfte aus den Kundendateien nach Absatz 1 werden

1. den Gerichten und Strafverfolgungsbehörden,

2. den Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr,

3. dem Zollkriminalamt und den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 23a des Zollfahndungsdienstgesetzes,

4. den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst,

5. den Notrufabfragestellen nach § 108 sowie der Abfragestelle für die Rufnummer 124 124,

6. der Bundesanstalt für Finanzdienstleistungsaufsicht sowie

7. den Behörden der Zollverwaltung für die in § 2 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen

nach Absatz 4 jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen an die Bundesnetzagentur im automatisierten Verfahren vorgelegt werden.

(3) [1]Das Bundesministerium für Wirtschaft und Technologie wird ermächtigt, im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium des Innern, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen sowie dem Bundesministerium der Verteidigung eine Rechtsverordnung mit Zustimmung des Bundesrates zu erlassen, in der geregelt werden

1. die wesentlichen Anforderungen an die technischen Verfahren

   (a) zur Übermittlung der Ersuchen an die Bundesnetzagentur,

   (b) zum Abruf der Daten durch die Bundesnetzagentur von den Verpflichteten einschließlich der für die Abfrage zu verwendenden Datenarten und

   (c) zur Übermittlung der Ergebnisse des Abrufs von der Bundesnetzagentur an die ersuchenden Stellen,

2. die zu beachtenden Sicherheitsanforderungen,

3. für Abrufe mit unvollständigen Abfragedaten und für die Suche mittels einer Ähnlichenfunktion

   (a) die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung der gesuchten Person,

   (b) die Zeichen, die in der Abfrage verwendet werden dürfen,

   (c) Anforderungen an den EinSatz sprachwissenschaftlicher Verfahren, die gewährleisten, dass unterschiedliche Schreibweisen eines Personen-, Straßen- oder Ortsnamens sowie Abweichungen, die sich aus der Vertauschung, Auslassung oder Hinzufügung von Namensbestandteilen ergeben, in die Suche und das Suchergebnis einbezogen werden,

   (d) die zulässige Menge der an die Bundesnetzagentur zu übermittelnden Antwortdatensätze sowie

4. wer abweichend von Absatz 1 Satz 1 aus Gründen der Verhältnismäßigkeit keine Kundendateien für das automatisierte Auskunftsverfahren vorhalten muss; in diesen Fällen gilt § 111 Absatz 1 Satz 7 entsprechend.

[2]Im Übrigen können in der Verordnung auch Einschränkungen der Abfragemöglichkeit für die in Absatz 2 Nr. 5 bis 7 genannten Stellen auf den für diese Stellen erforderlichen Umfang geregelt werden. [3]Die technischen Einzelheiten des automatisierten Abrufverfahrens gibt die Bundesnetzagentur in einer unter Beteiligung der betroffenen Verbände und der berechtigten Stellen zu erarbeitenden Technischen Richtlinie vor, die bei Bedarf an den Stand der Technik anzupassen und von der Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen ist. [4]Der Verpflichtete nach Absatz 1 und die berechtigten Stellen haben die Anforderungen der Technischen Richtlinie spätestens ein Jahr nach deren Bekanntmachung zu erfüllen. [5]Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.

(4) [1]Auf Ersuchen der in Absatz 2 genannten Stellen hat die Bundesnetzagentur die entsprechenden Datensätze aus den Kundendateien nach Absatz 1 abzurufen und an die ersuchende Stelle zu übermitteln. [2]Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlass besteht. [3]Die Verantwortung für die Zulässigkeit der Übermittlung tragen

1. in den Fällen des Absatzes 1 Satz 7 Nummer 1 die Bundesnetzagentur und

2. in den Fällen des Absatzes 1 Satz 7 Nummer 2 die in Absatz 2 genannten Stellen.

[4]Die Bundesnetzagentur protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum. [5]Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig. [6]Die Protokolldaten sind nach einem Jahr zu löschen.

(5) [1]Der Verpflichtete nach Absatz 1 hat alle technischen Vorkehrungen in seinem Verantwortungsbereich auf seine Kosten zu treffen, die für die Erteilung der Auskünfte nach dieser Vorschrift erforderlich sind. [2]Dazu gehören auch die Anschaffung der zur Sicherstellung der Vertraulichkeit und des Schutzes vor unberechtigten Zugriffen erforderlichen Geräte, die Einrichtung eines geeigneten Telekommunikationsanschlusses und die Teilnahme an dem geschlossenen Benutzersystem sowie die laufende Bereitstellung dieser Vorkehrungen nach Maßgaben der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3. [3]Eine Entschädigung für im automatisierten Verfahren erteilte Auskünfte wird den Verpflichteten nicht gewährt.

## § 113 Manuelles Auskunftsverfahren

(1) [1]Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, darf nach Maßgabe des Absatzes 2 die nach den §§ 95 und 111 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. [2]Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. [3]Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. [4]Für die Auskunftserteilung nach Satz 3 sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) [1]Die Auskunft darf nur erteilt werden, soweit eine in Absatz 3 genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 genannten Stellen unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt; an andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. [2]Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. [3]In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. [4]Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die in Absatz 3 genannten Stellen.

(3) [1]Stellen im Sinne des Absatzes 1 sind

1. die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden;
2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden;
3. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst.

(4) [1]Derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die zu beauskunftenden Daten unverzüglich und vollständig

zu übermitteln. [2]Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(5) [1]Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. [2]Wer mehr als 100 000 Kunden hat, hat für die Entgegennahme der Auskunftsverlangen sowie für die Erteilung der zugehörigen Auskünfte eine gesicherte elektronische Schnittstelle nach Maßgabe der Technischen Richtlinie nach § 110 Absatz 3 bereitzuhalten, durch die auch die gegen die Kenntnisnahme der Daten durch Unbefugte gesicherte Übertragung gewährleistet ist. [3]Dabei ist dafür Sorge zu tragen, dass jedes Auskunftsverlangen durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird.

## § 113a Verpflichtete; Entschädigung

(1) [1]Die Verpflichtungen zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit nach den §§ 113b bis 113g beziehen sich auf Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer. [2]Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, aber nicht alle der nach Maßgabe der §§ 113b bis 113g zu speichernden Daten selbst erzeugt oder verarbeitet, hat

1. sicherzustellen, dass die nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten oder verarbeiteten Daten gemäß § 113b Absatz 1 gespeichert werden, und
2. der Bundesnetzagentur auf deren Verlangen unverzüglich mitzuteilen, wer diese Daten speichert.

(2) [1]Für notwendige Aufwendungen, die den Verpflichteten durch die Umsetzung der Vorgaben aus den §§ 113b, 113d bis 113g entstehen, ist eine angemessene Entschädigung zu zahlen, soweit dies zur Abwendung oder zum Ausgleich unbilliger Härten geboten erscheint. [2]Für die Bemessung der Entschädigung sind die tatsächlich entstandenen Kosten maßgebend. [3]Über Anträge auf Entschädigung entscheidet die Bundesnetzagentur.

## § 113b Pflichten zur Speicherung von Verkehrsdaten

(1) [1]Die in § 113a Absatz 1 Genannten sind verpflichtet, Daten wie folgt im Inland zu speichern:

1. Daten nach den Absätzen 2 und 3 für zehn Wochen,
2. Standortdaten nach Absatz 4 für vier Wochen.

(2) [1]Die Erbringer öffentlich zugänglicher Telefondienste speichern

1. die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

2. Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone,

3. Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,

4. im Fall mobiler Telefondienste ferner

   (a) die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,

   (b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,

   (c) Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,

5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen. [2]Satz 1 gilt entsprechend

   (a) bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht;

   (b) für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Erbringer öffentlich zugänglicher Telefondienste die in Satz 1 genannten Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert.

(3) [1]Die Erbringer öffentlich zugänglicher Internetzugangsdienste speichern

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,

3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone.

(4) [1]Im Fall der Nutzung mobiler Telefondienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. [2]Bei öffentlich zugänglichen Internetzugangsdiensten ist im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. [3]Zusätzlich

sind die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben.

(5) [1]Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(6) [1]Daten, die den in § 99 Absatz 2 genannten Verbindungen zugrunde liegen, dürfen auf Grund dieser Vorschrift nicht gespeichert werden. [2]Dies gilt entsprechend für Telefonverbindungen, die von den in § 99 Absatz 2 genannten Stellen ausgehen. [3]§ 99 Absatz 2 Satz 2 bis 7 gilt entsprechend.

(7) [1]Die Speicherung der Daten hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(8) [1]Der nach § 113a Absatz 1 Verpflichtete hat die auf Grund des Absatzes 1 gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach Absatz 1, irreversibel zu löschen oder die irreversible Löschung sicherzustellen.

## § 113c Verwendung der Daten

(1) [1]Die auf Grund des § 113b gespeicherten Daten dürfen

1. an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt;

2. an eine Gefahrenabwehrbehörde der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt;

3. durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 113 Absatz 1 Satz 3 verwendet werden.

(2) [1]Für andere Zwecke als die in Absatz 1 genannten dürfen die auf Grund des § 113b gespeicherten Daten von den nach § 113a Absatz 1 Verpflichteten nicht verwendet werden.

(3) [1]Die Übermittlung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 110 Absatz 2 und der Technischen Richtlinie nach § 110 Absatz 3. [2]Die Daten sind so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b gespeichert waren. [3]Nach Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

## § 113d Gewährleistung der Sicherheit der Daten

[1]Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die auf Grund der Speicherpflicht nach § 113b Absatz 1 gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. [2]Die Maßnahmen umfassen insbesondere

1. den EinSatz eines besonders sicheren Verschlüsselungsverfahrens,
2. die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen,
3. die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet auf vom Internet entkoppelten Datenverarbeitungssystemen,
4. die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf Personen, die durch den Verpflichteten besonders ermächtigt sind, und
5. die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Verpflichteten besonders ermächtigt worden sind.

## § 113e Protokollierung

(1) [1]Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der auf Grund der Speicherpflicht nach § 113b Absatz 1 gespeicherten Daten protokolliert wird. [2]Zu protokollieren sind

1. der Zeitpunkt des Zugriffs,
2. die auf die Daten zugreifenden Personen,
3. Zweck und Art des Zugriffs.

(2) [1]Für andere Zwecke als die der Datenschutzkontrolle dürfen die Protokolldaten nicht verwendet werden.

(3) [1]Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die Protokolldaten nach einem Jahr gelöscht werden.

## § 113f Anforderungskatalog

(1) [1]Bei der Umsetzung der Verpflichtungen gemäß den §§ 113b bis 113e ist ein besonders hoher Standard der Datensicherheit und Datenqualität zu gewährleisten. [2]Die Einhaltung dieses Standards wird vermutet, wenn alle Anforderungen

des Katalogs der technischen Vorkehrungen und sonstigen Maßnahmen erfüllt werden, den die Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt.

(2) [1]Die Bundesnetzagentur überprüft fortlaufend die im Katalog nach Absatz 1 Satz 2 enthaltenen Anforderungen; hierbei berücksichtigt sie den Stand der Technik und der Fachdiskussion. [2]Stellt die Bundesnetzagentur Änderungsbedarf fest, ist der Katalog im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unverzüglich anzupassen.

(3) [1]§ 109 Absatz 6 Satz 2 und 3 gilt entsprechend. [2]§ 109 Absatz 7 gilt mit der Maßgabe, dass an die Stelle der Anforderungen nach § 109 Absatz 1 bis 3 die Anforderungen nach Absatz 1 Satz 1, § 113b Absatz 7 und 8, § 113d und nach § 113e Absatz 1 und 3 treten.

## § 113g Sicherheitskonzept

(1) [1]Der nach § 113a Absatz 1 Verpflichtete hat in das Sicherheitskonzept nach § 109 Absatz 4 zusätzlich aufzunehmen,

1. welche Systeme zur Erfüllung der Verpflichtungen aus den §§ 113b bis 113e betrieben werden,
2. von welchen Gefährdungen für diese Systeme auszugehen ist und
3. welche technischen Vorkehrungen oder sonstigen Maßnahmen getroffen oder geplant sind, um diesen Gefährdungen entgegenzuwirken und die Verpflichtungen aus den §§ 113b bis 113e zu erfüllen.

(2) [1]Der nach § 113a Absatz 1 Verpflichtete hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach dem Beginn der Speicherung nach § 113b und unverzüglich bei jeder Änderung des Konzepts vorzulegen. [2]Bleibt das Sicherheitskonzept unverändert, hat der nach § 113a Absatz 1 Verpflichtete dies gegenüber der Bundesnetzagentur im Abstand von jeweils zwei Jahren schriftlich zu erklären.

## § 114 Auskunftsersuchen des Bundesnachrichtendienstes

(1) [1]Wer öffentlich zugängliche Telekommunikationsdienste erbringt oder Übertragungswege betreibt, die für öffentlich zugängliche Telekommunikationsdienste genutzt werden, hat dem Bundesministerium für Wirtschaft und Technologie auf Anfrage entgeltfrei Auskünfte über die Strukturen der Telekommunikationsdienste und -netze sowie bevorstehende Änderungen zu erteilen. [2]Einzelne Telekommunikationsvorgänge und Bestandsdaten von Teilnehmern dürfen nicht Gegenstand einer Auskunft nach dieser Vorschrift sein.

(2) [1]Anfragen nach Absatz 1 sind nur zulässig, wenn ein entsprechendes Ersuchen des Bundesnachrichtendienstes vorliegt und soweit die Auskunft zur Erfüllung der Aufgaben nach den §§ 5 und 8 des Artikel 10-Gesetzes erforderlich ist. [2]Die Verwendung einer nach dieser Vorschrift erlangten Auskunft zu anderen Zwecken ist ausgeschlossen.

## § 115 Kontrolle und Durchsetzung von Verpflichtungen

(1) [1]Die Bundesnetzagentur kann Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Vorschriften des Teils 7 und der auf Grund dieses Teils ergangenen Rechtsverordnungen sowie der jeweils anzuwendenden Technischen Richtlinien sicherzustellen. [2]Der Verpflichtete muss auf Anforderung der Bundesnetzagentur die hierzu erforderlichen Auskünfte erteilen. [3]Die Bundesnetzagentur ist zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten zu betreten und zu besichtigen.

(2) [1]Die Bundesnetzagentur kann nach Maßgabe des Verwaltungsvollstreckungsgesetzes Zwangsgelder wie folgt festsetzen:

1. bis zu 500 000 Euro zur Durchsetzung der Verpflichtungen nach § 108 Abs. 1, § 110 Abs. 1, 5 oder Abs. 6, einer Rechtsverordnung nach § 108 Absatz 3, einer Rechtsverordnung nach § 110 Abs. 2, einer Rechtsverordnung nach § 112 Abs. 3 Satz 1, der Technischen Richtlinie nach § 108 Absatz 4, der Technischen Richtlinie nach § 110 Abs. 3 oder der Technischen Richtlinie nach § 112 Abs. 3 Satz 3,

2. bis zu 100 000 Euro zur Durchsetzung der Verpflichtungen nach den §§ 109, 109a, 112 Absatz 1, 3 Satz 4, Absatz 5 Satz 1 und 2, § 113 Absatz 5 Satz 2 und 3 oder § 114 Absatz 1 und

3. bis zu 20 000 Euro zur Durchsetzung der Verpflichtungen nach § 111 Absatz 1, 4 und 5 oder § 113 Absatz 4 und 5 Satz 1.

[2]Bei wiederholten Verstößen gegen § 111 Absatz 1 bis 5, § 112 Abs. 1, 3 Satz 4, Abs. 5 Satz 1 und 2 oder § 113 Absatz 4 und 5 Satz 1 kann die Tätigkeit des Verpflichteten durch Anordnung der Bundesnetzagentur dahin gehend eingeschränkt werden, dass der Kundenstamm bis zur Erfüllung der sich aus diesen Vorschriften ergebenden Verpflichtungen außer durch Vertragsablauf oder Kündigung nicht verändert werden darf.

(3) [1]Darüber hinaus kann die Bundesnetzagentur bei Nichterfüllung von Verpflichtungen des Teils 7 den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen.

(4) [1]Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden, tritt bei den Unternehmen an die Stelle der Kontrolle nach § 38 des Bundesdatenschutzgesetzes eine Kontrolle durch den Bundesbeauftragten

für den Datenschutz entsprechend den §§ 21 und 24 bis 26 Abs. 1 bis 4 des Bundesdatenschutzgesetzes. [2]Der Bundesbeauftragte für den Datenschutz richtet seine Beanstandungen an die Bundesnetzagentur und übermittelt dieser nach pflichtgemäßem Ermessen weitere Ergebnisse seiner Kontrolle.

(5) [1]Das Fernmeldegeheimnis des Artikels 10 des Grundgesetzes wird eingeschränkt, soweit dies die Kontrollen nach Absatz 1 oder 4 erfordern.

# §§ 201-206 Strafgesetzbuch (StGB)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Strafgesetzbuch |
| **Amtliche Abkürzung:** | StGB |
| **Ausfertigung:** | Neugefasst durch Bekanntmachung vom 13.11.1998, BGBl. I S. 3322 |
| **Inkrafttreten:** | 01.01.1872 |
| **Letzte Änderung:** | 26.07.2016, BGBl. I S. 1818 |

## Inhaltsübersicht


| | | |
|---|---|---|
| **Fünfzehnter Abschnitt: Verletzung des persönlichen Lebens- und Geheimbereichs** | | **192** |
| § 201 | Verletzung der Vertraulichkeit des Wortes | 192 |
| § 201a | Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen | 192 |
| § 202 | Verletzung des Briefgeheimnisses | 193 |
| § 202a | Ausspähen von Daten | 194 |
| § 202b | Abfangen von Daten | 194 |
| § 202c | Vorbereiten des Ausspähens und Abfangens von Daten | 194 |
| § 202d | Datenhehlerei | 195 |
| § 203 | Verletzung von Privatgeheimnissen | 195 |
| § 204 | Verwertung fremder Geheimnisse | 197 |
| § 205 | Strafantrag | 197 |
| § 206 | Verletzung des Post- oder Fernmeldegeheimnisses | 197 |
| § 207 | (weggefallen) | 198 |
| § 208 | (weggefallen) | 198 |
| § 209 | (weggefallen) | 198 |
| § 210 | (weggefallen) | 198 |

# Fünfzehnter Abschnitt: Verletzung des persönlichen Lebens- und Geheimbereichs

## § 201 Verletzung der Vertraulichkeit des Wortes

(1) [1]Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) [1]Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

[2]Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. 3Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

(3) [1]Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter die Vertraulichkeit des Wortes verletzt (Absätze 1 und 2).

(4) [1]Der Versuch ist strafbar.

(5) [1]Die Tonträger und Abhörgeräte, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. [2]§ 74a ist anzuwenden.

## § 201a Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

(1) [1]Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,

2. eine Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt, unbefugt herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,

3. eine durch eine Tat nach den Nummern 1 oder 2 hergestellte Bildaufnahme gebraucht oder einer dritten Person zugänglich macht oder

4. eine befugt hergestellte Bildaufnahme der in den Nummern 1 oder 2 bezeichneten Art wissentlich unbefugt einer dritten Person zugänglich macht und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt.

(2) [1]Ebenso wird bestraft, wer unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich macht.

(3) [1]Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer eine Bildaufnahme, die die Nacktheit einer anderen Person unter achtzehn Jahren zum Gegenstand hat,

1. herstellt oder anbietet, um sie einer dritten Person gegen Entgelt zu verschaffen, oder

2. sich oder einer dritten Person gegen Entgelt verschafft.

(4) [1]Absatz 1 Nummer 2, auch in Verbindung mit Absatz 1 Nummer 3 oder Nummer 4, Absatz 2 und 3 gelten nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen.

(5) [1]Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. [2]§ 74a ist anzuwenden.

## § 202 Verletzung des Briefgeheimnisses

(1) [1]Wer unbefugt

1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder

2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.

(2) [1]Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.

(3) [1]Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

## § 202a Ausspähen von Daten

(1) [1]Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) [1]Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

## § 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

## § 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) [1]Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) [1]§ 149 Abs. 2 und 3 gilt entsprechend.

## § 202d Datenhehlerei

(1) [1]Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) [1]Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) [1]Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. [2]Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie

2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

## § 203 Verletzung von Privatgeheimnissen

(1) [1]Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,

3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) [1]Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,

2. für den öffentlichen Dienst besonders Verpflichteten,

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,

5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. [2]Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) [1]Die Absätze 1 und 2 gelten entsprechend, wenn ein Beauftragter für den Datenschutz unbefugt ein fremdes Geheimnis im Sinne dieser Vorschriften offenbart, das einem in den Absätzen 1 und 2 Genannten in dessen beruflicher Eigenschaft anvertraut worden oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt hat.

(3) [1]Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. [2]Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. [3]Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlaß erlangt hat. [4]Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt

offenbart. [5]Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

## § 204 Verwertung fremder Geheimnisse

(1) [1]Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) [1]§ 203 Abs. 4 gilt entsprechend.

## § 205 Strafantrag

(1) [1]In den Fällen des § 201 Abs. 1 und 2 und der §§ 202, 203 und 204 wird die Tat nur auf Antrag verfolgt. [2]Dies gilt auch in den Fällen der §§ 201a, 202a, 202b und 202d, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

(2) [1]Stirbt der Verletzte, so geht das Antragsrecht nach § 77 Abs. 2 auf die Angehörigen über; dies gilt nicht in den Fällen der §§ 202a, 202b und 202d. [2]Gehört das Geheimnis nicht zum persönlichen Lebensbereich des Verletzten, so geht das Antragsrecht bei Straftaten nach den §§ 203 und 204 auf die Erben über. [3]Offenbart oder verwertet der Täter in den Fällen der §§ 203 und 204 das Geheimnis nach dem Tod des Betroffenen, so gelten die Sätze 1 und 2 sinngemäß.

## § 206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) [1]Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) [1]Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) [1]Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,

2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) [1]Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) [1]Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. [2]Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war.[3]Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

## § 207 (weggefallen)

## § 208 (weggefallen)

## § 209 (weggefallen)

## § 210 (weggefallen)

# § 23 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie |
| **Amtliche Abkürzung:** | keine - gängige Abkürzung: KunstUrhG |
| **Ausfertigung:** | 09.01.1907, RGBl. S. 7 |
| **Inkrafttreten:** | 01.07.1907 |
| **Letzte Änderung:** | 16.02.2001, BGBl. I S. 266 |

## § 23

(1) [1]Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der Zeitgeschichte;
2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;
4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

(2) [1]Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

# Datenschutzgütesiegelverordnung (DSGSVO)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung) |
| **Amtliche Abkürzung:** | DSGSVO |
| **Ausfertigung:** | 30.11.2013, GVOBl. 2013 S. 536 |
| **Inkrafttreten:** | 01.01.2014 |
| **Außerkrafttreten:** | 31.12.2018 |

## Inhaltsübersicht


| | | |
|---|---|---|
| § 1 | Zertifizierung von IT-Produkten | 201 |
| § 2 | Verfahren | 202 |
| § 3 | Anerkennung von Sachverständigen | 202 |
| § 4 | Gebühren | 203 |
| § 5 | Inkrafttreten, Außerkrafttreten | 203 |


## § 1 Zertifizierung von IT-Produkten

(1) [1]Ein informationstechnisches Produkt (IT-Produkt) wird auf Antrag vom Unabhängigen Landeszentrum für Datenschutz zertifiziert, wenn es mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar ist. [2]Die Gültigkeit des Zertifikats kann befristet werden. Das Zertifikat kann widerrufen werden, wenn die Voraussetzungen für die Erteilung nicht mehr vorliegen.

(2) [1]IT-Produkte im Sinne dieser Verordnung sind Hardware, Software, automatisierte Verfahren und Dienstleistungen, die zur Nutzung durch öffentliche Stellen geeignet sind.

(3) [1]Zertifizierte Produkte können durch ein Gütesiegel nach der Anlage zu dieser Verordnung gekennzeichnet werden. [2]Die Anlage ist Bestandteil dieser Verordnung. [3]Das Gütesiegel muss das graphische Symbol, die Registriernummer, im Falle der Befristung das Ablaufdatum und den Verweis auf die Internetseite www.datenschutzzentrum.de/guetesiegel/ enthalten. [4]Bei einer Verwendung des Gütesiegels im Internet ist es mit der Internetseite

www.datenschutzzentrum.de/guetesiegel/ zu verlinken. [5]Im Fall der Verwendung des Gütesiegels nach Ablauf der Gültigkeit muss in geeigneter Weise ein deutlicher Hinweis auf den Ablauf der Gültigkeit erfolgen. [6]Wurden wesentliche Änderungen an dem IT-Produkt vorgenommen, ist in geeigneter Weise darauf hinzuweisen, dass sich das Zertifikat auf eine Vorversion bezieht. [7]Ist innerhalb eines Jahres nach Ablauf der Gültigkeit oder nach Vornahme wesentlicher Änderungen am IT-Produkt keine erneute Zertifizierung erfolgt, darf das Gütesiegel nicht mehr verwendet werden.

(4) [1]Das Unabhängige Landeszentrum für Datenschutz führt und veröffentlicht ein Register über alle zertifizierten IT-Produkte.

## § 2 Verfahren

(1) [1]Voraussetzung für einen Antrag nach § 1 Abs. 1 ist die Überprüfung des IT-Produktes durch hierfür vom Unabhängigen Landeszentrum für Datenschutz anerkannte Sachverständige nach § 3. [2]Die Sachverständigen sind von der Antragstellerin oder dem Antragsteller zu beauftragen.

(2) [1]Ist ein IT-Produkt nach den Feststellungen der oder des Sachverständigen mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar, legen die Antragstellerin oder der Antragsteller das entsprechende Gutachten mit einer schriftlichen Dokumentation der Prüfung dem Unabhängigen Landeszentrum für Datenschutz mit folgenden Angaben vor:

1. Zeitpunkt der Prüfung,
2. detaillierte Bezeichnung des IT-Produktes und Versionsangabe,
3. Zweck und Einsatzbereich,
4. Eigenschaften des IT-Produktes in Bezug auf den Datenschutz und die Datensicherheit, insbesondere zur Datenvermeidung und Datensparsamkeit (§ 4 Abs. 1 und § 11 Abs. 4 und 6 LDSG), Maßnahmen zum Datenschutz und zur Datensicherheit (§§ 5 und 6 LDSG), Zulässigkeit der Datenverarbeitung (§§ 11 bis 16 LDSG), Gewährleistung der Rechte der Betroffenen (§§ 26 bis 30 LDSG),
5. Bewertung,
6. Zusammenfassung der Prüfergebnisse zum Zweck der Veröffentlichung durch das Unabhängige Landeszentrum für Datenschutz (Kurzgutachten).

[2]Das Unabhängige Landeszentrum für Datenschutz kann ergänzende Angaben und die Vorlage des zu zertifizierenden IT-Produktes anfordern.

## § 3 Anerkennung von Sachverständigen

(1) [1]Das Unabhängige Landeszentrum für Datenschutz erteilt die Anerkennung zur oder zum Sachverständigen auf Antrag, wenn die erforderliche Fachkun-

de, Zuverlässigkeit und Unabhängigkeit nachgewiesen wird. [2]Die Anerkennung kann fachlich beschränkt werden. [3]Das Anerkennungsverfahren kann über eine einheitliche Stelle nach den Vorschriften des Landesverwaltungsgesetzes abgewickelt werden. [4]Für die Anerkennung gilt § 111 a des Landesverwaltungsgesetzes.

(2) [1]Liegen die Voraussetzungen für eine Anerkennung nach Absatz 1 nicht mehr vor, widerruft das Unabhängige Landeszentrum für Datenschutz die Anerkennung.

(3) [1]Das Unabhängige Landeszentrum für Datenschutz führt und veröffentlicht eine Liste der anerkannten Sachverständigen, die auch etwaige fachliche Beschränkungen der Anerkennung ausweist.

(4) [1]Die Anerkennung einer oder eines Sachverständigen durch eine zuständige Behörde des Bundes oder anderer Länder ist im Geltungsbereich der Verordnung wirksam, wenn die Voraussetzungen für die Anerkennung denen in Absatz 1 im Wesentlichen entsprechen. [2]Sachverständige nach Satz 1 werden auf Antrag in die vom Unabhängigen Landeszentrum für Datenschutz geführte Liste der anerkannten Sachverständigen aufgenommen.

## § 4 Gebühren

[1]Das Unabhängige Landeszentrum für Datenschutz erhebt für die ihm durch diese Verordnung übertragenen Aufgaben Gebühren nach Maßgabe einer Gebührenordnung.

## § 5 Inkrafttreten, Außerkrafttreten

[1]Diese Verordnung tritt am 1. Januar 2014 in Kraft. [2]Sie tritt mit Ablauf des 31. Dezember 2018 außer Kraft.

# Schul-Datenschutzverordnung (Schul-DSVO)

| | |
|---|---|
| **Vollständige Bezeichnung:** | Landesverordnung über die Verarbeitung personenbezogener Daten an öffentlichen Schulen (Schul-Datenschutzverordnung) |
| **Amtliche Abkürzung:** | SchulDSVO |
| **Ausfertigung:** | 05.06.2015, NBl.MSB Schl.-Hol. 2015 S. 163 |
| **Inkrafttreten:** | 01.08.2015 |
| **Außerkrafttreten:** | 31.07.2020 |

## Inhaltsübersicht


**Abschnitt 1: Allgemeines** **206**
§ 1 Anwendungsbereich; Begriffe 206
§ 2 Verantwortliche Stellen 206
**Abschnitt 2: Schulen** **207**
**Unterabschnitt 1 - Allgemeine Vorschriften** **207**
§ 3 Verantwortliche Personen 207
§ 4 Belehrung 208
§ 5 Zweckbindung 208
§ 6 Datenbestand 208
§ 7 Zugriffsberechtigungen 208
§ 8 Aktenführung 209
§ 9 Anspruch der Betroffenen auf Auskunft und Akteneinsicht gegenüber der Schule 210
**Unterabschnitt 2 - Zulässigkeit der Datenverarbeitung** **210**
§ 10 Erhebung; Auskunftspflicht der Betroffenen 210
§ 11 Speicherung 211
§ 12 Übermittlung 211
§ 13 Löschung 213
**Unterabschnitt 3 - Formen der Datenverarbeitung** **214**
§ 14 Nicht automatisierte Verfahren 214
§ 15 Automatisierte Verfahren 215
§ 16 Datenverarbeitung im Auftrag 215
§ 17 Digitale Klassen- und Notizbücher 215

**Unterabschnitt 4 - Dienstliche Datenverarbeitung der Lehrkräfte** **217**
§ 18 Einsatz privater informationstechnischer Geräte 217
§ 19 Persönliche Pflicht zur Löschung 218
**Unterabschnitt 5 - Elternvertretungen** **219**
§ 20 Datenverarbeitung der Elternvertretungen 219
**Abschnitt 3: Schulpsychologischer Dienst** **219**
§ 21 Datenschutzrechtliche Verantwortlichkeit 219
§ 22 Datenverarbeitung 219
§ 23 Nicht automatisierte und automatisierte Verfahren 220
§ 24 Löschung 220
**Abschnitt 4: Meldebehörden** **220**
§ 25 Von der Meldebehörde zu übermittelnde Daten 220
**Abschnitt 5: Schlussvorschriften** **221**
§ 26 Inkrafttreten; Außerkrafttreten 221

# Abschnitt 1: Allgemeines

## § 1 Anwendungsbereich; Begriffe

(1) [1]Diese Verordnung gilt für die Verarbeitung personenbezogener Daten von Schülerinnen und Schülern sowie deren Eltern (Betroffene) durch öffentliche Schulen, Elternvertretungen, den schulpsychologischen Dienst, schulische Assistenzkräfte, Schulsozialarbeiterinnen und -arbeiter sowie durch die Meldebehörde. [2]Sie gilt auch, wenn Lehrkräfte dienstlich unter Zuhilfenahme dienstlicher oder privater informationstechnischer Geräte bei der Datenverarbeitung tätig werden.

(2) [1]Andere Rechtsvorschriften über die Verarbeitung personenbezogener Daten bleiben unberührt, soweit sich aus den nachstehenden Bestimmungen nichts anderes ergibt.

(3) [1]Bei der Anwendung dieser Verordnung sind die Begriffsbestimmungen des Landesdatenschutzgesetzes (LDSG) vom 9. Februar 2000 (GVOBl. Schl.-H. S. 169), zuletzt geändert durch Gesetz vom 19. Juni 2014 (GVOBl. Schl.-H. S. 105), der Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (DSVO) vom 5. Dezember 2013 (GVOBl. Schl.-H. S. 554) und des Schulgesetzes (SchulG) zugrunde zu legen.

## § 2 Verantwortliche Stellen

[1]Verantwortliche Stellen für die Verarbeitung personenbezogener Daten sind die jeweils handelnden

1. Schulen,

2. Elternvertretungen,
3. schulpsychologischen Dienste,
4. Schulsozialarbeiterinnen und -arbeiter und
5. Meldebehörden.

[2]Auch soweit diese Stellen personenbezogene Daten in ihrem Auftrag durch andere Stellen verarbeiten lassen, bleiben sie nach § 17 LDSG verantwortlich für die Datenverarbeitung.

# Abschnitt 2: Schulen

## Unterabschnitt 1 Allgemeine Vorschriften

### § 3 Verantwortliche Personen

(1) [1]Die Schulen handeln bei der Anwendung dieser Verordnung durch die bei ihnen tätigen

1. Schulleiterinnen oder Schulleiter,
2. Verwaltungskräfte im Sinne des § 33 Absatz 3 Satz 1 SchulG,
3. Lehrkräfte,
4. Lehrkräfte im Vorbereitungsdienst,
5. Lehramtsstudentinnen und -studenten im Praktikum und
6. Personen im Sinne des § 34 Absatz 6 und Absatz 7 Satz 1 SchulG.

(2) [1]Die Schulleiterin oder der Schulleiter trägt die Verantwortung für die Beachtung des Datenschutzes. [2]Sie oder er hat die Abläufe in der Schule entsprechend zu organisieren und die Einhaltung der Bestimmungen zu überwachen. [3]Zugleich ist die Person für die Beachtung des Datenschutzes verantwortlich, die bei der Datenverarbeitung tätig wird.

## § 4 Belehrung

(1) [1]Nimmt eine Lehrkraft oder eine Person im Sinne des § 34 Absatz 6 oder Absatz 7 Satz 1 SchulG ihre oder seine Tätigkeit auf, belehrt die Schulleiterin oder der Schulleiter sie oder ihn über die Pflicht zur Beachtung des Datenschutzes. [2]Hierfür soll das Musterformular verwendet werden, das im Nachrichtenblatt des für Bildung zuständigen Ministeriums veröffentlich ist (NBl. MSB. Schl.-H. S. 173). [3]Die Belehrung ist aktenkundig zu machen. [4]Gleiches gilt entsprechend für schulische Assistenzkräfte und für Schulbegleiterinnen und Schulbegleiter.

(2) [1]Hat eine solche Belehrung bei Aufnahme der Tätigkeit nicht stattgefunden, ist sie unverzüglich nachzuholen.

## § 5 Zweckbindung

[1]Schulen können die Daten der Betroffenen nach dieser Verordnung zu Verwaltungszwecken und zum Zweck der Verwendung im Rahmen ihrer didaktisch-pädagogischen Tätigkeit erheben und verarbeiten. [2]Dient die Erhebung oder Verarbeitung eines Datums nicht ausschließlich einem didaktisch-pädagogischen Zweck, handelt es sich um ein Datum der Schulverwaltung.

## § 6 Datenbestand

(1) [1]Der Umfang der personenbezogenen Daten, die nach § 30 Absatz 1 SchulG erhoben und verarbeitet werden dürfen, ergibt sich aus der Anlage. [2]Die Anlage ist Bestandteil dieser Verordnung.

(2) [1]Mit Einwilligung der Betroffenen darf die Schule über den Datenbestand der Anlage hinaus weitere personenbezogene Daten erheben und verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. [2]Die Einwilligung bedarf der Schriftform oder der elektronischen Form, wenn nicht aufgrund der Umstände eine andere Form angemessen ist. [3]Auch mit Einwilligung dürfen unzumutbare, nicht zweckdienliche oder sachfremde Angaben nicht erhoben und verarbeitet werden.

## § 7 Zugriffsberechtigungen

(1) [1]Die in § 3 Absatz 1 Nummer 2 bis 6 genannten sowie die zur Schulsozialarbeit eingesetzten Personen können auf den Datenbestand der Schule zugreifen, soweit dies zur Erfüllung der ihnen jeweils übertragenen Aufgaben erforderlich ist. [2]Die Zustimmung der Schulleiterin oder des Schulleiters ist erforderlich; diese kann im Einzelfall oder generell in Form von Dienstanweisungen erfolgen. [3]Die Schulleiterin oder der Schulleiter bestimmt auch, wie schulische Assistenzkräfte die zur Erfüllung der ihnen übertragenen Aufgaben erforderlichen personenbezogenen Daten erhalten.

(2) [1]Lehrkräfte, Lehrkräfte im Vorbereitungsdienst sowie Lehramtsstudentinnen und -studenten im Praktikum an Förderzentren können auch auf den Datenbestand an der Schule zugreifen, an der die jeweils betreuten Schülerinnen und Schüler mit sonderpädagogischem Förderbedarf inklusiv beschult werden, soweit die dortige Schulleiterin oder der dortige Schulleiter nach Maßgabe des Absatzes 1 zustimmt.

(3) [1]Das Recht auf Einsichtnahme durch Schulaufsichtsbeamtinnen und Schulaufsichtsbeamte im Rahmen ihrer Aufgaben bleibt unberührt.

## § 8 Aktenführung

(1) [1]Die Schule führt über jede Schülerinnen und jeden Schüler eine Schülerakte. Informationen über die Betroffenen, welche in der Schule über einen längeren Zeitraum für die didaktisch-pädagogische Arbeit oder für die notwendigen Verwaltungsarbeiten benötigt werden, sollen in der Schülerakte festgehalten werden, sofern diese Verordnung nichts anderes bestimmt. Hierzu zählen insbesondere

1. der Schüleraufnahmebogen,
2. Korrespondenz mit der Schülerin oder dem Schüler sowie mit deren oder dessen Eltern,
3. Vermerke und Gesprächsprotokolle,
4. Aufzeichnungen über pädagogische Maßnahmen,
5. Verwaltungsakte und der vollständige jeweils zugehörige Verwaltungsvorgang, insbesondere
   (a) der Aufnahmebescheid,
   (b) Beurlaubungen,
   (c) Ordnungsmaßnahmen,
   (d) Beschlüsse zu Versetzungsentscheidungen,
   (e) die Festsetzung einer Attestpflicht,
   (f) die Feststellung einer Lese-Rechtschreib-Schwäche und die Gewährung von Nachteilsausgleich, Notenschutz oder einer zurückhaltenden Gewichtung der Rechtschreibleistung.

[2]Gesondert zu führen sind

1. Akten über Abschlussprüfungen (einschließlich der Dokumentation von mündlichen Prüfungsteilen sowie die schriftlichen Prüfungsteile),
2. Zweit- und Durchschriften von Zeugnissen,
3. Klassenarbeiten und andere Leistungsnachweise,
4. Krankmeldungen sowie

5. sonderpädagogische Akten nach Absatz 2.

(2) [1]Für Schülerinnen und Schüler mit sonderpädagogischem Förderbedarf wird eine Schülerakte geführt, die neben den durch das zuständige Förderzentrum erhobenen Daten die zur Feststellung des sonderpädagogischen Förderbedarfs erforderlichen Daten enthält (sonderpädagogische Akte). [2]Die sonderpädagogische Akte ist stets Datenbestand des zuständigen Förderzentrums. [3]Wird eine Schülerin oder ein Schüler mit sonderpädagogischem Förderbedarf inklusiv an einer anderen Schule beschult, ist die getrennt von der sonderpädagogischen Akte zu führende Schülerakte Datenbestand der besuchten Schule. [4]Daten, die für die individuelle Förderung der Schülerin oder des Schülers erforderlich sind (insbesondere der Förderplan), können durch die besuchte Schule und das zuständige Förderzentrum gemeinsam verarbeitet werden.

(3) [1]Die Schule darf die Daten der Schülerinnen und Schüler einer jeden Jahrgangsstufe gemäß Nummern 1.1, 1.5, 3.2 und 3.7 der Anlage in einem Schülerhauptbuch oder einer Schülerkartei speichern.

### § 9 Anspruch der Betroffenen auf Auskunft und Akteneinsicht gegenüber der Schule

[1]Soweit ein Auskunfts- oder Einsichtsrecht nach § 30 Absatz 8 SchulG besteht, ist unter Beachtung der Kostenregelungen des Schulträgers auch das Anfertigen von Kopien der betreffenden Unterlagen in der Schule zulässig.

## Unterabschnitt 2
## Zulässigkeit der Datenverarbeitung

### § 10 Erhebung; Auskunftspflicht der Betroffenen

(1) [1]Zu Verwaltungszwecken erfolgt die Erhebung personenbezogener Daten nach § 6 Absatz 1 durch die Schulleitung und das ihr gegenüber weisungsgebundene Personal des Schulsekretariats (Schulverwaltung). [2]Die in § 3 Absatz 1 Nummer 3 bis 6 genannten Personen sind nicht berechtigt, diese Daten zu Verwaltungszwecken selbst zu erheben, sondern erhalten sie nach Maßgabe des § 7 aus dem Datenbestand der Schule.

(2) [1]Soweit es sich um Daten nach § 6 Absatz 1 handelt, sind die Betroffenen gegenüber der Schulverwaltung zur Auskunft verpflichtet. [2]Wenn sie in die Erhebung und Verarbeitung eines Lichtbildes schriftlich eingewilligt haben, stellen sie dieses zur Verfügung oder die Schulverwaltung fertigt das Lichtbild digital mit einem dienstlichen Gerät. [3]Das Lichtbild muss die Schülerin oder den Schüler in

Portraitaufnahme, ohne Kopfbedeckung und ohne Bedeckung der Augen zeigen. [4]Eine Kopfbedeckung ist zulässig, wenn religiöse Gebote dies vorschreiben; im Übrigen sind Ausnahmen aus gesundheitlichen Gründen zulässig. [5]Lichtbilder können von den Betroffenen in digitaler Form oder in Papierform beigebracht werden. [6]Werden Lichtbilder in Papierform beigebracht, darf die Schulverwaltung sie digitalisieren, wenn dies für die weitere Verarbeitung erforderlich ist.

(3) [1]Gestattet die Schule im Rahmen ihrer Aufsichtspflicht nach § 17 Absatz 2 SchulG einem Dritten, zu dessen eigenen Zwecken bei einer schulischen Veranstaltung personenbezogene Daten der Schülerinnen und Schüler zu erheben, liegt die datenschutzrechtliche Verantwortlichkeit allein bei dem Dritten. [2]Die Gestattung ist nur zulässig, wenn

1. die Angabe der personenbezogenen Daten freiwillig, jederzeit für die Zukunft widerruflich und nicht Voraussetzung für eine Teilnahme an der schulischen Veranstaltung ist und

2. die Schülerinnen und Schüler hierauf vorab mündlich und schriftlich hingewiesen werden.

[3]Die Schule hat frühzeitig

1. den Dritten auf diese Grundsätze hinzuweisen und

2. die Eltern minderjähriger Schülerinnen und Schüler über die vorgesehene Erhebung der personenbezogenen Daten durch den Dritten zu informieren.

[4]In den Jahrgangsstufen 1 bis 6 ist eine Gestattung unzulässig.

## § 11 Speicherung

[1]Die personenbezogenen Daten der Betroffenen dürfen in Akten und in elektronischen Dateien gespeichert werden. [2]Eine ausschließliche elektronische Speicherung ist nur unter den Bedingungen des § 6 Absatz 4 LDSG zulässig. [3]Zeugnisdurchschriften dürfen nur elektronisch gespeichert werden, wenn sie mit einer elektronischen Signatur nach dem Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154), versehen sind.

## § 12 Übermittlung

(1) [1]Bei der Übermittlung personenbezogener Daten der Betroffenen an andere öffentliche und nichtöffentliche Stellen sind insbesondere § 30 Absatz 3 SchulG und § 4 des Gesetzes zur Kooperation und Information im Kinderschutz (KKG) vom 22. Dezember 2011 (BGBl. I S. 2975) zu beachten.

(2) [1]Andere öffentliche Stellen im Sinne des § 30 Absatz 3 SchulG sind insbesondere

1. andere öffentliche Schulen,
2. Schulträger öffentlicher Schulen,
3. Schulaufsichtsbehörden,
4. Jugendämter,
5. Gesundheitsämter - schulärztlicher Dienst -,
6. der schulpsychologische Dienst,
7. Jobcenter (§ 6d SGB II) und
8. örtliche Agentur für Arbeit (§ 367 Absatz 2 SGB III).

[2]Die Übermittlung personenbezogener Daten der Betroffenen an eine öffentliche Stelle gemäß Nummer 7 oder Nummer 8 darf zu Zwecken der Förderung der beruflichen Ausbildung oder der Vermittlung in ein Ausbildungsverhältnis oder ein Qualifizierungsangebot erfolgen.

(3) [1]Bei einem Schulwechsel übermittelt die abgebende Schule der aufnehmenden Schule auf deren Anforderung die für die weitere Schulausbildung der Schülerin oder des Schülers erforderlichen Daten. Dies sind insbesondere

1. die Individualdaten der Schülerin oder des Schülers und der Eltern (Nummer 1 und 2 der Anlage zu § 6 Absatz 1),
2. Angaben über Schulbesuchszeiträume, über die bisher besuchten Schulen und Wiederholungen von Jahrgangsstufen (mit Gründen),
3. Angaben über erreichte Schulabschlüsse oder Ausbildungsabschlüsse sowie Einzelangaben, die für die neu begonnene Schullaufbahn unerlässlich sind (insbesondere Lernpläne, bisheriger Fremdsprachen- und naturwissenschaftlicher Unterricht und alle Leistungsergebnisse ab Jahrgangsstufe 9),
4. eine Zweitschrift der letzten beiden Zeugnisse, bei der Anmeldung für die weiterführende Schule eine Zweitschrift des Halbjahreszeugnisses und des Jahreszeugnisses der Jahrgangstufe 4,
5. Angaben über einen sonderpädagogischen Förderbedarf einschließlich Förderplan,
6. der kompetenzorientierte Entwicklungsbericht oder die Schulübergangsempfehlung, wenn der Wechsel in den Jahrgangsstufen 5 bis einschließlich 7 erfolgt.

[2]Die Übermittlung weiterer personenbezogener Daten ist nur zulässig, soweit besondere Umstände dies im Einzelfall rechtfertigen; die vollständige Schülerakte darf nur zur Einsichtnahme übergeben werden, verbunden mit dem Verbot, Kopien zu fertigen. [3]Die Schulleiterin oder der Schulleiter der abgebenden Schule hat die besonderen Umstände in der Schülerakte zu dokumentieren.

[4]Entsprechendes gilt für eine Übersendung der sonderpädagogischen Akte durch das zuständige Förderzentrum bei einer inklusiven Beschulung. [5]Bei einem Wechsel der Zuständigkeit eines Förderzentrums soll die vollständige sonderpädagogische Akte zum Verbleib übersandt werden.

(4) [1]Absatz 3 gilt entsprechend, wenn Schülerinnen und Schüler an schulischen Veranstaltungen im Zusammenhang mit lehrplanmäßigem Unterricht anderer Schulen teilnehmen.

(5) [1]Die Klassenelternbeiräte erhalten von den Schulen zur Durchführung ihrer Aufgaben die Adressdaten (einschließlich Telefonnummern und E-Mail-Adressen) der Eltern und der Lehrkräfte der jeweiligen Klasse, soweit die Betroffenen hierzu schriftlich ihre Einwilligung erteilt haben. [2]Die Schulelternbeiräte erhalten von den Schulen Namen und Adressdaten (einschließlich Telefonnummer und E-Mail-Adressen) der in den Schulelternbeirat entsandten Klassenelternbeiratsmitglieder und deren Vertretung.

(6) [1]Datenübermittlungen können schriftlich oder in elektronischer Form erfolgen. [2]Die Datenübermittlung per E-Mail ist zulässig, soweit sichergestellt ist, dass die personenbezogenen Daten der Betroffenen nicht durch Unbefugte eingesehen werden können. [3]Die E-Mail-Kommunikation öffentlicher Schulen untereinander und mit anderen Landeseinrichtungen hat ausschließlich im Landesnetz Bildung zu erfolgen, wenn sie personenbezogene Daten enthält. [4]Elektronische Datenträger, die versandt werden, dürfen ausschließlich personenbezogene Daten enthalten, die für die Empfängerin oder den Empfänger bestimmt sind; sie sind nach Maßgabe des § 6 Absatz 3 LDSG zu verschlüsseln.

## § 13 Löschung

(1) [1]Schulen haben personenbezogene Daten nach Ablauf der folgenden Fristen zu löschen. [2]Sie betragen

1. 2 Jahre
   bei Schülerakten und sonderpädagogischen Akten einschließlich Lern- und Förderplänen, kompetenzorientierten Entwicklungsberichten oder Schulübergangsempfehlungen und sonderpädagogischen Gutachten;

2. 3 Jahre
   bei Klassen- und Kursbüchern;

3. 10 Jahre
   bei Akten über Abschlussprüfungen einschließlich der Prüfungsniederschriften und der Arbeiten in der schriftlichen Prüfung;

4. 55 Jahre
   bei Schülerhauptbüchern und Schülerkarteien.

[3]Die Fristen beginnen mit Ablauf des Schuljahres, in dem die Unterlagen und Dateien jeweils geschlossen wurden. [4]Sie betragen ferner

1. 2 Jahre
   bei Klassenarbeiten und der Dokumentation anderer Leistungsnachweise;

2. 10 Jahre
   bei Zeugnislisten und -durchschriften, soweit sie nicht von Satz 2 Nummer 3 erfasst sind;

3. 40 Jahre
   bei Zweitschriften von Abgangs- und Abschlusszeugnissen.

[5]Die Fristen beginnen mit Ablauf des Schuljahres, in dem die Unterlagen und Dateien jeweils erstellt werden. [6]Alle übrigen personenbezogenen Daten sind zu löschen, sobald sie für die konkrete Aufgabenerfüllung nicht mehr erforderlich sind, spätestens aber fünf Jahre nach Ablauf des Schuljahres, in dem der Vorgang geschlossen worden ist. [7]Von Kindertageseinrichtungen an Grundschulen mit Einwilligung der Eltern übermittelte Daten der Betroffenen sind spätestens zwei Jahre nach Ablauf des Schuljahres zu löschen, in dem das Schulverhältnis begründet worden ist.

(2) [1]Elektronische Dateien, die personenbezogene Daten der Betroffenen enthalten, sind nach Erfüllung des Zwecks zu löschen, für den sie in elektronischer Form verwendet worden sind, spätestens aber mit Ablauf der Frist gemäß Absatz 1. [2]Sind diese Daten ausschließlich in elektronischen Dateien gespeichert, sind sie bei Zweckerfüllung vor Ablauf der Frist gemäß Absatz 1 vor der Löschung dieser Dateien auszudrucken und als Akte oder Kartei zu speichern.

(3) [1]Ohne gesetzliche Befugnis oder wirksame Einwilligung erhobene Daten dürfen nicht gespeichert oder anderweitig verarbeitet werden und sind unverzüglich zu löschen.

(4) [1]Unterlagen, die zu löschende Daten enthalten, sind nach Maßgabe des Landesarchivgesetzes vom 11. August 1992 (GVOBl. Schl.-H. S. 444), zuletzt geändert durch Gesetz vom 3. Januar 2005 (GVOBl. Schl.-H. S. 21), Zuständigkeiten und Ressortbezeichnungen zuletzt ersetzt durch Verordnung vom 4. April 2013 (GVOBl. Schl.-H. S. 143), einem Archiv zur Übernahme anzubieten.

## Unterabschnitt 3
## Formen der Datenverarbeitung

### § 14 Nicht automatisierte Verfahren

[1]Werden die personenbezogenen Daten der Betroffenen in Akten, Karteien oder anderen nichtautomatisierten Dateien gespeichert und in nichtautomatisierten Verfahren verarbeitet, hat die Schule alle Maßnahmen nach § 5 Absatz 1 LDSG durchzuführen.

## § 15 Automatisierte Verfahren

(1) [1]Werden die personenbezogenen Daten der Betroffenen in automatisierten Verfahren verarbeitet, hat die Schule alle technischen und organisatorischen Maßnahmen im Sinne der §§ 5 und 6 LDSG und §§ 3 bis 5 DSVO durchzuführen.

(2) [1]Informationstechnik der Schule, mit der personenbezogene Daten der Betroffenen verarbeitet wird, ist so zu gestalten, dass Berechtigte nur zu solchen personenbezogenen Daten Zugang erhalten, die für die jeweilige Aufgabenerfüllung erforderlich sind.

(3) [1]Daten der Schulverwaltung dürfen in automatisierten Verfahren nur mit informationstechnischen Geräten des Schulträgers oder des RBZ verarbeitet werden, sofern keine Ausnahme nach §§ 16 bis 18 vorliegt.

(4) [1]Informationstechnische Geräte der Schulverwaltung dürfen nicht mit informationstechnischen Geräten verbunden werden, die pädagogischen Zwecken dienen. [2]Wird ein informationstechnisches Gerät zeitweise zu Verwaltungs- und zeitweise zu pädagogischen Zwecken genutzt, gilt dieses Verbot für die jeweils ausgeübte Art der Nutzung.

(5) [1]Mit dem Internet dürfen informationstechnische Geräte der Schulverwaltung nur über das Landesnetz Bildung verbunden werden.

(6) [1]Auf informationstechnischen Geräten, die pädagogischen Zwecken dienen, dürfen zu Verwaltungszwecken allein die Namen und E-Mail-Adressen der Schülerinnen und Schüler sowie die Zugehörigkeit zu einer bestimmten Klasse oder Lerngruppe verarbeitet werden.

## § 16 Datenverarbeitung im Auftrag

[1]Abweichend von § 30 Absatz 2 Satz 1 SchulG darf die Schule mit Genehmigung des für Bildung zuständigen Ministeriums personenbezogene Daten der Betroffenen im Auftrag durch andere Stellen verarbeiten lassen. [2]Die Genehmigung ist zu erteilen, soweit die Voraussetzungen des § 17 Absatz 1 bis 4 LDSG vorliegen und der Auftragsdatenverarbeitung im Einzelfall keine besonderen Gründe entgegenstehen. [3]In der Genehmigung ist zu bestimmen, zu welchem Zeitpunkt die personenbezogenen Daten von den informationstechnischen Geräten des Auftragnehmers zu löschen und in die Informationstechnik der Schulverwaltung zu überführen sind. [4]Für Datenverarbeitungsverfahren, bei denen für die Schule allein ihr Schulträger tätig wird, gilt die Genehmigung als erteilt.

## § 17 Digitale Klassen- und Notizbücher

(1) [1]Digitale Klassenbücher sind Programme, die anstelle von Klassen- oder Kursbüchern in Papierform geführt werden können. [2]In dem sich aus Absatz 3 ergebenden Umfang dürfen sie von den Lehrkräften auch als Notizbücher genutzt werden.

(2) [1]Geht die Nutzung eines digitalen Klassenbuchs mit einer Datenverarbeitung im Auftrag einher, ist eine Genehmigung nach § 16 zu erteilen, wenn die dort genannten Voraussetzungen vorliegen und die Schule sicherstellt, dass

1. die digitalen Klassen- und Kursbücher nur den die jeweiligen Klassen oder Lerngruppen unterrichtenden Lehrkräften zugänglich sind,
2. der Zugang zu den digitalen Klassen- und Kursbüchern nur mit informationstechnischen Geräten
   (a) des Schulträgers oder des RBZ oder
   (b) der Lehrkräfte erfolgt, welche gemäß § 18 Absatz 1 Satz 1 genehmigt sind, und
3. der Identitätsnachweis der Nutzerin oder des Nutzers mittels einer Kombination von mindestens zwei verschiedenen und unabhängigen Komponenten erfolgt und
4. die personenbezogenen Daten nach Absatz 3 nicht auf dem Zugangsgerät gespeichert werden; zulässig sind vorübergehende Speicherungen, die flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen und deren alleiniger Zweck es ist, eine Übertragung in einem Netz zu ermöglichen.

(3) [1]In den digitalen Klassen- und Notizbüchern dürfen nur folgende personenbezogene Daten der Schülerinnen und Schüler der jeweiligen Klasse oder Lerngruppe gespeichert werden:

1. Name, Vorname, Geburtsdatum, Geschlecht und ein unter Beachtung des § 10 Absatz 2 Satz 2 erhobenes Lichtbild
2. Adressdaten, E-Mail-Adressen, Telefon- und vergleichbare Telekommunikationsverbindungen
3. Ausschließlich in codierter Form Angaben über für die Beschulung relevante gesundheitliche Beeinträchtigungen
4. Angaben zu Nachteilsausgleich, Notenschutz oder einer zurückhaltenden Gewichtung der Rechtschreibleistung
5. Entschuldigte und unentschuldigte Fehlzeiten des laufenden Schuljahrs sowie das Bestehen einer Attestpflicht
6. Persönliche Zwischenbewertungen von Unterrichtsbeiträgen und des allgemeinen Lernverhaltens sowie Zwischennoten für schriftliche Leistungsnachweise
7. Angaben zum Sozialverhalten

[2]Ferner können die Namen, Telefonnummern und E-Mail-Adressen der Eltern gespeichert werden.

## Unterabschnitt 4
## Dienstliche Datenverarbeitung der Lehrkräfte

### § 18 Einsatz privater informationstechnischer Geräte

(1) [1]In Ausübung ihres Dienstes dürften Lehrkräfte abweichend von § 30 Absatz 2 SchulG ihre privaten informationstechnischen Geräte zur automatisierten Verarbeitung von personenbezogenen Daten der Betroffenen einsetzen, soweit ihnen hierfür zuvor eine schriftliche Genehmigung der Schulleiterin oder des Schulleiters erteilt worden ist. [23]Datenverarbeitende Stelle im Sinne des LDSG bleibt auch in diesem Fall die jeweilige Schule.

(2) [1]Die Genehmigung nach Absatz 1 Satz 1 ist der Lehrkraft auf Antrag zu erteilen, wenn

1. die Lehrkraft schriftlich zusichert,
   (a) personenbezogene Daten im Sinne dieser Verordnung nur dienstlich und persönlich zu verarbeiten und sie keinem Dritten zugänglich zu machen,
   (b) die Daten ausschließlich auf genehmigten informationstechnischen Geräten zu verarbeiten oder, wenn dabei weitere informationstechnische Geräte eingebunden werden, nur genehmigte Geräte oder solche des Schulträgers oder RBZ einzusetzen,
   (c) alle technischen und organisatorischen Maßnahmen nach dem Stand der Technik im Sinne von §§ 5 und 6 LDSG durchzuführen, insbesondere die personenbezogenen Daten gemäß § 6 Absatz 3 LDSG zu verschlüsseln und Sicherheitsmaßnahmen zu ergreifen, um den Zugriff Unbefugter auf die Daten über das Internet zu verhindern (insbesondere aktivierte Firewall, Betriebssystem und sicherheitsrelevante Software mit den jeweils aktuellen Sicherheitsupdates sowie Antiviren-Programm mit stets aktuellen Antivirensignaturen),
   (d) dem Unabhängigen Landeszentrum für Datenschutz die Wahrnehmung der Kontrollaufgaben nach § 41 LDSG und der Schulleiterin oder dem Schulleiter die Wahrnehmung der Kontrollaufgaben nach § 6 Absatz 5 LDSG zu ermöglichen,
2. die Lehrkraft schriftlich die für die Verarbeitung zu verwendenden informationstechnischen Geräte und Programme genau bezeichnet und sich verpflichtet, alle zukünftigen Änderungen hieran unverzüglich mitzuteilen,
3. die für die Verarbeitung zu verwendenden informationstechnischen Geräte und Programme Gewähr dafür bieten, die Maßnahmen gemäß §§ 5 und 6 LDSG durchführen zu können, insbesondere das nach dem Stand der

Technik und der Schutzbedürftigkeit der Daten erforderliche und angemessene Maß an Vertraulichkeit sicherzustellen; dies kann für informationstechnische Geräte und Programme angenommen werden, die eine oberste Landesbehörde oder das Unabhängige Landeszentrum für Datenschutz als solche bezeichnet hat.

(3) [1]Die Wirksamkeit der Genehmigung endet vier Jahre nach Ablauf des Schuljahres, in dem sie erteilt worden ist. [2]Bei Folgeanträgen ist die Erklärung nach Satz 1 erneut abzugeben.

(4) [1]Die Genehmigung kann aus wichtigem Grund jederzeit widerrufen werden. Sie ist unverzüglich zu widerrufen, wenn die Lehrkraft gegen Bestimmungen dieser Verordnung oder andere datenschutzrechtliche Bestimmungen verstößt oder die von ihr abgegebenen Zusicherungen nicht einhält. [2]Die Schulleiterin oder der Schulleiter hat Verstöße unverzüglich der obersten Schulaufsichtsbehörde anzuzeigen.

(5) [1]Über die erteilten Genehmigungen hat die Schulleiterin oder der Schulleiter einen Nachweis zu führen. [2]Auch der Widerruf einer Genehmigung ist zu dokumentieren.

(6) [1]Für den Datenverkehr zwischen den Lehrkräften und der Schule sowie zwischen mehreren informationstechnischen Geräten der Lehrkräfte gilt § 12 Absatz 6 Satz 2 entsprechend.

(7) [1]Eine Genehmigung nach Absatz 1 berechtigt nicht dazu, die personenbezogenen Daten durch Dritte verarbeiten zu lassen, auch nicht durch die Nutzung von so genannten „Cloud-Diensten“. [2]Über § 17 Absatz 2 hinausgehende Ausnahmen hiervon kann das für Bildung zuständige Ministerium durch Verwaltungsvorschrift vorsehen.

## § 19 Persönliche Pflicht zur Löschung

(1) [1]Haben Lehrkräfte personenbezogene Daten der Betroffenen in ihren Unterlagen oder auf ihren informationstechnischen Geräten gespeichert, sind diese Daten zu löschen, sobald sie für die konkrete Aufgabenerfüllung nicht mehr erforderlich sind; bei Unterlagen soll das Löschen durch Schreddern erfolgen.

(2) [1]Die Aufbewahrung von Notizen im Sinne des § 30 Absatz 9 SchulG, die zur Dokumentation von Leistungsbewertungen in gerichtlichen Verfahren notwendig sein können, ist noch für zwei Jahre nach Ablauf des Schuljahres erforderlich, in dem die Leistung bewertet worden ist. Die Schulleiterin oder der Schulleiter kann bestimmen, dass solche Unterlagen in der Schulverwaltung zu speichern sind.

## Unterabschnitt 5
## Elternvertretungen

### § 20 Datenverarbeitung der Elternvertretungen

(1) [1]Die Elternvertretungen verarbeiten personenbezogene Daten eigenständig und entsprechend den Bestimmungen des LDSG. [2]Die Schulleiterin oder der Schulleiter kann für die Umsetzung der hierfür erforderlichen technischen und organisatorischen Maßnahmen allgemeine schriftliche Regelungen treffen.

(2) [1]Eine eigenständige Erhebung personenbezogener Daten der Betroffenen durch die Elternvertretungen ist nicht zulässig; die für ihre Aufgabenerfüllung notwendigen personenbezogenen Daten der Betroffenen erhalten sie gemäß § 12 Absatz 5 von der Schule.

(3) [1]An die Kreiselternbeiräte und an den Landeselternbeirat werden die für ihre Arbeit erforderlichen Namen und Anschriften nicht durch die Schule, sondern gemäß § 15 Absatz 2 der Landesverordnung über die Wahl der Elternbeiräte an öffentlichen Schulen vom 7. Mai 2012 (NBl. MBK. Schl.-H. S. 113) durch die Schulelternbeiratsvorsitzende oder den Schulelternbeiratsvorsitzenden übermittelt.

## Abschnitt 3:
## Schulpsychologischer Dienst

### § 21 Datenschutzrechtliche Verantwortlichkeit

[1]Verantwortlich für die Verarbeitung der personenbezogenen Daten der Betroffenen und sonstigen Personen ist der handelnde schulpsychologische Dienst.

### § 22 Datenverarbeitung

[1]Die Schulpsychologinnen und Schulpsychologen sowie die bei ihnen berufsmäßig tätigen Gehilfen dürfen die zu ihrer Aufgabenerfüllung erforderlichen personenbezogenen Daten verarbeiten.

## § 23 Nicht automatisierte und automatisierte Verfahren

(1) [1]Für nicht automatisierte Verfahren gilt § 14 entsprechend.

(2) [1]Für automatisierte Verfahren gilt § 15 Absatz 1 entsprechend.

(3) [1]Für die automatisierte Verarbeitung der personenbezogenen Daten dürfen ausschließlich dienstlich zur Verfügung gestellte informationstechnische Geräte verwendet werden; die Benutzung privater informationstechnischer Geräte ist nicht zulässig.

(4) [1]Die Anbindung der informationstechnischen Geräte an das Internet ist nur über die Informations- und Kommunikationsinfrastruktur des jeweiligen Trägers des schulpsychologischen Dienstes sowie über die der Landesverwaltung zulässig.

## § 24 Löschung

[1]Personenbezogene Daten sind zu löschen, sobald sie zur Aufgabenerfüllung nicht mehr erforderlich sind, spätestens jedoch fünf Jahre nach Abschluss des Vorganges, zu deren Bearbeitung sie erhoben worden sind.

# Abschnitt 4: Meldebehörden

## § 25 Von der Meldebehörde zu übermittelnde Daten

[1]Die Datenübermittlung von der Meldebehörde an die zuständige Grundschule gemäß § 30 Absatz 5 SchulG erfolgt bis zum 1. September nach dem Stand vom 15. August eines jeden Jahres, das dem Jahr vorausgeht, in dem die Kinder erstmals schulpflichtig werden.

# Abschnitt 5:
# Schlussvorschriften

## § 26 Inkrafttreten; Außerkrafttreten

(1) [1]Diese Verordnung tritt am 1. August 2015 in Kraft. Sie tritt mit Ablauf des 31. Juli 2020 außer Kraft.

(2) [1]Die Datenschutzverordnung Schule vom 12. November 2008 (GVOBl. Schl.-H. S. 694), zuletzt geändert durch Verordnung vom 28. Februar 2013 (NBl. MBW. Schl.-H. S. 59), tritt mit dem Inkrafttreten dieser Verordnung außer Kraft.

## Anlage zu § 6 Absatz 1

Daten von Schülerinnen und Schülern und Eltern, die von öffentlichen Schulen gemäß § 30 Absatz 1 SchulG verarbeitet werden dürfen:

1. Individualdaten der Schülerinnen und Schüler
   - 1.1. Name, ggf. Geburtsname, Vorname
   - 1.2. Lichtbild (bei Vorliegen einer wirksamen Einwilligung)
   - 1.3. Adressdaten
   - 1.4. Telefon, E-Mail-Adressen und vergleichbare Telekommunikationsverbindungen
   - 1.5. Geschlecht
   - 1.6. Familienstand
   - 1.7. Geburtsdatum, Geburtsort und -land
   - 1.8. Staatsangehörigkeit(en)
   - 1.9. Herkunfts- und Verkehrssprache
   - 1.10. Jahr des Zuzugs nach Deutschland
   - 1.11. Konfession
   - 1.12. Krankenversicherung
   - 1.13. Aussiedlereigenschaft
2. Daten der Eltern (gemäß § 2 Absatz 5 Satz 1 SchulG) und der Mitwirkungsberechtigten (gemäß § 2 Absatz 5 Satz 2 SchulG)

2.1. Name, Vorname

2.2. Adressdaten

2.3. Erreichbarkeit privat: Telefon, E-Mail-Adressen und vergleichbare Telekommunikationsverbindungen

2.4. Erreichbarkeit am Arbeitsplatz: Telefon, E-Mail-Adressen und vergleichbare Telekommunikationsverbindungen

2.5. Einverständniserklärung gemäß § 2 Absatz 5 Satz 2 SchulG

2.6. Mitgliedschaft in Elternbeiräten

3. Schullaufbahndaten

3.1. Datum der ersten Einschulung

3.2. Eintrittsdatum

3.3. Vorbildung bei Aufnahme (bisher erreichte Schul-/Ausbildungsabschlüsse)

3.4. Bisher besuchte Schulen (Zeiträume, Schulname, Schulnummer, Anschriften mit Schulform bzw. -art, soweit nicht Schleswig-Holstein)

3.5. Klassenbezeichnung, Jahrgangsstufe, Halbjahr

3.6. Klassenlehrerin, Klassenlehrer, Tutorin, Tutor

3.7. Entlassungsdatum (Aushändigungsvermerk des Zeugnisses) und Art des erreichten Abschlusses/der bestandenen Prüfung

3.8. Überweisungsdatum, Name, Anschrift der aufnehmenden Schule

3.9. Beurlaubung vom Unterricht, insbesondere Beurlaubung vom Sportunterricht (Umfang, Zeitraum), Datum der Abmeldung vom Religionsunterricht, Wiederanmeldung sowie Teilnahme am Religionsunterricht eines anderen Bekenntnisses

3.10. Fächer, Wahlpflichtfächer, Fremdsprachenfolge (einschließlich erreichter Abschlüsse), Fachleistungskurse, Kurswechsel (einschließlich erteilter Unterrichtsstunden)

3.11. Teilnahme an zusätzlichen freiwilligen Unterrichtsveranstaltungen und Umfang in Unterrichtsstunden

3.12. Teilnahme an schulischen Veranstaltungen außerhalb des lehrplanmäßigen Unterrichts

3.13. Besuch eines DaZ-Zentrums (Deutsch als Zweitsprache)

3.14. Teilnahme an Fördermaßnahmen (einschließlich Art und Umfang)

3.15. Praktika (Zeitraum, Ausbildungsstätte mit Anschrift)

3.16. BAFöG-Schulbescheinigung (Datum und Kennzeichen)

3.17. Vermerk über Funktion in Schülervertretung oder sonstige schulbezogene Funktionen (z.B. Schülerlotse)

3.18. Beurlaubung vom Schulbesuch (soweit nicht von Nummer 3.9 erfasst)

3.19. Unterrichtsversäumnisse; Teilnahme an einem anderweitigen Unterricht gemäß § 21 Absatz 1 Satz 2 SchulG

3.20. Schülerzusatzversicherungen

3.21. Maßnahmen bei Erziehungskonflikten

3.22. Gesundheitliche Beeinträchtigungen, Behinderungen, Lese-Rechtsschreib-Schwächen, Rechenschwächen

3.23. Ergebnisse der schulärztlichen, schulpsychologischen und sonderpädagogischen Untersuchungen.

3.24. Schulbegleitungen

4. Leistungsdaten, Prüfungsdaten gemäß Zeugnisordnung, individuelle Förderung

4.1. Zeugnisnoten (Gesamtnoten), Zeugnisnoten nach Fächern/Kursergebnissen mit Noten- bzw. Punktbewertung. Wesentliche Zeugnisbemerkungen zur jeweiligen Klasse/Jahrgangsstufe: zur Versetzung, Entlassung, Wiederholung, Überspringen einer Klasse und zur Leistung: Erläuterung der Fächer-/Kursergebnisse usw.

4.2. Zeitpunkt und Ergebnis von Prüfungen und Versetzungskonferenzen sowie Beschlüsse anderer Zeugnis- und Notenkonferenzen

4.3. Ergebnisse von Lernstandserhebungen und Vergleichsarbeiten

4.4. Angaben über die Benachrichtigung bei gefährdeter Versetzung einschließlich des Hinweises auf etwaige besondere Folgen einer Nichtversetzung

4.5. Lernplan; Förderplan

4.6. Sonderpädagogische Förderung in der inklusiven Beschulung

4.7. Herkunftssprachlicher Ergänzungsunterricht der Konsulate

5. Schulartspezifische Zusatzdaten

5.1. Grundschule

5.1.1. Vorzeitige Aufnahme einschließlich Untersuchungsergebnis

5.1.2. Leistungsbewertung und Anzahl der Schuljahre in der Eingangsphase

5.1.3. Sprachfeststellung (§ 22 Absatz 2 SchulG)

5.1.4. kompetenzorientierter Entwicklungsbericht oder Schulübergangsempfehlung

5.2. Regionalschule

5.2.1. Zuordnung zu einem Bildungsgang

5.2.2. Angaben zur Fachleistungsdifferenzierung

5.3. Gemeinschaftsschule

5.3.1. Angaben zum leistungsdifferenzierten Unterricht

5.4. Oberstufe

5.4.1. Profilwahl; zusätzliche Fächerwahl

5.4.2. Kurswahl Sekundarstufe II (Grund- und Leistungskurse)

5.4.3. Leistungsergebnisse ab 9/1 bzw. 10/1

5.4.4. Fremdsprachen (Art und Zeitraum in Sekundarstufe I und II)

5.4.5. Zulassung zum Abitur
5.4.6. Wahl der Prüfungsfächer zum Abitur
5.4.7. Wahl der Prüferinnen oder Prüfer zum Abitur
5.4.8. Einzelergebnisse im Abitur
5.4.9. Besondere Berechtigungen (Latinum, Graecum, Hebraicum)
5.4.10. Feststellungsprüfungen in Fremdsprachen

5.5. Berufsbildende Schulen

5.5.1. Vorbildung
5.5.2. Ausbildungsberuf oder Berufstätigkeit und Berufsfeld oder Fachrichtung
5.5.3. Beginn und Dauer des Ausbildungsverhältnisses laut Ausbildungsvertrag
5.5.4. Fremdsprachen (Art und Zeitraum)
5.5.5. Feststellungsprüfungen in Fremdsprachen
5.5.6. Verkürzung oder Verlängerung der Ausbildung nach § 8 Berufsbildungsgesetz (BBiG) vom 23. März 2005 (BGBl. I S. 931), zuletzt geändert durch Artikel 9 b des Gesetzes vom 7. September 2007 (BGBl. I S. 2246)
5.5.7. Bezeichnung der Ausbildungsstätte mit Anschrift und Telefon
5.5.8. Besuch der Schule als nicht gemäß § 24 Absatz 4 Satz 3 bis 5, 7 SchulG zuständige Schule
5.5.9. Die unter 5.4 genannten Daten, soweit für die Berufsbildende Schule zutreffend

6. Allgemeines Lernverhalten und Sozialverhalten in der Schule

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

---

*Schleswig-Holsteins*
*Servicezentrum für Datenschutz*
*und Informationszugang*