Niedersächsisches Datenschutzgesetz (NDSG)

vom 16. Mai 2018 (Nds. GVBl. S. 66),
- VORIS 20600 -

I n h a l t s ü b e r s i c h t

E r s t e r T e i l

Ergänzende Vorschriften für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung - DS-GVO -)

Zweites Kapitel

Technische und organisatorische Pflichten des Verantwortlichen und Auftragsverarbeiters

Drittes Kapitel

Datenübermittlungen an Drittländer und an internationale Organisationen

Viertes Kapitel

Rechte der betroffenen Personen

Fünftes Kapitel

Aufsichtsbehörde und Datenschutzbeauftragte öffentlicher Stellen

Dritter Teil

Schlussvorschriften

E r s t e r T e i l

Ergänzende Vorschriften für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679

Erstes Kapitel

Allgemeines

§ 1
Regelungsgegenstand und Anwendungsbereich

(1) [1]Dieser Teil des Gesetzes trifft ergänzende Regelungen zur Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1; Nr. L 314 S. 72) für die Verarbeitung personenbezogener Daten

1. durch Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen (öffentliche Stellen)

   a) des Landes,

   b) der Kommunen und

   c) der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts

sowie

2. durch Personen und Stellen außerhalb des öffentlichen Bereichs, soweit ihnen Aufgaben der öffentlichen Verwaltung übertragen sind,

soweit die Datenverarbeitung in den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung fällt oder nach § 2 auf die Datenverarbeitung die Regelungen der Datenschutz-Grundverordnung anzuwenden sind. [2]Personen und Stellen nach Satz 1 Nr. 2 sind öffentliche Stellen im Sinne der Vorschriften dieses Teils, soweit ihnen Aufgaben der öffentlichen Verwaltung übertragen sind. [3]Öffentliche Stellen sind auch Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Satz 1 genannten juristischen Personen des öffentlichen Rechts unmittelbar oder durch eine solche Vereinigung beteiligt sind.

(2) Für die Gerichte sowie für die Behörden der Staatsanwaltschaft gelten die Vorschriften dieses Teils nur, soweit sie Verwaltungsaufgaben wahrnehmen.

(3) Für den Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten gelten die Vorschriften dieses Teils nur, soweit sie Verwaltungsaufgaben wahrnehmen.

(4) Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen und dabei personenbezogene Daten in Ausübung ihrer wirtschaftlichen Tätigkeit verarbeiten, finden für sie selbst, ihre Zusammenschlüsse und Verbände die für nicht öffentliche Stellen geltenden Vorschriften Anwendung.

(5) Für öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten sowie deren Vereinigungen gelten § 12 dieses Gesetzes und im Übrigen die für nicht öffentliche Stellen geltenden Vorschriften.

(6) Besondere Rechtsvorschriften über die Verarbeitung personenbezogener Daten gehen den Vorschriften dieses Teils vor.

§ 2
Erweiterte Anwendung der Datenschutz-Grundverordnung

Die Regelungen der Datenschutz-Grundverordnung finden

1. abweichend von Artikel 2 Abs. 1 der Datenschutz-Grundverordnung mit Ausnahme der Artikel 30, 35 und 36 der Datenschutz-Grundverordnung auch Anwendung auf die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem weder gespeichert sind noch gespeichert werden sollen, und

2. abweichend von Artikel 2 Abs. 2 Buchst. a der Datenschutz-Grundverordnung auch Anwendung auf die Verarbeitung personenbezogener Daten

   a) zum Zweck der Vorbereitung öffentlicher Auszeichnungen und Ehrungen, soweit in § 15 Abs. 2 nichts anderes bestimmt ist,

   b) in Begnadigungsverfahren, soweit in § 16 Satz 2 nichts anderes bestimmt ist, und

   c) im Rahmen einer sonstigen nicht in den sachlichen Anwendungsbereich des Unionsrechts fallenden Tätigkeit, die nicht unter Artikel 2 Abs. 2 Buchst. b bis d der Datenschutz-Grundverordnung fällt, soweit die Datenverarbeitung durch Rechtsvorschrift nicht speziell geregelt ist.

Zweites Kapitel

Rechtsgrundlagen der Datenverarbeitung

§ 3
Zulässigkeit der Verarbeitung personenbezogener Daten

[1]Die Verarbeitung personenbezogener Daten ist zulässig, soweit sie zur Erfüllung einer in der Zuständigkeit der oder des Verantwortlichen liegenden Aufgabe, deren Wahrnehmung

1. im öffentlichen Interesse liegt oder

2. in Ausübung öffentlicher Gewalt, die der oder dem Verantwortlichen übertragen wurde, erfolgt,

erforderlich ist. [2]Im Übrigen bestimmt sich die Zulässigkeit der Datenverarbeitung nach Artikel 6 Abs. 1 der Datenschutz-Grundverordnung

§ 4
Hinweis bei der Datenerhebung bei anderen Personen

[1]Werden personenbezogene Daten nicht bei der betroffenen Person, sondern bei einer anderen Person oder einer Stelle außerhalb des öffentlichen Bereichs erhoben, so ist dieser anderen Person oder Stelle auf Verlangen der Erhebungszweck mitzuteilen, soweit dadurch schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden. [2]Soweit eine Auskunftspflicht besteht, ist sie hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 5
Übermittlung personenbezogener Daten

(1) [1]Die Übermittlung personenbezogener Daten an eine andere öffentliche Stelle ist zulässig, soweit sie zur Erfüllung der Aufgaben der übermittelnden Stelle oder der empfangenden Stelle erforderlich ist und die Daten für den Zweck erhoben worden sind oder die Voraussetzungen für eine Zweckänderung vorliegen. [2]Die Übermittlung personenbezogener Daten an eine nicht öffentliche Stelle ist zulässig, soweit

1. sie zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und die Daten für den Zweck erhoben worden sind oder die Voraussetzungen für eine Zweckänderung vorliegen oder

2. die empfangende Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an der Geheimhaltung überwiegt.

[3]Bei einer Übermittlung nach Satz 2 hat sich der Empfänger gegenüber der übermittelnden öffentlichen Stelle zu verpflichten, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihm übermittelt wurden. [4]An öffentlich-rechtliche Religionsgesellschaften ist die Übermittlung nur zulässig, sofern sichergestellt ist, dass bei dem Empfänger eine Datenverarbeitung im Einklang mit der Datenschutz-Grundverordnung erfolgt.

(2) [1]Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde Stelle. [2]Erfolgt die Übermittlung aufgrund eines Ersuchens einer öffentlichen Stelle, so trägt diese die Verantwortung. [3]Die übermittelnde Stelle hat dann lediglich zu prüfen, ob sich das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle hält. [4]Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht; die ersuchende Stelle hat der übermittelnden Stelle die für diese Prüfung erforderlichen Angaben zu machen. [5]Erfolgt die Übermittlung durch automatisierten Abruf (§ 7), so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Empfänger

(3) Sind mit personenbezogenen Daten weitere personenbezogene Daten der betroffenen oder einer anderen Person so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten an öffentliche Stellen zulässig, soweit nicht berechtigte Interessen der betroffenen oder einer anderen Person an deren Geheimhaltung offensichtlich überwiegen; eine weitere Verarbeitung dieser Daten ist unzulässig.

§ 6
Zweckbindung, Zweckänderung

(1) Zu dem Zweck einer Verarbeitung personenbezogener Daten zählt auch die Verarbeitung

1. zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung und zur Durchführung von Organisationsuntersuchungen sowie

2. zu Ausbildungs- und Prüfungszwecken, soweit nicht berechtigte Interessen der betroffenen Person an der Geheimhaltung der Daten überwiegen.

(2) Eine Verarbeitung von personenbezogenen Daten zu einem anderen Zweck als dem, für den die Daten erhoben wurden, ist zulässig, soweit und solange

1. die Datenverarbeitung zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit oder zur Abwehr von erheblichen Nachteilen für das Wohl des Bundes oder eines Landes erforderlich ist,

2. die Datenverarbeitung zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Strafvollstreckung oder zur Vollstreckung von Geldbußen erforderlich ist,

3. die Datenverarbeitung zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist,

4. die Datenverarbeitung zur Überprüfung von Angaben der betroffenen Person erforderlich ist,

5. die Datenverarbeitung zum Schutz der betroffenen Person erforderlich ist oder

6. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die Daten verarbeitende Stelle sie veröffentlichen dürfte, es sei denn, dass schutzwürdige Interessen der betroffenen Person der Datenverarbeitung offensichtlich entgegenstehen.

(3) Personenbezogene Daten, die einem Berufsgeheimnis oder einem besonderen Amtsgeheimnis unterliegen und der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind, dürfen nicht nach Absatz 2 zu anderen Zwecken verarbeitet werden.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Gewährleistung der Datensicherheit oder des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht nach Absatz 2 zu anderen Zwecken verarbeitet werden.

(5) Eine Information der betroffenen Person nach Artikel 13 Abs. 3 und Artikel 14 Abs. 4 der Datenschutz-Grundverordnung über die Datenverarbeitung nach Absatz 2 Nrn. 1 bis 4 erfolgt nicht, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde.

§ 7
Automatisierte Verfahren und gemeinsame Dateien

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

Drittes Kapitel

Rechte der Betroffenen

§ 8
Beschränkung der Informationspflicht nach Artikel 13 Abs. 1 und 2 und Artikel 14 Abs. 1 bis 3 der Datenschutz-Grundverordnung

Die Verantwortlichen können von der Erteilung der Information nach Artikel 13 Abs. 1 und 2 und Artikel 14 Abs. 1 bis 3 der Datenschutz-Grundverordnung absehen, soweit und solange

1. die Information die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde,

2. dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist oder

3. die Information dazu führen würde, dass ein Sachverhalt, der nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten einer anderen Person geheim zu halten ist, aufgedeckt wird.

§ 9
Beschränkung des Auskunftsrechts

(1) [1]Bezieht sich eine nach Artikel 15 der Datenschutz-Grundverordnung verlangte Auskunft auf personenbezogene Daten, die an

1. eine Behörde der Staatsanwaltschaft, eine Polizeidienststelle oder eine andere zur Verfolgung von Straftaten zuständige Stelle,

2. eine Verfassungsschutzbehörde, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst oder

3. das Bundesministerium der Verteidigung oder eine Behörde seines nachgeordneten Bereichs

übermittelt wurden, so ist dieser Behörde vor der Erteilung der Auskunft Gelegenheit zur Stellungnahme zu geben. [2]Im Fall des Satzes 1 Nr. 3 ist dies nur erforderlich, wenn die Erteilung der Auskunft die Sicherheit des Bundes berühren könnte. [3]Die Sätze 1 und 2 gelten entsprechend für personenbezogene Daten, die von einer Behörde nach Satz 1 übermittelt wurden.

(2) [1]Die Verantwortlichen können die Erteilung einer Auskunft ablehnen, soweit und solange

1. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde,

2. dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist oder

3. die Auskunft dazu führen würde, dass ein Sachverhalt, der nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten einer anderen Person geheim zu halten ist, aufgedeckt wird.

[2]Abgelehnt werden kann auch eine Auskunft über personenbezogene Daten, die ausschließlich zu Zwecken der Gewährleistung der Datensicherheit oder der Datenschutzkontrolle verarbeitet werden und durch geeignete technische und organisatorische Maßnahmen gegen eine Verarbeitung zu anderen Zwecken geschützt sind, wenn die Erteilung der Auskunft einen unverhältnismäßigen Aufwand erfordern würde.

(3) Die Ablehnung der Auskunft ist zu begründen, soweit nicht durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

(4) [1]Wird der betroffenen Person eine Auskunft nicht erteilt, so ist die Auskunft auf Verlangen der betroffenen Person der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde (§ 18 Abs. 1 Satz 2) zu erteilen. [2]Die Mitteilung der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

(5) Über personenbezogene Daten, die nicht automatisiert verarbeitet werden und die in einem Dateisystem weder gespeichert sind noch gespeichert werden sollen (§ 2 Nr. 1), wird die Auskunft nur erteilt, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem geltend gemachten Informationsinteresse steht.

§ 10
Beschränkung der Benachrichtigungspflicht nach Artikel 34 der Datenschutz-Grundverordnung

Die Verantwortlichen können von der Benachrichtigung nach Artikel 34 der Datenschutz-Grundverordnung absehen, soweit und solange

1. die Benachrichtigung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde,

2. dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist,

3. die Benachrichtigung dazu führen würde, dass ein Sachverhalt, der nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten einer anderen Person geheim zu halten ist, aufgedeckt wird oder

4. die Benachrichtigung die Sicherheit von automatisierten Informationssystemen gefährden würde

§ 11
Dokumentationspflicht bei der Beschränkung von Rechten der betroffenen Person

Werden aufgrund von Vorschriften dieses Teils, aufgrund von Vorschriften der Datenschutz-Grundverordnung oder aufgrund anderer datenschutzrechtlicher Bestimmungen Rechte der betroffenen Person beschränkt, so haben die Verantwortlichen die Gründe dafür zu dokumentieren.

Viertes Kapitel

Besonderer Datenschutz

§ 12
Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen

(1) Die beamtenrechtlichen Vorschriften über das Führen von Personalakten des § 50 des Beamtenstatusgesetzes und der §§ 88 bis 95 des Niedersächsischen Beamtengesetzes sind für alle nicht beamteten Beschäftigten einer öffentlichen Stelle entsprechend anzuwenden, soweit tarifvertraglich nichts anderes geregelt ist.

(2) [1]Werden Feststellungen über die Eignung einer Bewerberin oder eines Bewerbers für ein Dienst- oder Arbeitsverhältnis durch ärztliche oder psychologische Untersuchungen und Tests getroffen, so darf die Einstellungsbehörde von der untersuchenden Person oder Stelle in der Regel nur das Ergebnis der Eignungsuntersuchung und Feststellungen über Faktoren anfordern, die die gesundheitliche Eignung beeinträchtigen können. [2]Weitere personenbezogene Daten darf sie nur anfordern, wenn sie die Bewerberin oder den Bewerber zuvor schriftlich über die Gründe dafür unterrichtet hat.

§ 13
Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken

(1) [1]Öffentliche Stellen dürfen personenbezogene Daten einschließlich Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung für ein bestimmtes wissenschaftliches oder historisches Forschungsvorhaben verarbeiten oder an andere Stellen zu diesem Zweck übermitteln, wenn die Art und Verarbeitung der Daten darauf schließen lassen, dass ein schutzwürdiges Interesse der betroffenen Person der Verarbeitung der Daten für das Forschungsvorhaben nicht entgegensteht oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse der betroffenen Person überwiegt. [2]Das Ergebnis der Abwägung und seine Begründung sind aufzuzeichnen. [3]Über die Verarbeitung ist die oder der Datenschutzbeauftragte nach Artikel 37 der Datenschutz-Grundverordnung zu unterrichten.

(2) [1]Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken verarbeitet, so sind sie von der Forschungseinrichtung zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. [2]Bis dahin sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, getrennt zu speichern. [3]Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Im Rahmen von wissenschaftlichen oder historischen Forschungsvorhaben dürfen personenbezogene Daten nur veröffentlicht werden, wenn

1. die betroffene Person eingewilligt hat oder

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

(4) [1]Personenbezogene Daten dürfen an Empfängerinnen und Empfänger, auf die die Vorschriften dieses Teils keine Anwendung finden, zu wissenschaftlichen oder historischen Forschungszwecken nur übermittelt werden, wenn sich diese verpflichtet haben, die Daten ausschließlich für das von ihnen bezeichnete Forschungsvorhaben und nach Maßgabe der Absätze 1 bis 3 zu verarbeiten und Schutzmaßnahmen nach § 17 oder gleichwertige Maßnahmen zu treffen. [2]Die Übermittlung ist der von der oder dem Landesbeauftragten geleiteten Behörde frühzeitig anzuzeigen.

(5) Die Verantwortlichen können von einer Gewährung der Rechte aus den Artikeln 15, 16, 18 und 21 der Datenschutz-Grundverordnung absehen, soweit und solange die Inanspruchnahme dieser Rechte voraussichtlich die Verwirklichung der jeweiligen wissenschaftlichen oder historischen Forschungszwecke unmöglich macht oder ernsthaft beeinträchtigt und der Ausschluss dieser Rechte für die Erfüllung dieser Zwecke notwendig ist.

§ 14
Videoüberwachung

(1) [1]Die Beobachtung öffentlich zugänglicher Räume mithilfe von optisch-elektronischen Einrichtungen (Videoüberwachung) und die weitere Verarbeitung der dadurch erhobenen personenbezogenen Daten sind zulässig, soweit sie zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich sind und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der von der Videoüberwachung betroffenen Personen überwiegen. [2]Zur Wahrnehmung einer öffentlichen Aufgabe gehören auch

1. der Schutz von Personen, die der beobachtenden Stelle angehören oder diese aufsuchen,

2. der Schutz von Sachen, die zu der beobachtenden Stelle oder zu den Personen nach Nummer 1 gehören, und

3. die Wahrnehmung des Hausrechts der beobachtenden Stelle.

[3]Zu einem anderen Zweck dürfen die nach Satz 1 erhobenen Daten nur verarbeitet werden, soweit dies zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist; § 6 Abs. 5 gilt entsprechend.

(2) [1]Die Videoüberwachung ist durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. [2]Zudem ist auf den Namen und die Kontaktdaten des Verantwortlichen sowie die Möglichkeit, bei dem Verantwortlichen die Informationen nach Artikel 13 der Datenschutz-Grundverordnung zu erhalten, hinzuweisen.

(3) Beim Einholen des Rates der oder des Datenschutzbeauftragten zu einer Videoüberwachung nach Artikel 35 Abs. 2 der Datenschutz-Grundverordnung hat die öffentliche Stelle insbesondere den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, den betroffenen Personenkreis, die Maßnahmen nach Absatz 2 und die vorgesehenen Auswertungen mitzuteilen.

§ 15
Öffentliche Auszeichnungen und Ehrungen

(1) [1]Zur Vorbereitung öffentlicher Auszeichnungen und Ehrungen dürfen die zuständigen Stellen die dazu erforderlichen personenbezogenen Daten einschließlich besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung verarbeiten, es sei denn, dass der zuständigen Stelle bekannt ist, dass die betroffene Person ihrer öffentlichen Auszeichnung oder Ehrung oder der damit verbundenen Datenverarbeitung widersprochen hat. [2]Auf Anforderung der in Satz 1 genannten Stellen dürfen öffentliche Stellen die erforderlichen Daten übermitteln. [3]Eine Verarbeitung der personenbezogenen Daten für andere Zwecke ist nur mit Einwilligung der betroffenen Person zulässig; § 6 Abs. 2 findet keine Anwendung.

(2) Die Artikel 13 bis 15, 19 und 21 Abs. 4 der Datenschutz-Grundverordnung finden keine Anwendung.

§ 16
Begnadigungsverfahren

[1]In Begnadigungsverfahren dürfen die zuständigen Stellen die für eine Begnadigung erforderlichen Daten einschließlich besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung verarbeiten. [2]Die Artikel 13 bis 15 und 19 der Datenschutz-Grundverordnung finden keine Anwendung.

§ 17
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung ist zulässig, soweit und solange es erforderlich ist

1. zur Wahrnehmung von Rechten und Pflichten, die aus dem Recht der sozialen Sicherheit und des Sozialschutzes folgen,

2. zur Wahrnehmung von Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts,

3. zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit von beschäftigten Personen, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einer oder einem Angehörigen eines Gesundheitsberufs, wenn diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden,

4. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit und des Infektionsschutzes, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten; ergänzend zu den in den Absätzen 2 und 3 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten,

5. zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung,

6. 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 (StGB) oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen.

(2) Werden im Rahmen der Datenverarbeitung nach diesem Kapitel oder nach anderen datenschutzrechtlichen Bestimmungen besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung verarbeitet, so sind von den Verantwortlichen und den Auftragsverarbeitern zur Wahrung der

Grundrechte und Interessen der betroffenen Person die folgenden Maßnahmen zu treffen:

1. Sicherstellung, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten verarbeitet worden sind,

2. Beschränkung der Befugnisse für den Zugriff auf personenbezogene Daten auf das erforderliche Maß sowie die Dokumentation der Befugnisse,

3. Sensibilisierung der Personen, die Zugang zu den personenbezogenen Daten haben.

(3) [1]Soweit es zum Schutz besonderer Kategorien personenbezogener Daten erforderlich ist, haben die Verantwortlichen und Auftragsverarbeiter ergänzend zu Absatz 2 weitere angemessene und spezifische Maßnahmen zu treffen. [2]Als Maßnahmen kommen insbesondere in Betracht:

1. Sicherstellung, dass die personenbezogenen Daten zur Verarbeitung nur im Vier-Augen-Prinzip freigegeben werden,

2. Sicherstellung, dass auf die personenbezogenen Daten nur nach einer Zwei-Faktor-Authentisierung zugegriffen wird,

3. Sicherstellung, dass die elektronische Übermittlung von personenbezogenen Daten nur mit einer Verschlüsselung erfolgt,

4. Sicherstellung, dass in einem vernetzten IT-System die personenbezogenen Daten nur mit Verschlüsselung gespeichert werden,

5. Sicherstellung, dass durch eine redundante Auslegung der Systeme, der Energieversorgung und der Datenübertragungseinrichtungen ein Datenverlust vermieden wird,

6. Sicherstellung, dass Daten nicht unbefugt verändert werden und ihre Integrität gewahrt ist, etwa durch Einsatz einer elektronischen Signatur,

7. Schulung der Personen, die Zugang zu den personenbezogenen Daten haben.

(4) Art und Umfang der Maßnahmen nach den Absätzen 2 und 3 richten sich nach dem Stand der Technik und den Implementierungskosten, nach der Art, dem Umfang, den Umständen und dem Zweck der Datenverarbeitung sowie nach der

Eintrittswahrscheinlichkeit und der Schwere der mit der Datenverarbeitung verbundenen Risiken für die Grundrechte und Interessen der betroffenen Person.

Fünftes Kapitel
Die oder der Landesbeauftragte für den Datenschutz

§ 18
Aufsichtsbehörde, Rechtsstellung der oder des Landesbeauftragten für den Datenschutz

1) [1]Die oder der Landesbeauftragte für den Datenschutz leitet eine von der Landesregierung unabhängige oberste Landesbehörde mit Sitz in Hannover. [2]Diese Behörde ist Aufsichtsbehörde im Sinne des Artikels 51 Abs. 1 der Datenschutz-Grundverordnung für die Datenverarbeitung im Anwendungsbereich der Vorschriften dieses Teils.

(2) Neben der nach Artikel 53 Abs. 2 der Datenschutz-Grundverordnung erforderlichen Qualifikation, Erfahrung und Sachkunde, insbesondere im Bereich des Schutzes personenbezogener Daten, soll die oder der Landesbeauftragte die Befähigung zum Richteramt haben.

(3) [1]Die oder der Landesbeauftragte wird nach der Wahl durch den Landtag auf die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen. [2]Die einmalige Wiederwahl ist zulässig. Die Amtszeit verlängert sich bis zur Berufung einer Nachfolgerin oder eines Nachfolgers, längstens jedoch um sechs Monate.

(4) Für die Landesbeauftragte oder den Landesbeauftragten gilt keine Altersgrenze. § 37 des Niedersächsischen Beamtengesetzes ist nicht anzuwenden.

(5) [1]Eine Amtsenthebung nach Artikel 53 Abs. 4 der Datenschutz-Grundverordnung erfolgt durch Beschluss des Landtages. [2]Der Beschluss bedarf der Mehrheit von zwei Dritteln der Mitglieder des Landtages.

(6) [1]Die von der oder dem Landesbeauftragten geleitete Behörde wählt ihr eigenes Personal aus. [2]Das Personal untersteht ausschließlich der Leitung der oder des Landesbeauftragten. [3]Soweit dienstrechtliche Befugnisse der Landesregierung zustehen, werden Stellen auf Vorschlag der von der oder dem Landesbeauftragten geleiteten Behörde besetzt. [4]Soweit dienstrechtliche Befugnisse der Landesregierung zustehen, können die Beschäftigten ohne ihre Zustimmung nur im Einvernehmen mit der von der oder dem Landesbeauftragten geleiteten Behörde versetzt, abgeordnet oder umgesetzt werden.

(7) [1]Die von der oder dem Landesbeauftragten geleitete Behörde darf Aufgaben der Personalverwaltung ganz oder teilweise auf eine andere Behörde übertragen. [2]In diesem

Fall dürfen personenbezogene Daten aus der Personalakte auch ohne Einwilligung der betroffenen Person an diese Behörde übermittelt und von ihr verarbeitet werden, soweit dies für die Erfüllung der übertragenen Aufgabe erforderlich ist.

(8) Der Landesrechnungshof hat die Rechnungsprüfung bei der von der oder dem Landesbeauftragten geleiteten Behörde so durchzuführen, dass die Unabhängigkeit im Sinne des Artikels 52 Abs. 1 der Datenschutz-Grundverordnung nicht beeinträchtigt wird.

§ 19
Aufgaben der Aufsichtsbehörde

(1) Die von der oder dem Landesbeauftragten geleitete Behörde nimmt ihre Aufgaben als Aufsichtsbehörde nach der Datenschutz-Grundverordnung auch in Bezug auf die Vorschriften dieses Teils und andere datenschutzrechtliche Bestimmungen wahr.

(2) Die von der oder dem Landesbeauftragten geleitete Behörde ist bei Planungen des Landes, der Kommunen, der kommunalen Anstalten und der gemeinsamen kommunalen Anstalten, der kommunalen Zweckverbände sowie des Bezirksverbands Oldenburg und des Regionalverbandes „Großraum Braunschweig“ zum Aufbau automatisierter Informationssysteme frühzeitig zu unterrichten.

§ 20
Befugnisse der Aufsichtsbehörde, Mitwirkung

(1) Die von der oder dem Landesbeauftragten geleitete Behörde hat ihre Befugnisse nach Artikel 58 Abs. 1 bis 3 der Datenschutz-Grundverordnung auch in Bezug auf die Vorschriften dieses Teils und andere datenschutzrechtliche Bestimmungen.

(2) [1]Bestehen Anhaltspunkte dafür, dass eine Datenverarbeitung gegen die Datenschutz-Grundverordnung, die Vorschriften dieses Teils oder andere datenschutzrechtliche Bestimmungen verstößt, so kann die von der oder dem Landesbeauftragten geleitete Behörde den Verantwortlichen oder den Auftragsverarbeiter auffordern, innerhalb einer bestimmten Frist Stellung zu nehmen. [2]Die von der oder dem Landesbeauftragten geleitete Behörde unterrichtet gleichzeitig die Rechts- oder Fachaufsichtsbehörde über die Aufforderung. [3]In der Stellungnahme nach Satz 1 soll auch dargestellt werden, wie die Folgen eines Verstoßes beseitigt und künftige Verstöße vermieden werden sollen. [4]Die Verantwortlichen und Auftragsverarbeiter leiten der Rechts- oder Fachaufsichtsbehörde eine Abschrift ihrer Stellungnahme zu.

(3) [1]Auch Behörden und sonstige öffentliche Stellen des Landes können gerichtlich gegen sie betreffende verbindliche Entscheidungen der von der oder dem Landesbeauftragen

für den Datenschutz geleiteten Behörde vorgehen. [2]Die Klage hat aufschiebende Wirkung.

(4) [1]Die Behörden und sonstigen öffentlichen Stellen sind verpflichtet, die von der oder dem Landesbeauftragten geleitete Behörde bei der Wahrnehmung ihrer Aufgaben zu unterstützen. [2]Dazu haben sie der von der oder dem Landesbeauftragten geleiteten Behörde insbesondere jederzeit Zugang zu den Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die die von der oder dem Landesbeauftragten geleitete Behörde zur Erfüllung ihrer Aufgaben für erforderlich hält, zu gewähren. [3]Auf Verlangen der von der oder dem Landesbeauftragten geleiteten Behörde sind alle Unterlagen über die Verarbeitung personenbezogener Daten innerhalb einer bestimmten Frist vorzulegen.

(5) Die Befugnis, Geldbußen zu verhängen, steht der von der oder dem Landesbeauftragten geleiteten Behörde gegenüber öffentlichen Stellen nur zu, soweit diese als Unternehmen am Wettbewerb teilnehmen.

§ 21
Stellungnahme zum Tätigkeitsbericht

Die Landesregierung nimmt zu dem Tätigkeitsbericht der von der oder dem Landesbeauftragten geleiteten Behörde nach Artikel 59 der Datenschutz-Grundverordnung innerhalb von sechs Monaten gegenüber dem Landtag Stellung.

§ 22

Aufsichtsbehörde für die Datenverarbeitung außerhalb des Anwendungsbereichs der Vorschriften dieses Teils

[1]Die von der oder dem Landesbeauftragten geleitete Behörde ist auch Aufsichtsbehörde im Sinne des Artikels 51 Abs. 1 der Datenschutz-Grundverordnung in Verbindung mit § 40 des Bundesdatenschutzgesetzes

1. für die Datenverarbeitung durch nicht öffentliche Stellen und

2. für die Datenverarbeitung durch öffentliche Stellen, soweit nach § 1 Abs. 4 oder Abs. 5 die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes anzuwenden sind.

3.

[2]Die von der oder dem Landesbeauftragten geleitete Behörde nimmt dabei ihre Aufgaben und Befugnisse als Aufsichtsbehörde nach der Datenschutz-Grundverordnung auch in Bezug auf andere datenschutzrechtliche Bestimmungen wahr.

Z w e i t e r T e i l

Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Abs. 1 der Richtlinie (EU) 2016/680

(Hinweis: Umsetzung der sog. „JI-RL“,
dieser Teil gilt nicht für alle Behörden und sonstigen öffentlichen Stellen, sondern nur für die in § 23 Abs. 1 und 2 genannten öffentlichen Stellen!)

Erstes Kapitel

Anwendungsbereich und Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 23
Anwendungsbereich

(1) [1]Dieser Teil des Gesetzes gilt für die öffentlichen Stellen im Sinne des § 1 Abs. 1 Satz 1 Nr. 1 Buchst. a und b sowie des § 1 Abs. 1 Satz 2, die zuständig sind für die Verarbeitung personenbezogener Daten zur Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, soweit sie zum Zweck der Erfüllung dieser Aufgaben personenbezogene Daten verarbeiten. [2]Satz 1 gilt auch für diejenigen öffentlichen Stellen, die für die Vollstreckung und den Vollzug von Strafen, von Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 StGB, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind.

(2) Absatz 1 gilt auch für diejenigen öffentlichen Stellen, die Ordnungswidrigkeiten verfolgen und ahnden sowie Sanktionen vollstrecken.

(3) [1]Andere Rechtsvorschriften des Bundes- oder des Landesrechts, in denen die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, für die in Absatz 1 genannten Stellen besonders geregelt ist, gehen den Vorschriften dieses Teils vor. [2]Soweit diese besonderen Vorschriften keine abschließenden Regelungen enthalten, sind die Vorschriften dieses Teils ergänzend anzuwenden. [3]Die Sätze 1 und 2 gelten auch für die in Absatz 2 genannten öffentlichen Stellen.

§ 24
Begriffsbestimmungen

Im Sinne dieses Teils bezeichnet der Ausdruck

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

2. „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung" die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

6. „Verantwortlicher" die zuständige öffentliche Stelle im Sinne des § 23 Abs. 1 und 2, die innerhalb ihrer Aufgabenerfüllung allein oder gemeinsam mit anderen über

die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

7. „Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

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

9. „Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

10. „genetische Daten" personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

11. „biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

12. „Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

13. „besondere Kategorien personenbezogener Daten" personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen

Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung;

14. „Aufsichtsbehörde" eine von einem Mitgliedstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle;

15. „internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;

16. „Schengen-assoziierter Staat" einen Staat, der die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsabkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwendet und den Mitgliedstaaten der Europäischen Union insoweit gleichsteht;

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

18. „Anonymisierung" 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.

§ 25
Grundsätze für die Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle im Sinne des § 23 Abs. 1 und 2 ist zulässig, soweit und solange sie zur Erfüllung der in ihrer Zuständigkeit liegenden und in § 23 Abs. 1 und 2 genannten Aufgabe erforderlich und verhältnismäßig ist.

(2) Personenbezogene Daten müssen

1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden und

3. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein, wobei alle angemessenen Maßnahmen zu treffen sind, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

(3) [1]Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unerlässlich ist. [2]Für den Schutz bei der Verarbeitung besonderer Kategorien personenbezogener Daten für die in § 23 genannten Zwecke ist § 17 entsprechend anwendbar.

(4) [1]Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 23 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten, und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. [2]Die Verarbeitung personenbezogener Daten zu einem anderen, in § 23 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(5) [1]Die Verarbeitung kann zu im öffentlichen Interesse liegenden Archivzwecken oder statistischen Zwecken erfolgen. [2]Für die Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken ist § 13 Abs. 1 bis 4 entsprechend anwendbar, wobei die Rechte der betroffenen Person auf Auskunft nach § 51, Berichtigung und Einschränkung der Verarbeitung nach § 52 nicht bestehen, soweit die Inanspruchnahme dieser Rechte voraussichtlich die Verwirklichung der jeweiligen wissenschaftlichen oder historischen Forschungszwecke unmöglich macht oder ernsthaft beeinträchtigt und der Ausschluss dieser Rechte für die Erfüllung dieser Zwecke notwendig ist.

(6) [1]Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn dies zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen erfolgt. [2]Zulässig ist auch die Verarbeitung zu Ausbildungs- und Prüfungszwecken, soweit nicht berechtigte Interessen der betroffenen Personen an der Geheimhaltung der Daten überwiegen.

§ 26
Unterscheidung verschiedener Kategorien betroffener Personen

[1]Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten soweit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. [2]Es sind insbesondere folgende Kategorien zu unterscheiden:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,

2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,

3. verurteilte Straftäterinnen und Straftäter,

4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

5. andere Personen wie insbesondere Zeuginnen und Zeugen, Hinweisgeberinnen und Hinweisgeber oder Personen, die mit den in den Nummern 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

[3]Die Sätze 1 und 2 sind entsprechend anzuwenden, soweit personenbezogene Daten zum Zweck der Verfolgung, Ahndung und Sanktionierung von Ordnungswidrigkeiten verarbeitet werden.

§ 27
Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

Bei der Verarbeitung von personenbezogenen Daten hat der Verantwortliche so weit wie möglich zwischen auf Tatsachen beruhenden Daten und auf persönlichen Einschätzungen beruhenden Daten zu unterscheiden.

§ 28
Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(1) [1]Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn

1. ihre Verarbeitung unzulässig ist,

2. ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist oder

3. sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

[2]In den Fällen des Satzes 1 Nr. 2 tritt an die Stelle der Löschung die Abgabe an das zuständige Archiv.

(2) [1]Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigt würden,

2. die Daten zu Beweiszwecken in behördlichen oder gerichtlichen Verfahren, die Zwecken des § 23 dienen, weiter aufbewahrt werden müssen oder

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

[2]In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck, der ihrer Löschung entgegenstand, verarbeitet oder sonst mit Einwilligung der betroffenen Person verarbeitet werden.

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

(4) Unbeschadet der in Rechtsvorschriften festgesetzten Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder für eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

§ 29
Automatisierte Entscheidungsfindung

(1) Eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung, die für die betroffene Person mit einer nachteiligen Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt, einschließlich Profiling, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

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

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

§ 30
Datenübermittlung außerhalb des öffentlichen Bereichs

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

1. die Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an der Geheimhaltung überwiegt, oder

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

[2]In den Fällen des Satzes 1 Nr. 2 sind die betroffenen Personen über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise und rechtzeitig zu unterrichten.

(2) Die übermittelnde Stelle hat die Empfänger zu verpflichten, die Daten nur für die Zwecke zu verarbeiten, zu denen sie ihnen übermittelt wurden.

§ 31
Automatisiertes Abrufverfahren

Die Einrichtung und Nutzung eines automatisierten Abrufverfahrens oder einer gemeinsamen automatisierten Datei, in oder aus der mehrere Daten verarbeitende öffentliche Stellen personenbezogene Daten verarbeiten, ist nach den in § 7 genannten Voraussetzungen zulässig.

§ 32
Gewährleistung des Datenschutzes bei Übermittlungen oder sonstiger Bereitstellung

(1) [1]Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass unrichtige sowie ohne sachlichen Grund unvollständige oder nicht mehr aktuelle personenbezogene Daten nicht übermittelt oder sonst bereitgestellt werden. [2]Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der personenbezogenen Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. [3]Bei jeder Übermittlung personenbezogener Daten hat er, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) [1]Hat der Verantwortliche unrichtige personenbezogene Daten übermittelt oder war die Übermittlung unzulässig, so hat er dies dem Empfänger mitzuteilen. [2]Der Empfänger hat die übermittelten unrichtigen Daten zu berichtigen oder die unzulässig übermittelten Daten nach § 26 zu löschen oder in ihrer Verarbeitung einzuschränken.

(3) [1]Hat der Verantwortliche personenbezogene Daten nach § 28 Abs. 1 Satz 1 Nr. 1 gelöscht oder nach § 28 Abs. 2 Satz 1 Nrn. 1 und 2 in der Verarbeitung eingeschränkt, so hat er anderen Empfängern, denen er die Daten übermittelt hat, diese Maßnahmen mitzuteilen. [2]Der Empfänger hat die Daten zu löschen oder in ihrer Verarbeitung einzuschränken.

(4) [1]Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. [2]Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend gekennzeichnet werden.

(5) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und in Schengen assoziierten Staaten keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

(6) § 5 ist bei der Übermittlung im Anwendungsbereich dieses Teils entsprechend anwendbar.

§ 33
Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

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

(3) [1]Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. [2]Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. [3]Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

(4) [1]Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. [2]Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. [3]Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. [4]Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, so ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

(5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

Zweites Kapitel

Technische und organisatorische Pflichten des Verantwortlichen und Auftragsverarbeiters

§ 34
Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit

(1) Der Verantwortliche hat unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere

des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten.

(2) [1]Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. [2]Er hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten sowie berechtigte Interessen der betroffenen Personen zu berücksichtigen. [3]Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. [4]Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

(3) [1]Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. [2]Dies betrifft die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. [3]Die Maßnahmen müssen insbesondere sicherstellen, dass die personenbezogenen Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

§ 35
Anforderungen bei der automatisierten Datenverarbeitung, Protokollierung

(1) Im Fall einer automatisierten Verarbeitung hat der Verantwortliche auf Grundlage einer Risikobewertung nach § 34 Abs. 1 und 2 Maßnahmen zu ergreifen, die je nach Art der Daten und ihrer Verwendung geeignet sind,

1. Unbefugten den Zugang zu den Verarbeitungsanlagen zu verwehren (Zugangskontrolle),

2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),

3. zu verhindern, dass personenbezogene Daten unbefugt in den Speicher eingegeben oder gespeicherte personenbezogene Daten zur Kenntnis genommen, verändert oder gelöscht werden (Speicherkontrolle),

4. zu verhindern, dass Datenverarbeitungssysteme mithilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),

5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten Zugriff haben (Zugriffskontrolle),

6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

7. zu gewährleisten, dass überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in automatisierte Datenverarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),

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

9. zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeber verarbeitet werden können (Auftragskontrolle),

10. zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

11. die innerbehördliche oder innerbetrieblicheOrganisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle),

12. zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung),

13. zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),

14. zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

(2) In automatisierten Datenverarbeitungssystemen hat der Verantwortliche zumindest folgende Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,

2. Veränderung,

3. Abfrage,

4. Offenlegung einschließlich Übermittlung,

5. Kombination und

6. Löschung

der personenbezogenen Daten.

(3) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identifizierung der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers solcher personenbezogenen Daten festzustellen.

(4) [1]Die Protokolldaten dürfen ausschließlich verwendet werden für

1. Strafverfahren,

2. die Gewährleistung der Datensicherheit oder des ordnungsgemäßen Betriebes eines Datenverarbeitungssystems,

3. die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten oder durch die von dem oder der Landesbeauftragten für den Datenschutz geleitete Behörde.

[2]Der Verantwortliche hat die Protokolle der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde auf Anforderung zur Verfügung zu stellen. [3]Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.

§ 36
Datengeheimnis

[1]Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). [2]Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort. [3]Die Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten.

§ 37
Verarbeitung auf Weisung

Jede einem Verantwortlichen unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist.

§ 38
Verzeichnis von Verarbeitungstätigkeiten

[1]Der Verantwortliche hat ein Verzeichnis von Verarbeitungstätigkeiten in entsprechender Anwendung des Artikels 30 Abs. 1 der Datenschutz-Grundverordnung zu erstellen, in das zusätzlich die Rechtsgrundlage der Verarbeitung sowie gegebenenfalls die Verwendung von Profiling aufgenommen werden. [2]Artikel 30 Abs. 3 und 4 der Datenschutz-Grundverordnung ist entsprechend anwendbar.

§ 39
Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Datenverarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

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

(3) [1]Die Folgenabschätzung hat die Rechte und die schutzwürdigen Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener angemessen zu berücksichtigen. [2]Sie ist schriftlich zu dokumentieren und enthält zumindest

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,

2. eine Bewertung der Erforderlichkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,

3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

4. die Maßnahmen, mit denen die bestehenden Risiken eingedämmt werden sollen, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden soll.

(4) Der Verantwortliche holt bei der Durchführung der Datenschutz-Folgenabschätzung den Rat der oder des behördlichen Datenschutzbeauftragten ein.

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

§ 40
Vorherige Anhörung der Aufsichtsbehörde

(1) [1]Vor der Inbetriebnahme neu anzulegender Datenverarbeitungssysteme hat der Verantwortliche die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 39 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hätte und der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder

2. die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien und Verfahren, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hätte.

[2]Die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

(2) Die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde ist bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften anzuhören, die die Verarbeitung personenbezogener Daten betreffen.

3) Der von der oder dem Landesbeauftragten geleiteten Behörde sind die in Artikel 36 Abs. 3 der Datenschutz-Grundverordnung genannten Informationen sowie auf Anforderung weitere Informationen vorzulegen, die sie benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(4) [1]Falls die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, so kann sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. [2]Die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. [3]Sie hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen oder gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren und die Gründe für die Verzögerung mitzuteilen.

(5) [1]Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, so kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 4 genannten Frist beginnen. [2]In diesem Fall sind die Empfehlungen der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde nachträglich zu berücksichtigen, wobei die Art und Weise der Verarbeitung insoweit gegebenenfalls anzupassen ist.

§ 41

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) [1]Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten in entsprechender Anwendung des Artikels 33 Abs. 1 bis 4 der Datenschutz-Grundverordnung der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde zu melden und in entsprechender Anwendung des Artikels 33 Abs. 5 der Datenschutz-Grundverordnung zu dokumentieren. [2]Wenn personenbezogene Daten von dem oder an den Verantwortlichen eines anderen Mitgliedstaates übermittelt wurden, so sind die Informationen in entsprechender Anwendung des Artikels 33 Abs. 3 der Datenschutz-Grundverordnung unverzüglich auch an diesen zu melden.

(2) In einem Strafverfahren gegen die Meldepflichtige oder den Meldepflichtigen oder ihre oder seine in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen darf die Meldung nach Absatz 1 nur mit Zustimmung der oder des Meldepflichtigen verwendet werden.

§ 42

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) [1]Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich zu benachrichtigen. [2]Artikel 34 der Datenschutz-Grundverordnung ist entsprechend anwendbar.

(2) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in Artikel 34 Abs. 3 der Datenschutz-Grundverordnung genannten Voraussetzungen unterbleiben und unter den in § 51 Abs. 3 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund des von der Verletzung ausgehenden hohen Risikos im Sinne des Absatzes 1 überwiegen.

(3) § 41 Abs. 2 ist entsprechend anwendbar.

§ 43
Vertrauliche Meldung von Verstößen

(1) Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

(2) [1]Die Beschäftigten einer öffentlichen Stelle im Sinne des § 23 Abs. 1 und 2 dürfen sich unbeschadet ihres Rechts nach Absatz 1 in allen Angelegenheiten des Datenschutzes jederzeit an die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde wenden. [2]Der Einhaltung des Dienstweges bedarf es nicht, wenn die oder der Beschäftigte auf einen Verstoß gegen datenschutzrechtliche Vorschriften oder auf die Gefahr hingewiesen hat, dass eine Person in unzulässiger Weise in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt wird, und diesem Hinweis binnen angemessener Frist nicht abgeholfen worden ist.

§ 44
Gemeinsam Verantwortliche

[1]Zwei oder mehr Verantwortliche können gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. **[2]**Artikel 26 Abs. 1 und 3 der Datenschutz-Grundverordnung ist entsprechend anwendbar.

§ 45
Auftragsverarbeitung

(1) [1]Werden personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet, so bleibt dieser für die Einhaltung der Vorschriften dieses Teils und anderer Vorschriften über den Datenschutz verantwortlich. [2]Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind gegenüber dem Verantwortlichen geltend zu machen. [3]Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

(2) Für die Auswahl der Auftragsverarbeiter durch den Verantwortlichen ist Artikel 28 Abs. 1 der Datenschutz-Grundverordnung entsprechend anwendbar.

(3) [1]Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen in Artikel 28 Abs. 3 Satz 1 der Datenschutz-Grundverordnung genannten Rechtsinstruments zu erfolgen. [2]Der Vertrag oder das andere Rechtsinstrument hat insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung des Verantwortlichen handelt,

2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,

3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten,

4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht,

5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die nach § 35 Abs. 2 bis 5 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt,

6. Überprüfungen, die von dem Verantwortlichen oder einer von diesem beauftragten prüfenden Person durchgeführt werden, ermöglicht und dazu beiträgt,

7. die in Absatz 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält,

8. alle nach § 35 Abs. 1 erforderlichen Maßnahmen ergreift und

9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 25 bis 28, 32, 34 bis 42, 45 Abs. 6 und § 57 Abs. 4 genannten Pflichten unterstützt.

(4) Der Vertrag oder das andere Rechtsinstrument im Sinne des Absatzes 3 ist schriftlich oder elektronisch abzufassen.

(5) [1]Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag oder anderen Rechtsinstrument mit dem Verantwortlichen nach Absatz 3 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer

Vorschriften verbindlich sind. [2]Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters. [3]Für die vorherige schriftliche Genehmigung der Beauftragung eines weiteren Auftragsverarbeiters durch den Verantwortlichen ist Artikel 28 Abs. 2 der Datenschutz-Grundverordnung entsprechend anwendbar.

(6) [1]Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, so meldet er diese dem Verantwortlichen unverzüglich. [2]Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, so hat er den Verantwortlichen unverzüglich zu informieren.

(7) [1]Der Auftragsverarbeiter hat ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung in entsprechender Anwendung des Artikels 30 Abs. 2 der Datenschutz-Grundverordnung zu erstellen. [2]Artikel 30 Abs. 3 und 4 der Datenschutz-Grundverordnung ist entsprechend anwendbar.

(8) Im Übrigen hat der Auftragsverarbeiter die Verpflichtungen aus den §§ 34 bis 37, 40, 45 Abs. 6 und § 57 Abs. 4 einzuhalten oder den Verantwortlichen bei der Einhaltung seiner in Absatz 3 Satz 2 Nr. 9 genannten Verpflichtungen zu unterstützen.

Drittes Kapitel

Datenübermittlungen an Drittländer und an internationale Organisationen

§ 46

Allgemeine Voraussetzungen

(1) [1]Die Übermittlung personenbezogener Daten an Stellen in Drittländern oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die in § 23 genannten Zwecke zuständig ist und

2. die Europäische Kommission nach Artikel 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 einen Angemessenheitsbeschluss gefasst hat, gemäß § 47 geeignete Garantien für den Schutz personenbezogener Daten bestehen oder eine Ausnahme nach § 48 vorliegt.

[2]Eine Übermittlung nach Satz 1 Nr. 2 ist unzulässig, wenn ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person der Übermittlung entgegenstehen. [3]Bei seiner Beurteilung hat der Verantwortliche maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

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

(3) [1]Der Verantwortliche, der Daten nach Absatz 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an Stellen in anderen Drittländern oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. [2]Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittland oder der internationalen Organisation, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. [3]Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an die Stelle im anderen Drittland oder die andere internationale Organisation zulässig wäre. [4]Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 47
Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 46 Abs. 1 Nr. 2 kein Angemessenheitsbeschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 vor, so ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen von § 46 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

2. der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) [1]Der Verantwortliche hat Übermittlungen nach Absatz 1 Nr. 2 zu dokumentieren. [2]Die Dokumentation hat den Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, die Begründung der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. [3]Sie ist der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde auf Anforderung zur Verfügung zu stellen.

(3) [1]Der Verantwortliche hat der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Absatz 1 Nr. 2 erfolgt sind. [2]In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 48

Ausnahmen für eine Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 46 Abs. 1 Nr. 2 kein Angemessenheitsbeschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 47 Abs. 1 vor, so ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 46 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,

2. zur Wahrung berechtigter Interessen der betroffenen Person,

3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,

4. im Einzelfall für die in § 23 genannten Zwecke oder

5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 23 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Absatz 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Für Übermittlungen nach Absatz 1 ist § 47 Abs. 2 und 3 entsprechend anwendbar.

§ 49
Sonstige Datenübermittlung an Empfänger in Drittländern

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittländer geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 46 Abs. 1 Nr. 1 genannte Stellen in Drittländern übermitteln, wenn die Übermittlung zur Erfüllung ihrer Aufgaben für die in § 23 genannten Zwecke unerlässlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,

2. die Übermittlung an die in § 46 Abs. 1 Nr. 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und

3. der Verantwortliche dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

(2) Im Fall des Absatzes 1 hat der Verantwortliche die in § 46 Abs. 1 Nr. 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 47 Abs. 2 und 3 entsprechend

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

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

Viertes Kapitel

Rechte der betroffenen Personen

§ 50
Allgemeine Informationen

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke, für die personenbezogene Daten im Rahmen seiner Aufgabenerfüllung verarbeitet werden,

2. die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,

3. den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten und

4. das Bestehen des Rechts, die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde anzurufen, sowie deren Kontaktdaten.

§ 51
Auskunft

(1) [1]Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft zu erteilen über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,

2. den Zweck und die Rechtsgrundlage der Verarbeitung,

3. die verfügbaren Informationen über die Herkunft der Daten,

4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind, und

5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer.

[2]Der Verantwortliche hat die betroffene Person auf ihre Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten durch den Verantwortlichen und das Bestehen des Rechts nach § 55, die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde anzurufen, hinzuweisen und deren Kontaktdaten mitzuteilen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Gewährleistung der Datensicherheit oder der Datenschutzkontrolle verarbeitet werden, wenn eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) [1]Der Verantwortliche kann die Auskunftserteilung einschränken oder ablehnen, soweit und solange

1. die Auskunft die Erfüllung der in § 23 bezeichneten Aufgaben gefährden würden,

2. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes einen Nachteil bereiten würde oder

3. die Auskunft die Interessen einer anderen Person an der Geheimhaltung gefährden würde,

es sei denn, das Informationsinteresse der betroffenen Person überwiegt das Interesse an der Vermeidung dieser Gefahren. [2]Die Auskunftserteilung kann auch eingeschränkt oder abgelehnt werden, soweit und solange die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift geheim gehalten werden müssen.

(4) [1]Bezieht sich die Auskunftserteilung auf personenbezogene Daten, die an die Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung übermittelt wurden, so ist sie nur mit Zustimmung dieser Stellen zulässig. [2]Satz 1 gilt entsprechend für personenbezogene Daten, die von einer Behörde nach Satz 1 übermittelt wurden.

(5) [1]Der Verantwortliche hat die betroffene Person über die Ablehnung oder die Einschränkung der Auskunftserteilung unverzüglich schriftlich zu unterrichten. [2]Die Ablehnung oder Einschränkung der Auskunft nach Satz 1 ist zu begründen, es sei denn, dass durch die Mitteilung der Gründe der mit der Ablehnung oder Einschränkung der Auskunft verfolgte Zweck gefährdet würde. [3]Soweit die Ablehnung oder die

Einschränkung der Auskunftserteilung nicht nach Satz 2 begründet wird, sind die Gründe hierfür aktenkundig zu machen.

(6) [1]Wird die betroffene Person nach Absatz 5 über die Ablehnung oder die Einschränkung der Auskunftserteilung unterrichtet, so kann die betroffene Person ihr Auskunftsrecht auch über die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde ausüben. [2]Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäß § 55 die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde anrufen oder gerichtlichen Rechtsschutz suchen kann. [3]Auf Verlangen der betroffenen Person erteilt der Verantwortliche der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde die begehrte Auskunft und stellt dieser die nach Absatz 5 Satz 3 dokumentierten Gründe für die Ablehnung oder Einschränkung der Auskunftserteilung zur Verfügung, es sei denn, es liegt ein Ausschlussgrund nach § 57 Abs. 8 vor. [4]Die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen oder eine Überprüfung durch sie erfolgt sind, oder über die Gründe, aus denen eine Überprüfung nicht erfolgt ist. [5]Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. [6]Die Mitteilung der von dem oder der Landesbeauftragten für den Datenschutz geleiteten Behörde an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern er nicht einer weitergehenden Auskunft zustimmt. [7]Der Verantwortliche darf die Zustimmung nur soweit und solange verweigern, wie er nach Absatz 3 von einer Auskunft absehen oder sie einschränken könnte.

§ 52
Berichtigung, Löschung und Einschränkung der Verarbeitung

(1) [1]Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. [2]Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Beurteilung, sondern die Tatsache, dass die Aussage oder Beurteilung so erfolgt ist. [3]Hat der Verantwortliche eine Berichtigung vorgenommen, so hat er einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. [4]Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, so tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. [5]In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. [6]Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn ihre Verarbeitung unzulässig oder

ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) § 28 Abs. 2 und 3 und § 32 Abs. 2 und 3 sind anwendbar.

(4) [1]Der Verantwortliche hat die betroffene Person über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung und über die Gründe hierfür schriftlich zu unterrichten. [2]Dies gilt nicht, wenn die Erteilung dieser Informationen eine Gefährdung im Sinne des § 51 Abs. 3 mit sich bringen würde. [3]Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde. [4]§ 51 Abs. 6 und 7 ist entsprechend anwendbar

§ 53
Verfahren für die Ausübung der Rechte der betroffenen Person

(1) [1]Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. [2]Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwenden.

(2) Bei Eingang von Anträgen zur Ausübung der Betroffenenrechte hat der Verantwortliche die betroffene Person unverzüglich schriftlich darüber in Kenntnis zu setzen, wie mit dem Antrag verfahren wird.

(3) [1]Informationen nach § 50, Benachrichtigungen nach speziellen Rechtsvorschriften und nach § 42 sowie die Bearbeitung von Anträgen nach den §§ 51 und 52 erfolgen für die betroffene Person unentgeltlich. [2]Bei offenkundig unbegründeten oder exzessiven Anträgen der betroffenen Person nach den §§ 51 und 52 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage des Verwaltungsaufwands verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. [3]In diesem Fall trägt der Verantwortliche die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter des Antrags.

(4) Hat der Verantwortliche begründete Zweifel an der Identität der betroffenen Person, die die Anträge nach § 51 oder § 52 gestellt hat, so kann er bei der betroffenen Person zusätzliche Informationen oder Nachweise anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 54
Schadensersatz

(1) Wird einer betroffenen Person durch eine nach diesem Teil oder nach anderen auf die Verarbeitung des Verantwortlichen anwendbaren datenschutzrechtlichen Vorschriften rechtswidrige Verarbeitung ihrer personenbezogenen Daten ein Schaden zugefügt, so sind ihr der Verantwortliche oder deren Rechtsträger unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet.

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

(3) Im Fall einer nicht automatisierten Verarbeitung besteht die Ersatzpflicht nicht, wenn der Verantwortliche nachweist, dass die Unzulässigkeit der Datenverarbeitung nicht von ihm zu vertreten ist.

(4) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welcher von mehreren Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche oder sein Rechtsträger.

(5) [1]Auf ein Mitverschulden der betroffenen Person ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anwendbar. [2]Auf die Verjährung des Schadensersatzanspruchs sind die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechend anwendbar.

§ 55
Anrufung der Aufsichtsbehörde

(1) [1]Jede betroffene Person, die meint, durch die Verarbeitung ihrer personenbezogenen Daten in ihren Rechten durch einen Verantwortlichen oder einen Auftragsverarbeiter verletzt worden zu sein, der der Kontrolle nach den Vorschriften dieses Teils unterliegt, kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde wenden. [2]Dies gilt nicht für die Verarbeitung personenbezogener Daten im Rahmen der justiziellen Tätigkeit durch Gerichte im Anwendungsbereich des § 23 Abs. 1. [3]Die betroffene Person kann sich bei der Wahrnehmung ihres Beschwerderechts entsprechend Artikel 80 der Datenschutz-Grundverordnung vertreten lassen.

(2) Die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde hat die beschwerdeführende Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie auf die Möglichkeit gerichtlichen Rechtsschutzes hinzuweisen.

(3) [1]Die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde leitet eine bei ihr eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde des anderen Staates weiter. [2]Sie hat in diesem Fall die beschwerdeführende Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

§ 56
Rechtsschutz bei Untätigkeit der Aufsichtsbehörde

[1]Wenn sich die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde nicht mit einer Beschwerde nach § 55 befasst oder die beschwerdeführende Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt wurde, so kann die beschwerdeführende Person gerichtlich dagegen vorgehen. [2]Die Regelungen aus § 20 des Bundesdatenschutzgesetzes und Artikel 78 Abs. 2 der Datenschutz-Grundverordnung sind insoweit entsprechend anwendbar.

Fünftes Kapitel
Aufsichtsbehörde und Datenschutzbeauftragte öffentlicher Stellen

§ 57
Aufgaben und Befugnisse der Aufsichtsbehörde

(1) Die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde nach § 18 ist auch Aufsichtsbehörde nach Artikel 41 Abs. 1 der Richtlinie (EU) 2016/680.

(2) Sie hat die Aufgabe,

1. die Anwendung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zu überwachen und durchzusetzen,

2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären,

3. den Landtag, die Landesregierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,

4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus der Umsetzung der Richtlinie (EU) 2016/680 entstehenden Pflichten zu sensibilisieren,

5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aus den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenzuarbeiten,

6. sich mit Beschwerden einer betroffenen Person, auch wenn sie von einer Stelle, einer Organisation oder einem Verband nach Artikel 55 der Richtlinie (EU) 2016/680 eingelegt wurden, zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere über eine notwendige Untersuchung oder eine Koordinierung mit einer anderen Aufsichtsbehörde,

7. mit anderen Aufsichtsbehörden auch durch Informationsaustausch zusammenzuarbeiten und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zu gewährleisten,

8. Untersuchungen über die Anwendung der Vorschriften dieses Teils und sonstiger Vorschriften über den Datenschutz zur Umsetzung der Richtlinie (EU) 2016/680 durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen öffentlichen Stelle,

9. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken,

10. Beratung in Bezug auf die in § 40 genannten Verarbeitungsvorgänge zu leisten und

11. Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses zu leisten.

(3) [1]Die Aufsicht über die Erhebung personenbezogener Daten durch Strafverfolgungsbehörden bei der Ermittlung, Aufdeckung oder Verfolgung von Straftaten ist erst nach Abschluss des Strafverfahrens zulässig. [2]Sie erstreckt sich nicht auf eine

Datenverarbeitung, die gerichtlich überprüft wurde. [3]Die Sätze 1 und 2 gelten für die Strafvollstreckung entsprechend.

(4) [1]Der Verantwortliche hat mit der von der oder dem Landesbeauftragten geleiteten Behörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten und sie bei der Wahrnehmung ihrer Aufgaben zu unterstützen. [2]Er hat ihr insbesondere

1. Auskunft zu erteilen sowie Einsicht in alle Unterlagen zu gewähren, die die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde zur Erfüllung ihrer Aufgaben für erforderlich hält,

2. die in Nummer 1 genannten Unterlagen auf Verlangen innerhalb einer bestimmten Frist zu übersenden und

3. den Zugang zu den Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen zu gewähren,

soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. [3]Die Untersuchungsbefugnis der von der oder dem Landesbeauftragten geleiteten Behörde erstreckt sich auch auf von öffentlichen Stellen im Sinne des § 23 Abs. 1 und 2 erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs sowie solche personenbezogene Daten, die aufgrund von Maßnahmen, die in das Recht der Unverletzlichkeit der Wohnung eingreifen, erhoben wurden. [4]Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) sowie das Grundrecht auf Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden insoweit eingeschränkt.

(5) [1]Bestehen Anhaltspunkte dafür, dass eine beabsichtigte Verarbeitung personenbezogener Daten gegen die Vorschriften dieses Teils oder gegen andere Rechtsvorschriften im Sinne des § 23 Abs. 3 Satz 1 verstößt, so kann die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde den Verantwortlichen oder den Auftragsverarbeiter warnen, dass die Datenverarbeitung voraussichtlich gegen die Vorschriften dieses Teils oder gegen andere Rechtsvorschriften im Sinne des § 23 Abs. 3 Satz 1 verstößt. [2]Stellt die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde einen solchen Verstoß im laufenden Betrieb einer Verarbeitung personenbezogener Daten fest, so kann sie den Verstoß

1. im Fall einer verantwortlichen öffentlichen Stelle des Landes im Sinne des § 23 Abs. 1 und 2 gegenüber der zuständigen obersten Landesbehörde,

2. im Fall einer verantwortlichen Kommune dieser gegenüber mit der Aufforderung beanstanden, innerhalb einer bestimmten Frist Stellung zu nehmen. 3In den Fällen

des Satzes 2 Nr. 2 ist gleichzeitig die zuständige Kommunal- und Fachaufsichtsbehörde zu unterrichten.

(6) Im Übrigen sind für die Aufsichtsbehörde nach Absatz 1 § 20 Abs. 6 und § 21 sowie Artikel 57 Abs. 2 bis 4 und Artikel 61 Abs. 1 bis 7 der Datenschutz-Grundverordnung entsprechend anwendbar.

(7) [1]Wenn eine oberste Landesbehörde im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet, dürfen die Rechte nach Absatz 4 nur von der oder dem Landesbeauftragten für den Datenschutz persönlich ausgeübt werden. [2]In diesem Fall entscheidet die oberste Landesbehörde, ob personenbezogene Daten einer betroffenen Person, der von dem Verantwortlichen Vertraulichkeit besonders zugesichert worden ist, der oder dem Landesbeauftragten für den Datenschutz gegenüber offenbart werden.

(8) [1]Auch Behörden und sonstige öffentliche Stellen des Landes können gerichtlich gegen sie betreffende verbindliche Entscheidungen der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde vorgehen. [2]Die Klage hat aufschiebende Wirkung.

§ 58
Datenschutzbeauftragte öffentlicher Stellen

(1) [1]Die Person, die nach Artikel 37 der Datenschutz-Grundverordnung als Datenschutzbeauftragte oder Datenschutzbeauftragter zu bestellen ist, nimmt im Sinne dieses Teils zusätzlich zumindest folgende Aufgaben wahr:

1. Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach den Vorschriften dieses Teils, der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften und sonstiger Vorschriften über den Datenschutz,

2. Überwachung der Einhaltung der Vorschriften dieses Teils, der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften und sonstiger Vorschriften über den Datenschutz sowie der Strategien der öffentlichen Stelle für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an Verarbeitungsvorgängen beteiligten Beschäftigten und der diesbezüglichen Überprüfungen,

3. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß § 39,

4. Zusammenarbeit mit der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde und

5. Tätigkeit als Anlaufstelle für die in Nummer 4 genannte Behörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Anhörung gemäß § 40, und gegebenenfalls Beratung zu allen sonstigen Fragen.

[2]Organisatorisch hat die oder der Datenschutzbeauftragte bei der Aufgabenwahrnehmung nach Satz 1 eine Stellung entsprechend Artikel 38 der Datenschutz-Grundverordnung.

(2) [1]Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf sie zulassen, verpflichtet, soweit er oder sie hiervon nicht durch die betroffene Person befreit wird. [2]Dies gilt auch nach Beendigung der Tätigkeit als Datenschutzbeauftragte oder Datenschutzbeauftragter.

(3) [1]Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten 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 der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

D r i t t e r T e i l

Schlussvorschriften

§ 59
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer

1. als Person, die bei einer öffentlichen Stelle oder deren Auftragsverarbeiter dienstlichen Zugang zu nicht allgemein zugänglichen personenbezogenen Daten hat oder hatte, diese Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck

   a) speichert, verändert oder übermittelt,

   b) zum Abruf bereithält,

   c) abruft oder sich oder einem anderen verschafft oder

   d) in anderer Weise verarbeitet

oder

2. personenbezogene Daten, die in dem Anwendungsbereich dieses Gesetzesverarbeitet werden und nicht allgemein zugänglich sind, durch Vortäuschung falscher Tatsachen sich oder einer anderen Person verschafft oder sich oder einer anderen Person durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung offenlegen lässt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 Euro geahndet werden.

§ 60
Straftaten

(1) [1]Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, eine in § 59 genannte Handlung begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. [2]Ebenso wird bestraft, wer

unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person zusammenführt und dadurch wieder bestimmbar macht.

(2) Der Versuch ist strafbar.

(3) [1]Die Tat wird nur auf Antrag verfolgt. [2]Antragsberechtigt sind die betroffene Person, der Verantwortliche, der Auftragsverarbeiter und die von der oder dem Landesbeauftragten geleitete Behörde.

§ 61
Übergangsvorschrift

(1) [1]Die am 24. Mai 2018 im Amt befindliche Landesbeauftragte für den Datenschutz gilt für den Rest ihrer Amtszeit als nach § 18 Abs. 3 Satz 1 und § 57 Abs. 1 berufen. [2]Ihre Rechtsstellung sowie ihre Aufgaben und Befugnisse richten sich im Anwendungsbereich des Ersten Teils nach den Vorschriften der Datenschutz-Grundverordnung sowie nach den §§ 18 bis 22 und im Anwendungsbereich des zweiten Teils nach § 57.

(2) Im Anwendungsbereich des Zweiten Teils sind vor dem 6. Mai 2016 eingerichtete automatisierte Verarbeitungssysteme zeitnah, in Ausnahmefällen, in denen dies mit einem unverhältnismäßigen Aufwand verbunden ist, jedoch spätestens bis zum 6. Mai 2023 mit § 35 Abs. 2 und 3 in Einklang zu bringen.

Artikel 2-26

Vom Abdruck der Artikel 2 bis 26 des Gesetzes zur Neuordnung des niedersächsischen Datenschutzrechts (Artikel 2 bis 25 Änderung besondere Rechtsvorschriften, Artikel 26: Inkrafttreten) wird abgesehen.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstr. 5
30159 Hannover
Tel.: 0511 120 - 4500
Fax: 0511 1204599
E-Mail: poststelle@lfd.niedersachsen.de