**Entwurf**

# G e s e t z
# zur Neuordnung des niedersächsischen Datenschutzrechts

## Artikel 1
## Niedersächsisches Datenschutzgesetz (NDSG)

Inhaltsübersicht

## Erster Abschnitt
## Allgemeines

### § 1
### Regelungsgegenstand und Anwendungsbereich des Gesetzes

(1) [1]Dieses Gesetz 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 und sonstige öffentliche Stellen

   a) des Landes,

   b) der Kommunen und

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

   und deren Vereinigungen 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 dieses Gesetzes, soweit ihnen Aufgaben der öffentlichen Verwaltung übertragen sind.

(2) Für die Gerichte sowie für die Behörden der Staatsanwaltschaft gilt dieses Gesetz nur, soweit sie Verwaltungsaufgaben wahrnehmen.

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

(4) [1]Dieses Gesetz gilt nicht, soweit

1. juristische Personen des öffentlichen Rechts oder deren organisatorisch selbständige Einrichtungen, die am Wettbewerb teilnehmen,

2. wirtschaftliche Unternehmen der Kommunen ohne eigene Rechtspersönlichkeit (Eigenbetriebe) und Zweckverbände, die überwiegend wirtschaftliche Aufgaben wahrnehmen, und

3. öffentliche Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden,

personenbezogene Daten in Ausübung ihrer wirtschaftlichen Tätigkeit verarbeiten. [2]Für die Datenverarbeitung im Rahmen dieser Tätigkeit finden die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes (BDSG) Anwendung.

(5) Für öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten sowie deren Vereinigungen gelten § 10 dieses Gesetzes und im Übrigen die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes.

(6) Besondere Rechtsvorschriften über die Verarbeitung personenbezogener Daten gehen den Bestimmungen dieses Gesetzes vor.

§ 2

Erweiterte Anwendung der Datenschutz-Grundverordnung

Die Regelungen der Datenschutz-Grundverordnung finden

1. abweichend von Artikel 2 Abs. 1 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 § 13 Abs. 2 nichts anderes bestimmt ist,

   b) in Begnadigungsverfahren, soweit in § 14 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.

## Zweiter Abschnitt
## **Rechtsgrundlagen der** Datenverarbeitung

§ 3

Zulässigkeit der Verarbeitung personenbezogener Daten

[1]Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die den Verantwortlichen übertragen wurde, erforderlich ist. [2]Im Übrigen bestimmt sich die Zulässigkeit der Datenverarbeitung nach Artikel 6 Abs. 1 der Datenschutz-Grundverordnung.

## § 4
## Erhebung personenbezogener Daten

[1]Werden in den Fällen des § 3 Satz 1 personenbezogene Daten nicht bei der betroffenen Person, sondern bei einer anderen Person oder einer Stelle außerhalb des öffentlichen Bereichs erhoben, so ist dieser 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 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, so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Empfänger.

(2) Sind mit personenbezogenen Daten weitere personenbezogene Daten der betroffenen oder einer anderen Person so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem 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.

(3) Die Absätze 1 und 2 gelten nur für Datenverarbeitungen, deren Zulässigkeit sich nach § 3 Satz 1 richtet.

## § 6
## Zweckbindung, Zweckänderung

(1) In den Fällen des § 3 Satz 1 zählt zu dem Zweck einer Verarbeitung personenbezogener Daten 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 unmittelbaren Gefahr für die öffentliche Sicherheit oder zur Abwehr von 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.

## Dritter Abschnitt
## **Rechte der betroffenen Person**

### § 7
### 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. Grund zu der Annahme besteht, dass die Information die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde,

2. die Information die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde 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.

### § 8
### Beschränkung des Auskunftsrechts nach Artikel 15 der Datenschutz-Grundverordnung

(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. Grund zu der Annahme besteht, dass die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde,

2. die Auskunft die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde 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) [1]Die Ablehnung der Auskunft ist zu begründen, soweit nicht durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. [2]Soweit die Ablehnung der Auskunft nicht nach Satz 1 begründet wird, sind die Gründe dafür aktenkundig zu machen.

(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 (§ 16 Abs. 1 Satz 2) zu erteilen, es sei denn, dass die zuständige oberste Landesbehörde im Einzelfall feststellt, dass durch die Auskunft die Sicherheit des Bundes oder eines Landes gefährdet würde. [2]Wird der von der oder dem Landesbeauftragten geleiteten

Behörde für den Datenschutz eine Auskunft nicht erteilt, so sind die Gründe dafür aktenkundig zu machen.

§ 9

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. Grund zu der Annahme besteht, dass die Benachrichtigung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde,

2. die Benachrichtigung die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde,

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.

## Vierter Abschnitt
## **Besonderer Datenschutz**

§ 10

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 oder

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.

## § 11
## Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken

(1) [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.

(2) 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.

(3) [1]Personenbezogene Daten dürfen an Empfängerinnen und Empfänger, auf die dieses Gesetz keine Anwendung findet, 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 und 2 zu verarbeiten. [2]Für eine Übermittlung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung ist es außerdem erforderlich, dass sich die Empfängerin oder der Empfänger verpflichtet, Absatz 4 zu beachten und Schutzmaßnahmen nach § 15 oder gleichwertige Maßnahmen zu treffen. [3]Die Übermittlung ist der von der oder dem Landesbeauftragten geleiteten Behörde frühzeitig anzuzeigen.

(4) [1]Besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung dürfen für wissenschaftliche oder historische Forschungszwecke verarbeitet werden, wenn der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann und wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens dem Interesse der betroffenen Person am Unterbleiben der Verarbeitung erheblich überwiegt. [2]Das Ergebnis der Abwägung und dessen Begründung sind aufzuzeichnen. [3]Über die Verarbeitung ist die oder der Datenschutzbeauftragte nach Artikel 37 der Datenschutz-Grundverordnung zu unterrichten.

(5) Die Rechte aus den Artikeln 15, 16, 18 und 21 der Datenschutz-Grundverordnung bestehen nicht, 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.

## § 12
## Videoüberwachung

(1) [1]Die Beobachtung öffentlich zugänglicher Räume mit Hilfe 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 unmittelbaren 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) [1]Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet und verarbeitet, so ist die betroffene Person über die Verarbeitung über die Artikel 13 und 14 der Datenschutz-Grundverordnung hinaus auch darüber zu informieren. [2]§ 7 gilt entsprechend. [3]Von einer Information kann auch abgesehen werden, wenn diese im Einzelfall einen unverhältnismäßigen Aufwand erfordert.

(4) Wenn die öffentliche Stelle nach Artikel 35 Abs. 2 der Datenschutz-Grundverordnung den Rat der oder des Datenschutzbeauftragten nach Artikel 37 der Datenschutz-Grundverordnung zu einer Videoüberwachung einholt, hat sie insbesondere den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, den betroffenen Personenkreis, die Maßnahmen nach Absatz 2 und die vorgesehenen Auswertungen mitzuteilen.

## § 13
## 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.

## § 14
## 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.

## § 15
## Schutzmaßnahmen bei der Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Werden im Rahmen der Datenverarbeitung nach den §§ 10 bis 14 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.

(2) [1]Soweit es zum Schutz besonderer Kategorien personenbezogener Daten erforderlich ist, haben die Verantwortlichen und Auftragsverarbeiter ergänzend zu Absatz 1 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 Ende-zu Ende-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.

(3) Art und Umfang der Maßnahmen nach den Absätzen 1 und 2 richten sich nach dem Stand der Technik und den Kosten, nach der Art, dem Umfang, den Umständen und dem Zweck der Datenverarbeitung sowie nach der Eintrittswahrscheinlichkeit und der Schwere der mit der Datenverarbeitung verbundenen Gefahren für die Grundrechte und Interessen der betroffenen Person.

## Fünfter Abschnitt
## **Die oder der Landesbeauftragte für den Datenschutz**

### § 16
### 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 dieses Gesetzes.

(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. [3]Die Amtszeit verlängert sich bis zur Berufung einer Nachfolgerin oder eines Nachfolgers, längstens jedoch um sechs Monate.

(4) [1]Für die Landesbeauftragte oder den Landesbeauftragten gilt keine Altersgrenze. [2]§ 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.

## § 17
## Aufgaben der Aufsichtsbehörde, Mitwirkung

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

(2) Die Behörden und sonstigen öffentlichen Stellen sind verpflichtet, die von der oder dem Landesbeauftragten geleitete Behörde bei der Wahrnehmung ihrer Aufgaben zu unterstützen.

(3) 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.

## § 18
## Befugnisse der Aufsichtsbehörde

(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 dieses Gesetz und andere datenschutzrechtliche Bestimmungen.

(2) [1]Bestehen Anhaltspunkte dafür, dass eine Datenverarbeitung gegen die Datenschutz-Grundverordnung, dieses Gesetz 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) Die öffentlichen Stellen sind verpflichtet, der von der oder dem Landesbeauftragten geleiteten Behörde jederzeit Zugang zu den Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu gewähren.

(4) 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.

## § 19
## 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.

§ 20

Aufsichtsbehörde für die Datenverarbeitung
außerhalb des Anwendungsbereichs dieses Gesetzes

[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 BDSG

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

[2]§ 17 Abs. 1 und § 18 Abs. 1 gelten entsprechend.

## Sechster Abschnitt
## **Schlussvorschriften**

§ 21

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 verarbeitet oder
2. personenbezogene Daten, die in dem Anwendungsbereich dieses Gesetzes verarbeitet 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.

§ 22
Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, eine in § 21 Abs. 1 genannte Handlung begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(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.

§ 23
Übergangsvorschrift

[1]Die am 24. Mai 2018 im Amt befindliche Landesbeauftragte für den Datenschutz gilt für den Rest ihrer Amtszeit als nach § 16 Abs. 3 Satz 1 berufen. [2]Ihre Rechtsstellung sowie ihre Aufgaben und Befugnisse richten sich nach den Vorschriften der Datenschutz-Grundverordnung und nach den §§ 16 bis 20.

## Artikel 2
## Änderung des Niedersächsischen Archivgesetzes

Das Niedersächsische Archivgesetz vom 25. Mai 1993 (Nds. GVBl. S. 129), geändert durch Artikel 1 des Gesetzes vom 5. November 2004 (Nds. GVBl. S. 402), wird wie folgt geändert:

1. § 3 wird wie folgt geändert:

   a) In Absatz 1 Satz 2 werden am Ende ein Komma und die Worte „und Schriftgut, das besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie

95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) enthält“ eingefügt.

b) Absatz 6 wird wie folgt geändert:

aa) Satz 2 erhält folgende Fassung:

„[2]Die §§ 3 b und 4 Satz 2 sowie die §§ 5 bis 6 a sind anzuwenden; § 3 a ist entsprechend anzuwenden.“

bb) Es wird der folgende Satz 3 angefügt:

[3]Die Einrichtungen regeln ihre Rechte und Pflichten hinsichtlich des Archivgutes durch Vereinbarung mit dem Landesarchiv.“

2. Nach § 3 werden die folgenden §§ 3 a und 3 b eingefügt:

„§ 3 a
Löschung personenbezogener Daten in Schriftgut

Der im öffentlichen Interesse liegende Archivzweck (Artikel 17 Abs. 3 Buchst. d der Datenschutz-Grundverordnung) steht einer Löschung von in Schriftgut enthaltenen personenbezogenen Daten nach Artikel 17 Abs. 1 Buchst. a der Datenschutz-Grundverordnung nicht mehr entgegen, wenn

1. die in § 1 Abs. 1 Satz 1 und Abs. 2 genannten Stellen das Schriftgut dem Landesarchiv angeboten haben und das Landesarchiv

a) festgestellt hat, dass es sich nicht um Archivgut handelt, oder

b) die Feststellung, ob es sich um Archivgut handelt, nicht innerhalb von sechs Monaten nach dem Angebot getroffen hat,

oder

2. das Landesarchiv entschieden hat, dass dieses Schriftgut nicht anzubieten ist (§ 3 Abs. 4 Satz 2).“

§ 3 b

Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung ist zulässig.“

3. § 5 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

aa) In Satz 4 werden die Worte „zur Person Betroffener“ durch die Worte „zu einer betroffenen Person“ ersetzt.

bb) In Satz 5 wird das Wort „Betroffener“ durch die Worte „betroffener Personen“ ersetzt.

b) Absatz 3 wird wie folgt geändert:

aa) Satz 1 erhält folgende Fassung:

„[1]Für die Nutzung von Archivgut, das dem Sozialgeheimnis unterliegende Daten enthält, gelten die Schutzfristen nach den §§ 11 und 12 des Bundesarchivgesetzes vom 10. März 2017 (BGBl. I S. 410), geändert durch Artikel 10 Abs. 3 des Gesetzes vom 3. Oktober 2017 (BGBl. I S. 3618).“

bb) In Satz 2 werden die Worte „§ 2 Abs. 3 Satz 1 des Bundesarchivgesetzes“ durch die Worte „§ 7 des Bundesarchivgesetzes oder nach § 2 Abs. 3 Satz 1 des Bundesarchivgesetzes vom 6. Januar 1988 (BGBl. I S. 62), zuletzt geändert durch Artikel 4 Abs. 35 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666), dieses wiederum geändert durch Artikel 4 des Gesetzes vom 10. März 2017 (BGBl. I S. 410),“ ersetzt.

c) Absatz 5 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „Betroffener“ durch die Worte „betroffener Personen“ ersetzt.

bb) In Satz 2 Nr. 2 werden die Worte „der Betroffenen“ durch die Worte „betroffener Personen“ ersetzt.

4. § 6 wird wie folgt geändert:

a) Die Absätze 1 und 2 erhalten folgende Fassung:

„(1) [1]Die Erteilung einer Auskunft nach Artikel 15 der Datenschutz-Grundverordnung ist abzulehnen, soweit und solange

1. das Archivgut nicht erschlossen ist,

2. die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen,

3. der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem geltend gemachten Informationsinteresse steht,

4. Grund zu der Annahme besteht, dass die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde, oder

5. 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]Die Ablehnung ist zu begründen. [3]Die Ablehnung nach Satz 1 Nr. 4 oder 5 muss nicht begründet werden, soweit durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. [4]Soweit die Ablehnung nach Satz 3 nicht begründet wird, sind die Gründe dafür aktenkundig zu machen. [5]Weitergehende Ansprüche nach Artikel 15 der Datenschutz-Grundverordnung bestehen nicht.

(2) [1]Besteht nach Artikel 15 der Datenschutz-Grundverordnung ein Anspruch auf Auskunft, so kann anstelle der Auskunft Einsichtnahme in das Archivgut gewährt werden, wenn der Erhaltungszustand des Archivgutes dies erlaubt. [2]Ist das

Archivgut in maschinenlesbaren Dateien gespeichert, so wird die Einsichtnahme in das Archivgut nur in eine Abbildung gewährt."

b) Absatz 3 wird gestrichen.

c) Der bisherige Absatz 4 wird Absatz 3 und wie folgt geändert:

aa) In Satz 1 werden die Worte „Machen Betroffene" durch die Worte „Macht eine betroffene Person", die Worte „können die Betroffenen" durch die Worte „kann die betroffene Person" und das Wort „ihnen" durch das Wort „ihr" ersetzt.

bb) In Satz 3 wird das Wort „Betroffene" durch die Worte „betroffene Personen" ersetzt.

5. Nach § 6 wird der folgende § 6 a eingefügt:

„§ 6 a
Ausschluss von Rechten und Pflichten
nach der Datenschutz-Grundverordnung

Rechte betroffener Personen nach Artikel 16 Satz 1 und den Artikeln 18, 20 und 21 und die Mitteilungspflicht nach Artikel 19 der Datenschutz-Grundverordnung bestehen nicht."

6. § 7 wird wie folgt geändert:

a) In der Überschrift werden die Worte „Sicherung des Archivgutes" durch das Wort „Archivgut" ersetzt.

b) § 7 Abs. 3 Satz 2 erhält folgende Fassung:

„[2]Die §§ 3 a, 3 b und 4 Satz 1 sowie die §§ 5 bis 6 a gelten entsprechend."

## Artikel 3
## Änderung des Niedersächsischen Mediengesetzes

Das Niedersächsische Mediengesetz vom 11. Oktober 2010 (Nds. GVBl. S. 480), geändert durch Gesetz vom 18. Februar 2016 (Nds. GVBl. S. 50), wird wie folgt geändert:

1. § 54 erhält folgende Fassung:

„§ 54

Datenverarbeitung durch vergleichbare Anbieter von Telemedien

(1) [1]Personen, die tätig sind für Anbieter von Telemedien, die mit den in § 57 RStV genannten Stellen vergleichbar sind, dürfen personenbezogene Daten, die sie zu journalistischen Zwecken verarbeiten, nicht zu anderen Zwecken verarbeiten (Datengeheimnis). [2]Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis hinzuweisen. [3]Das Datengeheimnis besteht nach Beendigung ihrer Tätigkeit fort. [4]Auf die Verarbeitung personenbezogener Daten zu journalistischen Zwecken durch Personen nach Satz 1 finden von der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) nur die Artikel 1 bis 5 Abs. 1 Buchst. f und Abs. 2, die Artikel 24, 32, 77 bis 84 sowie 92 bis 99 Anwendung. [5]Artikel 82 der Datenschutz-Grundverordnung gilt mit der Maßgabe, dass Anspruch auf Schadenersatz nur besteht, wenn ein Schaden durch einen Verstoß gegen Artikel 5 Abs. 1 Buchst. f, Artikel 24 oder 32 der Datenschutz-Grundverordnung entstanden ist. [6]Artikel 82 der Datenschutz-Grundverordnung gilt entsprechend, wenn gegen das Datengeheimnis nach Satz 1 oder 3 verstoßen wurde und dadurch ein materieller oder immaterieller Schaden entstanden ist.

(2) [1]Werden personenbezogene Daten durch Personen nach Absatz 1 Satz 1 zu journalistischen Zwecken verarbeitet, so ist der betroffenen Person auf Verlangen Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen. [2]Die Auskunft kann verweigert werden, soweit durch die Auskunft die Rechte oder Interessen Dritter oder die journalistische Arbeit beeinträchtigt würden. [3]Die Auskunft kann nicht nach Satz 2 verweigert werden, wenn das Interesse der betroffenen Person an der Auskunftserteilung die durch Satz 2 geschützten Interessen überwiegt.

(3) [1]Auf Verlangen der betroffenen Person sind unrichtige personenbezogene Daten unverzüglich zu berichtigen oder durch eine Darstellung der betroffenen Person zu ergänzen. [2]Die Daten sind nur dann durch eine Darstellung der betroffenen Person zu ergänzen, wenn sie einen angemessenen Umfang hat. [3]Die weitere Speicherung unrichtiger personenbezogener Daten ist zulässig, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Wahrnehmung berechtigter Interessen erforderlich ist.

(4) [1]Verbreitete Gegendarstellungen sowie Verpflichtungserklärungen und gerichtliche Entscheidungen über das Unterlassen der Verbreitung oder über den Widerruf des Inhalts personenbezogener Daten und Widerrufe sind zusammen mit den personenbezogenen Daten, auf die sie sich beziehen, und für dieselbe Zeitdauer zu speichern. [2]Werden personenbezogene Daten übermittelt, zu denen eine Gegendarstellung, eine Verpflichtungserklärung, eine gerichtliche Entscheidung oder ein Widerruf gespeichert ist, so sind auch die Gegendarstellung, die Verpflichtungserklärung, die gerichtliche Entscheidung und der Widerruf zu übermitteln.“

2. § 55 erhält folgende Fassung:

„§ 55

Datenschutzkontrolle in Bezug auf den Rundfunkstaatsvertrag

[1]Sieht die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde bei ihrer Tätigkeit als Aufsichtsbehörde nach § 20 des Niedersächsischen Datenschutzgesetzes (NDSG) Anhaltspunkte dafür, dass die Datenverarbeitung eines Rundfunkveranstalters privaten Rechts gegen datenschutzrechtliche Bestimmungen des Rundfunkstaatsvertrages verstößt, so kann sie über Artikel 58 Abs. 1 bis 3 der Datenschutz-Grundverordnung hinaus den Verantwortlichen oder den Auftragsverarbeiter auffordern, innerhalb einer bestimmten Frist Stellung zu nehmen. [2]Sie unterrichtet gleichzeitig die Landesmedienanstalt. [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 die Auftragsverarbeiter leiten der Landesmedienanstalt eine Abschrift ihrer Stellungnahme zu. [5]§ 18 Abs. 3 NDSG gilt entsprechend.“

## Artikel 4
## Änderung des Niedersächsischen Pressegesetzes

§ 19 des Niedersächsischen Pressegesetzes vom 22. März 1965 (Nds. GVBl. S. 9), zuletzt geändert durch Artikel 2 des Gesetzes vom 11. Oktober 2010 (Nds. GVBl. S. 480), erhält folgende Fassung:

„§ 19

Datenschutz

[1]Personen, die für Unternehmen der Presse oder deren Hilfsunternehmen tätig sind, dürfen personenbezogene Daten, die sie zu journalistischen Zwecken verarbeiten, nicht zu anderen Zwecken verarbeiten (Datengeheimnis). [2]Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis hinzuweisen. [3]Das Datengeheimnis besteht nach Beendigung ihrer Tätigkeit fort. [4]Auf die Verarbeitung personenbezogener Daten zu journalistischen Zwecken durch Personen nach Satz 1 finden von der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) nur die Artikel 1 bis 5 Abs. 1 Buchst. f und Abs. 2, die Artikel 24, 32, 77 bis 84 sowie 92 bis 99 Anwendung. [5]Artikel 82 der Datenschutz-Grundverordnung gilt mit der Maßgabe, dass Anspruch auf Schadenersatz nur besteht, wenn ein Schaden durch einen Verstoß gegen Artikel 5 Abs. 1 Buchst. f, Artikel 24 oder 32 der Datenschutz-Grundverordnung entstanden ist. [6]Artikel 82 der Datenschutz-Grundverordnung gilt entsprechend, wenn gegen das Datengeheimnis nach Satz 1 oder 3 verstoßen wurde und dadurch ein materieller oder immaterieller Schaden entstanden ist.“

## Artikel 5
## Änderung des Niedersächsischen Ausführungsgesetzes zum Bundesmeldegesetz

Das Niedersächsische Ausführungsgesetz zum Bundesmeldegesetz vom 17. September 2015 (Nds. GVBl. S. 186) wird wie folgt geändert:

1. § 4 erhält folgende Fassung:

„§ 4
Besonderer Meldeschein für Beherbergungsstätten

[1]Gemeinden, die nach § 10 Abs. 1 Satz 1 oder 4 des Niedersächsischen Kommunalabgabengesetzes einen Gästebeitrag erheben, können durch Satzung bestimmen, dass der besondere Meldeschein für Beherbergungsstätten nach § 30 BMG zusätzlich zu den in § 30 Abs. 2 BMG genannten Daten für die Erhebung des Gästebeitrags Familiennamen, Vornamen und Alter der Mitreisenden enthält. [2]Die in dem besonderen Meldeschein enthaltenen Daten dürfen für die Erhebung des Gästebeitrags verarbeitet werden.“

2. In § 8 Abs. 2 Nr. 3 werden die Worte „Speicherung und sonstigen“ gestrichen.

3. § 9 wird gestrichen.

**Artikel 6**
**Änderung des Niedersächsischen Rettungsdienstgesetzes**

§ 11 Abs. 4 des Niedersächsischen Rettungsdienstgesetzes in der Fassung vom 2. Oktober 2007 (Nds. GVBl. S. 473), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. Dezember 2016 (Nds. GVBl. S. 270), wird gestrichen.

**Artikel 7**
**Änderung des Niedersächsischen Brandschutzgesetzes**

Das Niedersächsische Brandschutzgesetz vom 18. Juli 2012 (Nds. GVBl. S. 269), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. September 2017 (Nds. GVBl. S. 297), wird wie folgt geändert:

1. Es wird der folgende neue Fünfte Teil eingefügt:

„F ü n f t e r  T e i l

**Datenverarbeitung**

§ 35 a

Verarbeitung personenbezogener Daten aus einsatzbedingter Kommunikation

(1) Die Feuerwehr-Einsatz-Leitstelle (§ 3 Abs. 1 Satz 2 Nr. 4) zeichnet Notrufe und den einsatzbedingten Fernmeldeverkehr auf und fertigt über jeden Einsatz ein Protokoll.

(2) [1]Die zur Durchführung dieses Gesetzes zuständigen Stellen dürfen personenbezogene Daten aus einsatzbedingter Kommunikation verarbeiten, soweit dies

1. zur Durchführung, Abwicklung oder zum Nachweis der ordnungsgemäßen Durchführung von Einsätzen,
2. zur Kostenerstattung,
3. zur Vorbereitung oder Durchführung von gerichtlichen Verfahren oder Verwaltungsverfahren,
4. für Zwecke des Qualitätsmanagements,
5. zu statistischen Zwecken oder
6. zur Aus- oder Fortbildung

erforderlich ist, oder wenn die betroffene Person eingewilligt hat. [2]Für die Zwecke nach Satz 1 Nrn. 4 bis 6 sind die personenbezogenen Daten zu anonymisieren oder zu pseudonymisieren, es sei denn, dass die Zwecke mit anonymisierten oder pseudonymisierten Daten nicht erreicht werden können.

(3) [1]Die für die Durchführung dieses Gesetzes zuständigen Stellen dürfen die für die Zwecke nach Absatz 2 Satz 1 Nrn. 1 bis 3 gespeicherten Daten an Polizeibehörden, Staatsanwaltschaften, Gerichte, Gemeinden, Landkreise, das Land, wirtschaftliche Unternehmen und öffentliche Einrichtungen mit Werkfeuerwehr (§ 16) und die Träger des Rettungsdienstes (§ 3 Abs. 1 des Niedersächsischen Rettungsdienstgesetzes) übermitteln, soweit dies zur Erfüllung von deren Aufgaben erforderlich ist. [2]Die nach Absatz 2 Satz 1 gespeicherten Daten dürfen nach vorheriger Anonymisierung oder Pseudonymisierung auch für wissenschaftliche Zwecke an Forschungseinrichtungen übermittelt werden.

## § 35 b

## Verarbeitung personenbezogener Daten von Mitgliedern der Feuerwehren sowie Lehrgangsteilnehmerinnen und Lehrgangsteilnehmern

Die zur Durchführung dieses Gesetzes zuständigen Stellen dürfen für die Feuerwehrbedarfsplanung, die Einsatzplanung, die Brandschutzerziehung, die Brandschutzaufklärung, die Mitgliederverwaltung sowie die Lehrgangsplanung und -durchführung die folgenden personenbezogenen Daten von Mitgliedern der Feuerwehren und Lehrgangsteilnehmerinnen und Lehrgangsteilnehmern verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist:

1. Name,
2. Vornamen,
3. Geburtsdatum,
4. Anschrift,
5. Beruf,
6. akademische Grade,
7. Telefonnummern und andere Angaben über die Erreichbarkeit,
8. Beschäftigungsstelle,
9. Angaben über die körperliche Tauglichkeit und die Strahlen- und Schadstoffbelastung,
10. Datum des Eintritts in die Feuerwehr,
11. Name der Feuerwehr,
12. Personalnummer, Dienstausweisnummer,
13. persönliche Ausrüstung,
14. Aus- und Fortbildungslehrgänge einschließlich der Ergebnisse von Beurteilungen,
15. Dienstgrad, Beförderungen,
16. Funktion in der Feuerwehr,
17. besondere Kenntnisse und Fähigkeiten,
18. Auszeichnungen und Ehrungen,
19. Einsätze, Dienstzeiten, sonstige geleistete Stunden,
20. Bankverbindungen,

21. Familienstand,

22. Angehörige und

23. Erziehungsberechtigte.“

2. Der bisherige Fünfte Teil wird Sechster Teil.

## Artikel 8
## Änderung des Niedersächsischen Gesetzes über das amtliche Vermessungswesen

§ 3 Abs. 2 Satz 3 des Niedersächsischen Gesetzes über das amtliche Vermessungswesen vom 12. Dezember 2002 (Nds. GVBl. 2003 S. 5) erhält folgende Fassung:

„[3]Zu den Liegenschaften sind Eigentumsangaben in Übereinstimmung mit dem Grundbuch zu führen.“

## Artikel 9
## Änderung des Niedersächsischen Statistikgesetzes

Das Niedersächsische Statistikgesetz vom 27. Juni 1988 (Nds. GVBl. S. 113), zuletzt geändert durch Artikel 8 des Gesetzes vom 16. Dezember 2004 (Nds. GVBl. S. 634), wird wie folgt geändert:

1. In § 1 Abs. 1 Nr. 1 werden die Worte „vom 22. Januar 1987 (BGB. I S. 462) zuletzt geändert durch Artikel 16 des Gesetzes vom 21. August 2002 (BGBl. I S. 3322)“ durch die Worte „in der Fassung vom 20. Oktober 2016 (BGBl. I. S. 2394)“ ersetzt.

2. § 8 wird wie folgt geändert:

   a) Es wird der folgende neue Absatz 2 eingefügt:

      „(2) Die Landesstatistikbehörde darf dem Statistischen Bundesamt und den statistischen Ämtern der anderen Länder zur Erstellung koordinierter Länderstatistiken oder für methodische Untersuchungen Einzelangaben übermitteln.“

   b) Die bisherigen Absätze 2 bis 7 werden Absätze 3 bis 8.

## Artikel 10
## Änderung des Niedersächsischen Spielbankengesetzes

Das Niedersächsische Spielbankengesetz vom 16. Dezember 2004 (Nds. GVBl. S. 605), zuletzt geändert durch Artikel 3 des Gesetzes vom 21. Juni 2012 (Nds. GVBl. S. 190), wird wie folgt geändert:

1. Nach § 10 c wird der folgende neue § 10 d eingefügt:

„§ 10 d
Zulassungsinhaber als Verantwortlicher bei der Verarbeitung personenbezogener Daten

Soweit dieses Gesetz, sonstiges Landesrecht oder Bundesrecht dem Zulassungsinhaber Zwecke und Mittel der Verarbeitung von personenbezogenen Daten vorgeben, ist der Zulassungsinhaber Verantwortlicher nach Artikel 4 Nr. 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/45/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72).“

2. Der bisherige § 10 d wird § 10 e.

3. In § 11 Nr. 11 wird die Verweisung „§ 10 d Abs. 2 und 3“ durch die Verweisung „§ 10 e Abs. 2 und 3“ ersetzt.

## Artikel 11
## Änderung des Gesetzes über das Leichen-, Bestattungs- und Friedhofswesen

Das Gesetz über das Leichen-, Bestattungs- und Friedhofswesen vom 8. Dezember 2005 (Nds. GVBl. S. 381) wird wie folgt geändert:

1. § 6 Abs. 4 wird wie folgt geändert:

   a) Satz 2 wird gestrichen.

b) Der bisherige Satz 3 wird Satz 2 und wie folgt geändert:

Die Angabe „oder 2“ wird gestrichen.

2. In § 18 Abs. 1 Nr. 9 wird die Angabe „§ 6 Abs. 4 Satz 3“ durch die Angabe „§ 6 Abs. 4 Satz 2“ ersetzt.

## Artikel 12
## Änderung des Niedersächsischen Gesetzes über Hilfen und Schutzmaßnahmen für psychisch Kranke

Das Niedersächsische Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke vom 16. Juni 1997 (Nds. GVBl. S. 272), zuletzt geändert durch Artikel 1 des Gesetzes vom 21. September 2017 (Nds. GVBl. S. 300), wird wie folgt geändert:

1. § 32 erhält folgende Fassung:

„§ 32
Datenverarbeitung

(1) Auf die Verarbeitung personenbezogener Daten im Rahmen dieses Gesetzes finden ergänzend 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) die Vorschriften des Niedersächsischen Datenschutzgesetzes (NDSG) Anwendung, soweit in diesem Gesetz nichts anderes bestimmt ist.

(2) Abweichend von § 6 Abs. 1 Nr. 1 NDSG dürfen personenbezogene Daten nur dann zur Erfüllung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen verarbeitet werden, wenn dies nach der Beurteilung der öffentlichen Stelle, die eine solche Befugnis wahrnimmt, erforderlich ist, weil sie ihre Aufgabe sonst nicht oder nur mit unverhältnismäßigem Aufwand auf andere Weise, insbesondere mit anonymisierten Daten, erfüllen kann.“

2. § 33 erhält folgende Fassung:

„§ 33
Besonders schutzwürdige Daten

[1]Besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung und andere personenbezogene Daten, die einem Berufsgeheimnis oder einem besonderen Amtsgeheimnis unterfallen, dürfen von den Stellen, die Aufgaben nach diesem Gesetz wahrnehmen, zur Erfüllung ihrer jeweiligen Aufgaben verarbeitet werden. [2]Der Sozialpsychiatrische Dienst oder die an Schutzmaßnahmen beteiligten Stellen dürfen die in Satz 1 genannten Daten für andere Zwecke verarbeiten, wenn

1. die betroffene Person eingewilligt hat,
2. ein Gesetz dies vorschreibt oder
3. eine Lebensgefahr oder eine Gefahr für die körperliche Unversehrtheit nicht anders abgewendet werden kann.

[3]Eine Übermittlung an das Betreuungsgericht, an das Familiengericht, an die Betreuungsstelle oder an eine gesetzliche Vertreterin oder einen gesetzlichen Vertreter ist darüber hinaus zulässig, soweit dies für die Unterbringung nach diesem Gesetz oder für die gesetzliche Vertretung erforderlich ist. [4]§ 15 NDSG gilt entsprechend.“

3. § 35 wird gestrichen.

4. § 36 erhält folgende Fassung:

„§ 36
Auskunft

[1]Der Anspruch auf Auskunft über die nach diesem Gesetz gespeicherten personenbezogenen Daten kann durch die Auskunft einer Ärztin oder eines Arztes erfüllt werden. [2]Die Erteilung einer Auskunft kann über § 8 Abs. 2 NDSG hinaus auch abgelehnt werden, soweit der Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen gefährdet werden würde.“

## Artikel 13
## Änderung des Niedersächsischen Maßregelvollzugsgesetzes

Das Niedersächsische Maßregelvollzugsgesetz vom 1. Juni 1982 (Nds. GVBl. S. 131), zuletzt geändert durch Artikel 1 des Gesetzes vom 12. Mai 2015 (Nds. GVBl. S. 82), wird wie folgt geändert:

1. § 21 a erhält folgende Fassung:

„§ 21 a
Datenverarbeitung

(1) [1]Auf die Verarbeitung personenbezogener Daten einschließlich der Daten, die aus der Überwachung der Besuche, des Postverkehrs und der Telekommunikation gewonnen werden, findet ergänzend 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. 119 S. 1, Nr. L 314 S. 72) das Niedersächsische Datenschutzgesetz (NDSG) Anwendung, soweit in diesem Gesetz nichts anderes bestimmt ist. [2]§ 15 NDSG gilt entsprechend.“

2. Nach § 21 a wird der folgende neue § 21 b eingefügt:

„§ 21 b
Besonders schutzwürdige Daten

Besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung und andere personenbezogene Daten, die einem Berufsgeheimnis oder einem besonderen Amtsgeheimnis unterfallen, dürfen von den Stellen, die Aufgaben nach diesem Gesetz wahrnehmen, zur Erfüllung ihrer jeweiligen Aufgaben verarbeitet werden.“

3. Der bisherige § 21 b wird § 21 c und wie folgt geändert:

a) In der Überschrift werden die Worte „und Akteneinsicht“ gestrichen.

b) Der einleitende Satzteil erhält folgende Fassung:

„Die Erteilung einer Auskunft kann über § 8 Abs. 2 NDSG hinaus auch abgelehnt werden, soweit und solange der Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen gefährdet werden würde“.

c) In Nummer 2 werden die Worte „oder Akteneinsicht“ gestrichen.

## Artikel 14
## Änderung des Niedersächsischen Schulgesetzes

§ 31 des Niedersächsischen Schulgesetzes in der Fassung vom 3. März 1998 (Nds. GVBl. S. 137), zuletzt geändert durch Gesetz vom 16. August 2017 (Nds. GVBl. S. 260), wird wie folgt geändert:

1. Dem Absatz 1 wird der folgende Satz 3 angefügt:

„[3]In Absatz 2 Satz 3 genannte personenbezogene Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten dürfen

1. den Agenturen für Arbeit zum Zwecke der Berufsberatung nach § 30 des Dritten Buchs des Sozialgesetzbuchs,

2. den Trägern der Jugendhilfe zum Zwecke des Angebots

   a) sozialpädagogischer Hilfen nach § 13 Abs. 1 des Achten Buchs des Sozialgesetzbuchs (SGB VIII) oder

   b) geeigneter sozialpädagogisch begleiteter Ausbildungs- und Beschäftigungsmaßnahmen nach § 13 Abs. 2 SGB VIII, auch in Verbindung mit § 27 Abs. 3 Satz 2 SGB VIII, auch in Verbindung mit § 41 Abs. 2 SGB VIII

   sowie

3. den Trägern der Grundsicherung für Arbeitsuchende nach § 6 des Zweiten Buchs des Sozialgesetzbuchs (SGB II) zum Zwecke der Beratung und der Eingliederung in Ausbildung nach § 1 Abs. 3 SGB II sowie zum Zwecke der Wahrnehmung der Aufgaben nach § 4 Abs. 2 SGB II

übermittelt werden, soweit dies für die Wahrnehmung der jeweiligen Aufgabe erforderlich ist.“

2. Es werden die folgenden neuen Absätze 2 und 3 eingefügt:

„(2) [1]Die Meldebehörde der alleinigen Wohnung oder der Hauptwohnung übermittelt den Grundschulen zum Zwecke der Gewährleistung der Erfüllung der Schulpflicht personenbezogene Daten der im jeweiligen Schulbezirk gemeldeten Kinder, deren Schulpflicht nach § 64 Abs. 1 Satz 1 im folgenden Jahr beginnt, sowie der gesetzlichen Vertreter dieser Kinder. [2]Satz 1 gilt entsprechend in Bezug auf die Kinder, die nach der Übermittlung nach Satz 1 und vor dem Beginn der Schulpflicht nach § 64 Abs. 1 Satz 1 durch Umzug innerhalb der Gemeinde den Schulbezirk wechseln oder in die Gemeinde zuziehen. [3]Zu übermitteln sind folgende personenbezogene Daten:

1. zum Kind

   a) Familienname,

   b) Vornamen unter Kennzeichnung des gebräuchlichen Vornamens,

   c) Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,

   d) Geschlecht,

2. zu den gesetzlichen Vertreterinnen oder Vertretern

   a) Familienname,

   b) Vornamen,

   c) Anschrift,

   d) Auskunftssperren nach § 51 des Bundesmeldegesetzes und bedingte Sperrvermerke nach § 52 des Bundesmeldegesetzes.

(3) [1]Wechselt eine schulpflichtige Schülerin oder ein schulpflichtiger Schüler die Schule innerhalb Niedersachsens, so übermittelt die abgebende Schule der aufnehmenden Schule die in Absatz 2 Satz 3 genannten personenbezogenen Daten der Schülerin oder des Schülers und der gesetzlichen Vertreterinnen oder Vertreter. [2]Die aufnehmende Schule übermittelt der abgebenden Schule die Aufnahmeentscheidung. [3]Bis zur Übermittlung der Aufnahmeentscheidung durch die aufnehmende Schule obliegt der abgebenden Schule die Gewährleistung der Erfüllung der Schulpflicht. [4]Zieht eine Person, deren Schulpflicht nach § 64 Abs. 1 Satz 1 begonnen hat und die das 18. Lebensjahr noch nicht vollendet hat, aus einem anderen Bundesland oder dem Ausland zu, so über-

mittelt die Meldebehörde der alleinigen Wohnung oder der Hauptwohnung der Schulbehörde die in Absatz 2 Satz 3 genannten personenbezogenen Daten dieser Person und der gesetzlichen Vertreterinnen oder Vertreter zum Zwecke der Gewährleistung der Erfüllung der Schulpflicht.“

3. Der bisherige Absatz 2 wird Absatz 4.

4. Der bisherige Absatz 3 wird gestrichen.

5. Der bisherige Absatz 4 wird Absatz 5.

## Artikel 15
## Änderung des Niedersächsischen Bodenschutzgesetzes

§ 13 des Niedersächsischen Bodenschutzgesetzes vom 19. Februar 1999 (Nds. GVBl. S. 46), zuletzt geändert durch Artikel 10 des Gesetzes vom 5. November 2004 (Nds. GVBl. S. 417), wird wie folgt geändert:

1. Satz 2 erhält folgende Fassung:

   „[2]Die zuständige Behörde kann von anderen öffentlichen Stellen die Übermittlung personenbezogener Daten verlangen, die zur Führung des Altlastenverzeichnisses erforderlich sind, auch wenn diese Daten von den anderen öffentlichen Stellen zu einem anderen Zweck erhoben wurden. “

2. Satz 4 wird gestrichen.

## Artikel 16
## Inkrafttreten

[1]Dieses Gesetz tritt am 25. Mai 2018 in Kraft. [2]Gleichzeitig tritt das Niedersächsische Datenschutzgesetz in der Fassung vom 29. Januar 2002 (Nds. GVBl. S. 22), zuletzt geändert durch Artikel 1 des Gesetzes vom 12. Dezember 2012 (Nds. GVBl. S. 589), außer Kraft.

## Begründung

### A. Allgemeiner Teil

### I. Anlass, Ziele und Schwerpunkte des Entwurfs

Am 25. Mai 2016 ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) – im Folgenden: DSGVO – in Kraft getreten. Gemäß ihrem Artikel 99 Abs. 2 gilt sie ab dem 25. Mai 2018.

Gemäß Artikel 288 des Vertrages über die Arbeitsweise der Europäischen Union gelten EU-Verordnungen unmittelbar und bedürfen keiner Umsetzung in das mitgliedstaatliche Recht. Nichtsdestotrotz enthält die Datenschutz-Grundverordnung sogenannte Öffnungsklauseln für den nationalen Gesetzgeber mit Regelungsoptionen und konkreten Regelungsaufträgen. Der sich daraus ergebende Anpassungsbedarf soll mit diesem Gesetz umgesetzt werden.

Wiederholungen von Regelungen der Datenschutz-Grundverordnung dürfen im nationalen Recht nur insoweit erfolgen, als dass im Fall von Präzisierungen oder Einschränkungen von Regelungen der Datenschutz-Grundverordnung durch das nationale Recht diese erforderlich sind, um die Kohärenz zu wahren und die Vorschriften des nationalen Rechts für die Personen, für die sie gelten, verständlicher zu machen (Erwägungsgrund 8 der Datenschutz-Grundverordnung). Insoweit musste auf Wiederholungen von Regelungen der Datenschutz-Grundverordnung weitgehend verzichtet werden.

Zu Artikel 1 (Niedersächsisches Datenschutzgesetz):

Mit diesem Gesetz wird das bisherige Niedersächsische Datenschutzgesetz in einer Neufassung an die Datenschutz-Grundverordnung angepasst. Dabei sind der Datenschutz-Grundverordnung widersprechende Regelungen aufzuheben, gleichlautende Vorschriften grundsätzlich ebenfalls aufzuheben und Regelungsaufträge zu erfüllen. Darüber hinaus werden Regelungsoptionen so genutzt, dass der bisherige Datenschutzstandard des Landes Niedersachsen aufrecht erhalten werden kann, insbesondere was die materiellen Anforderungen an die Datenverarbeitung betrifft.

Wegen der grundlegenden strukturellen Änderung des im Bereich des Schutzes des Rechts auf informationelle Selbstbestimmung anzuwendenden Rechts ist eine bloße Änderung des Niedersächsischen Datenschutzgesetzes nicht opportun. Mit der Neufassung soll der Systemwechsel im Datenschutzrecht deutlich gemacht werden. Die Datenschutz-Grundverordnung ist unmittelbar in den Mitgliedstaaten anzuwenden. Das Niedersächsische Datenschutzgesetztrifft künftig nur noch ergänzende Regelungen zur Datenschutz-Grundverordnung.

Zu Artikel 3 (Niedersächsisches Mediengesetz):

Nach der ab 25. Mai 2018 europaweit unmittelbar geltenden 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 L 119 S. 1) haben die Mitgliedstaaten gem. Artikel 85 der Verordnung das Recht auf den Schutz personenbezogener Daten in Einklang zu bringen mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken. Dafür gesteht Artikel 85 Absatz 2 Datenschutz-Grundverordnung weitreichende Abweichungsbefugnisse vom Regelungsgehalt der Grundverordnung zu. Die Änderungen dienen der Anpassung der Vorschriften an die neuen europarechtlichen Vorgaben. Die Länder haben zu diesem Zweck eine parallel in der Beratung befindliche Änderung des Rundfunkstaatsvertrags erarbeitet. In einem neuen § 9c werden dort das Datengeheimnis und das Medienprivileg einheitlich für den öffentlich-rechtlichen und den privaten Rundfunk geregelt. Hinzu kommen in § 57 Regelungen über die Datenverarbeitung zu journalistischen Zwecken, soweit öffentlich-rechtliche oder private Rundfunkveranstalter oder Presseunternehmen als Anbieter von Telemedien agieren. Für die davon nicht erfassten, weiteren und vergleichbaren Telemedienanbieter wird das Medienprivileg im neugefassten § 54 festgeschrieben.

Vor allem die journalistische Arbeit ist mit den Anforderungen der Grundverordnung nicht vollends in Einklang zu bringen. Die Verpflichtung zum Schutz des Rechts auf freie Meinungsäußerung erfordert es, Abweichungen zu regeln. Der Schutzbereich der Pressefreiheit ist grundsätzlich weit und reicht von der Informationsbeschaffung über die Informationsbearbeitung bis hin zur Informationsverbreitung. Dies soll auch für Anbieter von Telemedien gelten, die Rundfunkveranstaltern oder Presseunternehmen vergleichbar sind. Rundfunk, Presse und vergleichbare Anbieter von Telemedien sind bei Erfüllung ihrer verfassungsrechtlich verbürgten Aufgabe bei der öffentlichen und individuellen Meinungsbildung zwingend auf die Verwendung personenbezogener Daten angewiesen. Einflüsse von außen auf diese Daten müssen deshalb so weit wie möglich von vornherein vermieden werden. Das Medienprivileg soll verhindern, dass der Datenschutz der freien journalistischen Tätigkeit entgegensteht. Geschützt werden

hierdurch nicht nur die Journalisten, sondern auch Informanten und sonstige Betroffene. Erfasst wird insbesondere auch der Schutz der Quellen der Journalisten und die Speicherung und sonstige Verarbeitung personenbezogener Daten, etwa in Redaktions- oder Nachrichtenarchiven.

Die Vorschriften entsprechen im Regelungsinhalt und in der Satzfolge weitgehend den neuen Regelungen in § 57 Rundfunkstaatsvertrag, um einen größtmöglichen Gleichlauf zu erreichen. Soweit der Gesetzentwurf davon abweicht, ist dies das Ergebnis der Einbeziehung der Arbeitsgruppe Rechtsvereinfachung als Normprüfungsstelle der Landesregierung. Für das europarechtlich notwendige Notifizierungsverfahren bei der Europäischen Kommission ist klarzustellen, dass Abweichungen zu den entsprechenden Vorschriften des Rundfunkstaatsvertrags hierin ihre Ursache finden; materiell-rechtlich sind identische Regelungsinhalte intendiert.

Im Ergebnis sind die widerstreitenden Rechtspositionen der Meinungs- und Pressefreiheit im Bereich der Telemedien einerseits und des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung andererseits durch die vorgesehenen Regelungen insgesamt im Rahmen einer Abwägung zueinander in einen sachgemäßen Ausgleich bzw. in Einklang gebracht. Die Ausnahmen sind deshalb im Interesse der Meinungs- bzw. Pressefreiheit entsprechend Artikel 85 Absatz 2 Datenschutz-Grundverordnung auch erforderlich.

Zu Artikel 4 (Niedersächsisches Pressegesetz)

Nach der ab 25. Mai 2018 europaweit unmittelbar geltenden 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 L 119 S. 1) haben die Mitgliedstaaten gem. Artikel 85 der Verordnung das Recht auf den Schutz personenbezogener Daten in Einklang zu bringen mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken. Dafür gesteht Artikel 85 Abs. 2 Datenschutz-Grundverordnung weitreichende Abweichungsbefugnisse vom Regelungsgehalt der Grundverordnung zu.

Vor allem die journalistische und literarische Arbeit ist mit den Anforderungen der Grundverordnung nicht vollends in Einklang zu bringen. Die Verpflichtung zum Schutz des Rechts auf freie Meinungsäußerung erfordert es, Abweichungen zu regeln. Der Schutzbereich der Pressefreiheit ist grundsätzlich weit und reicht von der Informationsbeschaffung über die Informationsbearbeitung bis hin zur Informationsverbreitung. Die Presse ist bei Erfüllung ihrer verfassungsrechtlich verbürgten Aufgabe bei der öffentlichen und individuellen Meinungsbildung zwingend auf die Verwendung personenbezogener Daten angewiesen. Journalistische Arbeit,

vor allem auch eine verdeckte Recherche, wäre nicht möglich ohne die Möglichkeit, personenbezogene Daten auch ohne Einwilligung der betroffenen Personen zu erheben, zu speichern und zu nutzen. Entsprechendes gilt, wenn den betroffenen Personen konkrete Auskunfts- und daraus folgende Berichtigungsansprüche zu nicht veröffentlichten redaktionellen Daten eingeräumt würden. Einflüsse von außen auf diese Daten müssen deshalb so weit wie möglich von vornherein vermieden werden. Das Medienprivileg soll verhindern, dass der Datenschutz der freien journalistischen Tätigkeit entgegensteht. Geschützt werden hierdurch nicht nur die Journalisten, sondern auch Informanten und sonstige Betroffene. Erfasst wird insbesondere auch der Schutz der Quellen der Journalisten und die Speicherung und sonstige Verarbeitung personenbezogener Daten, etwa in Redaktions- oder Nachrichtenarchiven.

Ziel ist es, unter der Geltung der Datenschutz-Grundverordnung die Pressefreiheit unter dem Gesichtspunkt des Datenschutzes im bisherigen Umfang zu gewährleisten. Hierfür sieht der Gesetzentwurf mehrere Regelungen vor.

Die Vorschriften entsprechen im Regelungsinhalt und in der Satzfolge weitgehend den neuen Regelungen in § 9c Rundfunkstaatsvertrag, um einen größtmöglichen Gleichlauf der Vorschriften für den Rundfunk und die Presse zu erreichen. Die Länder waren im Vorfeld auch um eine weitgehende sprachliche Angleichung der jeweiligen landesrechtlichen Ergänzungen in den Landespressegesetzen bemüht. Soweit der Gesetzentwurf davon abweicht, ist dies das Ergebnis der Einbeziehung der Arbeitsgruppe Rechtsvereinfachung als Normprüfungsstelle der Landesregierung. Für das europarechtlich notwendige Notifizierungsverfahren bei der Europäischen Kommission ist klarzustellen, dass Abweichungen zu den entsprechenden Vorschriften des Rundfunkstaatsvertrags und denen anderer Landespressegesetze hierin ihre Ursache finden; materiell-rechtlich sind identische Regelungsinhalte intendiert.

Im Ergebnis sind die widerstreitenden Rechtspositionen der Meinungs- und Pressefreiheit einerseits und des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung andererseits durch die vorgesehenen Regelungen insgesamt im Rahmen einer Abwägung zueinander in einen sachgemäßen Ausgleich bzw. in Einklang gebracht. Die Ausnahmen sind deshalb im Interesse der Meinungs- bzw. Pressefreiheit entsprechend Artikel 85 Absatz 2 Datenschutz-Grundverordnung auch erforderlich.

Zu Artikel 5 (Niedersächsisches Ausführungsgesetz zum Bundesmeldegesetz):

Mit der Datenschutz-Grundverordnung sollen die Regelungen für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen unionsweit verein-

heitlicht werden. Auch in melderechtlicher Hinsicht folgt hieraus Anpassungsbedarf. Das Niedersächsische Ausführungsgesetz zum Bundesmeldegesetz (Nds. AG BMG) ist zu ändern und insbesondere in terminologischer Hinsicht an die Verordnung (EU) 2016/679 anzupassen.

Zu Artikel 10 (Änderung des Niedersächsischen Spielbankengesetzes):

Auch das NSpielbG ist anlässlich der am 25. Mai 2018 unmittelbar wirksam werdenden Verordnung (EU) 2016/679 anzupassen.

Durch die Regelung im NSpielbG wird die Bindung des Zulassungsinhabers als juristische Person des Privatrechts an die maßgeblichen Vorgaben der Datenschutz-Grundverordnung sowie an deren weitere Umsetzung durch das Bundesdatenschutzgesetz sichergestellt.

Zu Artikel 14 (Niedersächsisches Schulgesetz):

Der Gesetzentwurf dient der Umsetzung bildungspolitischer Ziele der Landesregierung im Hinblick auf die Stärkung der Berufsorientierung und die bessere Verzahnung von Berufsorientierungsmaßnahmen im Rahmen koordinierter Beratungsstrukturen. Insbesondere soll die gesetzliche Grundlage für eine Übermittlung der personenbezogenen Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten an die am Übergang von der Schule in den Beruf beteiligten Agenturen für Arbeit, die Träger der Jugendhilfe sowie die Träger der Grundsicherung für Arbeitsuchende geschaffen werden. Auf diese Weise sollen die vorgenannten Behörden in die Lage versetzt werden, insbesondere im Rahmen einer koordinierten und intensivierten Zusammenarbeit ihren gesetzlichen Aufgaben in Bezug auf die Durchführung von Maßnahmen am Übergang von der Schule in den Beruf nachkommen zu können.

Neu geschaffen wird ferner die Rechtsgrundlage für die Übermittlung personenbezogener Daten zur Überwachung der Schulpflicht der Schülerinnen und Schüler.

Des Weiteren wird das Niedersächsische Schulgesetz an die durch das Inkrafttreten der Verordnung (EU) 2016/679 neue Rechtslage angepasst.

## II. Wesentliche Ergebnisse der Gesetzesfolgenabschätzung

Zu Artikel 1:

Die Neufassung des Niedersächsischen Datenschutzgesetzes ist erforderlich, da ab dem 25. Mai 2018 die Datenschutz-Grundverordnung gelten wird, die in den Mitgliedstaaten unmittelbare Wirkung haben wird. Das Recht in den Mitgliedstaaten muss zu diesem Zeitpunkt der Datenschutz-Grundverordnung angepasst sein, d. h. es darf keine der Datenschutz-Grundverordnung entgegenstehende Vorschriften und grundsätzlich auch keine mit der Datenschutz-Grundverordnung identische Vorschriften enthalten. Darüber hinaus enthält die Datenschutz-Grundverordnung Regelungsaufträge und Regelungsoptionen für die Mitgliedstaaten, die mit dem neuen Niedersächsischen Datenschutzgesetz umgesetzt wurden.
Das bisherige Niedersächsische Datenschutzgesetz ist zu dem oben genannten Zeitpunkt aufzuheben und das neue Niedersächsische Datenschutzgesetz in Kraft zu setzen. Zur Rechtsform eines Gesetzes besteht keine Regelungsalternative. Das neue Niedersächsische Datenschutzgesetz beinhaltet - wie auch das bisherige Niedersächsische Datenschutzgesetz - Eingriffe in das grundrechtlich verankerte Recht auf informationelle Selbstbestimmung, insbesondere durch eine Einschränkung der Betroffenenrechte. Somit greift der Parlamentsvorbehalt.

Die Finanzfolgenabschätzung ergibt, dass durch dieses Gesetz keine Kosten entstehen. Soweit durch die Datenschutzreform der EU neue Anforderungen und Instrumentarien eingeführt wurden, die Kosten verursachen könnten, ergeben sich diese unmittelbar aus der Datenschutz-Grundverordnung. Durch die Regelungen des neuen Niedersächsischen Datenschutzgesetzes werden keine Mehrkosten gegenüber dem bisherigen Niedersächsischen Datenschutzgesetz verursacht. Auch wird von Regelungsoptionen der Datenschutz-Grundverordnung nicht in der Weise Gebrauch gemacht, dass gegenüber den Kostenfolgen der Datenschutz-Grundverordnung Mehrkosten entstehen würden.

Zu Artikel 5:

Die Änderung des Niedersächsischen Ausführungsgesetzes zum Bundesmeldegesetz (Nds. AG BMG) wird weder in rechtlicher noch in praktischer Hinsicht bedeutende Veränderungen nach sich ziehen. Die Änderungen dienen einer Anpassung des Gesetzestextes an die begrifflichen Bestimmungen der Verordnung (EU) 2016/679. Darüber hinaus erfolgen eine Präzisierung des Gesetzestextes in sprachlicher Hinsicht und eine Anpassung an die Neufassung des

Niedersächsischen Kommunalabgabengesetzes. § 9 Nds. AG BMG kommt lediglich eine klarstellende Funktion ohne Regelungsgehalt zu. Die Streichung dient dem Gebot der Normenklarheit und den Bestrebungen des Bürokratieabbaus.

Zu Artikel 14:
Um in das in Artikel 2 Abs. 1 GG i.V.m. Artikel 1 Abs. 1 GG verankerte Grundrecht auf informationelle Selbstbestimmung eingreifen zu können und die erforderlichen Daten verarbeiten zu dürfen, bedarf es nach dem Parlamentsvorbehalt einer gesetzlichen Grundlage. Alternativ wäre die Durchführung von Berufsorientierungsmaßnahmen insbesondere im Rahmen koordinierter Beratungsstrukturen nicht vollumfänglich entsprechend dem Grundsatz „Niemand darf verloren gehen“ zu gewährleisten. Auch wären die Voraussetzungen für eine lückenlose Überwachung der Schulpflicht alternativ nicht gegeben.

## III. Auswirkungen auf die Umwelt, den ländlichen Raum und die Landesentwicklung sowie auf die Verwirklichung der Gleichstellung von Frauen und Männern und Familien und Menschen mit Behinderungen

Der Gesetzentwurf hat keine diesbezüglichen Auswirkungen.

## IV. Voraussichtliche Kosten und haushaltsmäßige Auswirkungen des Entwurfs

Der Gesetzentwurf verursacht keine Kosten und hat keine haushaltsmäßigen Auswirkungen.

## VII. Beteiligung von Verbänden und Organisationen

*Äußerungen der Beteiligten:*

## B. Besonderer Teil

### Zu Artikel 1 (Niedersächsisches Datenschutzgesetz)

#### Zu Abschnitt 1 (Allgemeines):
#### Zu § 1 (Regelungsgegenstand und Anwendungsbereich des Gesetzes)

Zu Absatz 1:
Regelungsgegenstand des Gesetzes ist es, zur Durchführung der Datenschutz-Grundverordnung (DSGVO) ergänzende Regelungen zu treffen. Durch diese Formulierung soll für die Anwenderinnen und Anwender des Gesetzes sowie die betroffenen Personen deutlich gemacht werden, dass zunächst die Datenschutz-Grundverordnung unmittelbar anzuwenden ist und dieses Gesetz lediglich ergänzende Regelungen enthält.
Wie im bisherigen Niedersächsischen Datenschutzgesetzsoll das Gesetz gemäß Satz 1 Nummer 1 im Anwendungsbereich der Datenschutz-Grundverordnung für alle öffentlichen Stellen des Landes Niedersachsen, für die Kommunen sowie die sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und deren Vereinigungen gelten, soweit diese personenbezogene Daten verarbeiten. Nach Nummer 2 gilt das Gesetz auch für Personen und Stellen außerhalb des öffentlichen Bereichs, soweit ihnen Aufgaben der öffentlichen Verwaltung übertragen sind. Dies war im bisherigen Recht auch bereits so und wird hier ausdrücklich berücksichtigt, um eine vollständige Aufzählung zu erhalten.
Im Anschluss an die Aufzählung der Behörden wird der Bezug hergestellt zum sachlichen Anwendungsbereich der Datenschutz-Grundverordnung (Fall 1) bzw. zur erweiterten Anwendung der Datenschutz-Grundverordnung nach § 2 (Fall 2). Mit dem Verweis auf § 2 wird klargestellt, dass für die Verarbeitungen personenbezogener Daten, die nicht in den Anwendungsbereich des Unionsrechts im Sinne des Artikels 2 Abs. 2 Buchst. a DSGVO fallen, in diesem Gesetz ebenfalls Regelungen getroffen werden.
Satz 2 entspricht § 1 Abs. 1 Satz 2 der bisherigen Fassung des Niedersächsischen Datenschutzgesetzes.

Zu Absatz 2:
Absatz 2 sieht für Gerichte und Behörden der Staatsanwaltschaft eine Ausnahme von der Anwendbarkeit des Niedersächsischen Datenschutzgesetzes vor, soweit diese keine Verwaltungsaufgaben wahrnehmen. Dass auch Gerichte vollumfänglich der Datenschutz-Grundverordnung unterliegen, folgt aus dem Umkehrschluss des Artikel 55 Abs. 3 DSGVO, wonach die Aufsichtsbehörden nicht für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen

Tätigkeit vorgenommenen Verarbeitungen zuständig sind. Für die justiziellen Aufgaben wird die Datenschutz-Grundverordnung durch das Bundesdatenschutzgesetz und ggf. speziellere bundesrechtliche Regelungen ergänzt.

Zu Absatz 3:
Die Ausnahmeregelung für den Landtag wurde in der Systematik der Vorschrift dem Wortlaut des Absatzes 2 angeglichen. Die Geltung des Niedersächsischen Datenschutzgesetzes für Verwaltungsaufgaben wird nunmehr positiv angeordnet. Sie entspricht im Ergebnis jedoch inhaltlich der bisherigen Regelung des § 2 Abs. 2 NDSG. Parlamentarische Aufgaben fallen nach Artikel 2 Abs. 2 a) DSGVO nicht in den Anwendungsbereich der Datenschutz-Grundverordnung. Für die Wahrnehmung parlamentarischer Aufgaben gilt wie bisher die vom Landtag erlassene Datenschutzordnung.

Zu Absatz 4:
Die Regelung entspricht dem bisherigen § 2 Abs. 3 NDSG. Die Datenverarbeitung der in Absatz 4 benannten Stellen zu wirtschaftlichen Zwecken unterliegt nicht den Regelungen für öffentliche Stellen. Für den Bereich der wirtschaftlichen Tätigkeit gelten ergänzend zu den Regelungen der Datenschutz-Grundverordnung die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes bzw. die weiterer spezieller Gesetze. Dieses soll die Chancengleichheit im Wettbewerb sichern.
Zu der Nummer 2 zählen die Eigenbetriebe gemäß § 136 Abs. 2 Nr. 1 NKomVG. Nummer 3 erfasst die öffentlichen Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe (vgl. § 140 NKomVG) geführt werden.
Die im bisherigen § 2 Abs. 3 für anwendbar erklärten Regelungen der §§ 8, 19 und 26 finden sich in der unmittelbar geltenden Datenschutz-Grundverordnung wieder. Soweit die genannten Stellen personenbezogene Daten nicht für wirtschaftliche Zwecke verarbeiten, gilt ergänzend zur Datenschutz-Grundverordnung dieses Gesetz. Dies betrifft beispielsweise die Personaldatenverarbeitung. Diese erfolgt auf Grundlage von § 13 dieses Gesetzes.

Zu Absatz 5:
Die Regelung entspricht dem bisherigen § 2 Abs. 4 NDSG. Für öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten sowie deren Vereinigungen gelten § 10 und im Übrigen ergänzend zu den Regelungen der Datenschutz-Grundverordnung die für nichtöffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes bzw. die weiterer spezieller Gesetze.

Zu Absatz 6:
Die Regelung zur Spezialität wie im bisherigen § 2 Abs. 6 wird zur Klarstellung aufrechterhalten.

Eine Regelung vergleichbar dem bisherigem § 1 (Aufgabe des Gesetzes) kann nicht aufrechterhalten werden. Die Aufgabe dieses (Ergänzungs)Gesetzes kann keine andere sein, als die der Datenschutz-Grundverordnung. Im Gegensatz zum bisherigen Niedersächsischen Datenschutzgesetz hat die Datenschutz-Grundverordnung neben dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten auch den freien Datenverkehr zum Gegenstand (vgl. Artikel 1 Abs. 3, sowie Titel der Datenschutz-Grundverordnung). Die Regelungen in den Absätzen 5, 7 und 8 der bisherigen Fassung des § 2 NDSG werden ebenfalls nicht übernommen. Absatz 5 regelte die Geltung des Rechts des jeweiligen Sitzlandes für öffentlich-rechtliche Rundfunkanstalten. Diese Regelung kann und wird auch faktisch bereits an anderer Stelle getroffen. Nach § 41 Abs. 1 des Gesetzes zum Staatvertrag über den Norddeutschen Rundfunk gilt für den Datenschutz beim NDR das Hamburgische Datenschutzgesetz. Eine Klärung des Anwendungsvorrangs wie in dem bisherigen Absatz 7 ist ebenfalls entbehrlich. Eine Regelung wie im bisherigen § 2 Absatz 8 zum Begnadigungsverfahren entfällt an dieser Stelle; diesbezügliche Vorschriften befinden sich nunmehr in § 2 Nr. 2 b) und § 17 dieses Gesetzes.

**Zu § 2 (Erweiterte Anwendung der Datenschutz-Grundverordnung):**

Dem Anwendungsbereich der Datenschutz-Grundverordnung unterfallen nicht alle Bereiche der Verarbeitung personenbezogener Daten durch öffentliche Stellen.

Dem Anwendungsbereich der Verordnung (EU) 2016/679 unterfallen alle ganz oder teilweise automatisierten Verarbeitungen personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert werden. Damit unterfallen dem Anwendungsbereich neben der elektronischen Datenverarbeitung auch die Verarbeitung personenbezogener Daten in Papierakten, wenn diese einer gewissen Ordnung, z.B. nach einem Aktenplan, unterliegen. Nicht vom Anwendungsbereich der Verordnung (EU) 2016/679 erfasst ist hingegen die Datenverarbeitung in Akten oder Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind (vgl. Artikel 2 Absatz 1 der Verordnung (EU) 2016/679, Erwägungsgrund 15 der Verordnung (EU) 2016/679).

Nummer 1 sieht daher vor, dass die Regelungen der Datenschutz-Grundverordnung abweichend von Artikel 2 Abs. 1 DSGVO auch für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem weder gespeichert sind noch gespeichert werden sollen, gelten. Mit dieser Regelung sollen alle ausschließlich in Papierform gespeicherten personenbezogenen Daten, welche nicht dem Anwendungsbereich der Datenschutz-Grundverordnung unterfallen, dem allgemein geltenden Datenschutzregime unterworfen werden. Soweit in Papierform geführte Unterlagen von Behörden und öffentlichen Stellen zum Zweck der Auffindbarkeit und Auswertbarkeit registriert und damit „nach bestimmten Kriterien geordnet“ werden, gilt für diese Datenverarbeitungen die Datenschutz-Grundverordnung unmittelbar (vgl. Erwägungsgrund 15 zur Datenschutz-Grundverordnung). Mit § 2 Nummer 1 soll sichergestellt werden, dass auch für Daten in sonstigen Akten die allgemeinen Datenschutzvorschriften gelten.

Nummer 2 bestimmt die erweiterte Anwendung der Datenschutz-Grundverordnung und des Niedersächsischen Datenschutzgesetzes auch für die Bereiche, die nicht in den Anwendungsbereich des Unionsrechts im Sinne des Artikels 2 Abs. 2 Buchst. a DSGVO fallen. Nummer 2 Buchst. a nennt die Verarbeitungen personenbezogener Daten zum Zweck der Vorbereitung öffentlicher Auszeichnungen und Ehrungen, soweit in § 13 nichts anderes bestimmt ist, Buchstabe b nennt die Verarbeitungen personenbezogener Daten in Begnadigungsverfahren, soweit in § 14 Satz 2 nichts anderes bestimmt ist, und Buchstabe c) nennt die Verarbeitung personenbezogener Daten im Rahmen einer sonstigen nicht in den sachlichen Anwendungsbereich des Unionsrecht fallenden Tätigkeit, die nicht unter Artikel 2 Abs. 2 Buchst. b bis d DSGVO fällt (z. B. Tätigkeiten des Verfassungsschutzes), soweit die Datenverarbeitung durch Rechtsvorschrift nicht speziell geregelt ist. Mit dieser Regelung sollen mögliche Gesetzeslücken vermieden werden, sodass keine Bereiche entstehen können, für die keine datenschutzrechtlichen Regelungen gelten.

Damit wird auch für solche Bereiche sichergestellt, dass im Grundsatz die für alle öffentlichen Stellen geltenden allgemeinen Rechtsvorschriften zur Anwendung kommen. Ausnahmen hierzu sind in diesem Gesetz in den §§ 13 und 14 geregelt. Darüber hinaus sind Abweichungen wie bisher spezialgesetzlich zu regeln.

**Zu Abschnitt 2 (Rechtsgrundlagen der Datenverarbeitung):**

Die allgemeinen Regelungen zur Zulässigkeit der Verarbeitung personenbezogener Daten durch die öffentlichen Stellen im Land Niedersachsen finden sich zukünftig in Artikel 6 Abs. 1 DSGVO. Dies entspricht im Wesentlichen dem bisherigen § 4 Abs. 1 i.V.m. §§ 9 ff. NDSG.

Nach Artikel 6 Abs. 2, Abs. 3 i. V. m. Abs. 1 Satz 1 Buchstaben c) und e) DSGVO haben die Mitgliedstaaten Regelungsbefugnisse bzw. Gestaltungsspielräume in dem dort genannten Umfang. Eine weitere Regelungsbefugnis besteht im Hinblick auf die Datenverarbeitung zu anderen Zwecken gemäß Artikel 6 Abs. 4 Fall 2 DSGVO.

**Zu § 3 (Zulässigkeit der Verarbeitung personenbezogener Daten):**

Mit § 3 wird eine Rechtsgrundlage für die Datenverarbeitung auf der Grundlage von Artikel 6 Abs. 1 Buchstabe e) i.V.m. Artikel 6 Abs. 2, Abs. 3 Satz 1 DSGVO geschaffen. Dies ist rechtlich notwendig, da Artikel 6 Abs. 1 Buchstabe e) DSGVO selbst keine Rechtsgrundlage für die Verarbeitung von Daten schafft, was sich aus der Formulierung in Artikel 6 Abs. 3 Satz 1 DSGVO ergibt. Der Unions- oder der nationale Gesetzgeber hat eine Rechtsgrundlage zu setzen. Diesem Regelungsauftrag wird nachgekommen.
Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nach der Vorschrift zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Die Verarbeitung personenbezogener Daten ist allerdings nicht nur auf dieser Rechtsgrundlage zulässig, sondern auch auf der Grundlage der weiteren in Artikel 6 Absatz 1 DSGVO aufgeführten Erlaubnistatbestände einschließlich der auf der Grundlage der Datenschutz-Grundverordnung erlassenen bereichsspezifischen Regelungen. So ist etwa die Zulässigkeit der Verarbeitung von Schülerdaten nach dem Schulgesetz oder von Sozialdaten abschließend im SGB X in Verbindung mit dem SGB I sowie in den übrigen Sozialgesetzbüchern geregelt. Die Einwilligung als Rechtsgrundlage der Verarbeitung personenbezogener Daten ergibt sich aus Artikel 6 Absatz 1 Satz 1 Buchstabe a) DSGVO unmittelbar.
§ 3 kann nicht als Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Abs. 1 DSGVO hereingezogen werden. Hier gelten die Regelungen des Artikels 9 Abs. 2 DSGVO.

**Zu § 4 (Erhebung personenbezogener Daten):**

Der bisher in § 9 Abs. 1 Satz 2 und 3 NDSG geregelte Grundsatz der Direkterhebung wird mit der Neufassung des Gesetzes nicht aufrechterhalten. Die Datenschutz-Grundverordnung enthält, ebenso wie die bisherige RL 95/46/EG, diesen Grundsatz nicht. Im Sinne einer Harmonisierung und der damit einhergehenden weitest gehenden 1:1-Anpassung an das EU-Recht wird auf die Beibehaltung des Grundsatzes, der mit dem bisherigen § 9 Abs. 1 Satz 3 NDSG ohnehin diverse Ausnahmen hatte, verzichtet. Materiell-rechtlich wird dieser Verzicht durch die

mit der Datenschutz-Grundverordnung in Artikel 13 und 14 eingeführten umfangreichen Informationspflichten des Verantwortlichen kompensiert.
Die Datenschutz-Grundverordnung enthält allerdings keine Regelung zur Information einer anderen Person (nicht die betroffene Person), bei der die Daten erhoben werden. Entsprechend der bisher geltenden Vorschrift (§ 9 Abs. 3 NDSG) soll eine solche Informationspflicht für Fälle der Datenverarbeitung nach § 3 Satz 1 auch zukünftig normiert werden, um auch gegenüber einer anderen Person, bei der Daten erhoben werden sollen, ein größtmögliches Maß an Transparenz herzustellen (in Anlehnung an Artikel 5 Abs. 1 Buchstabe a) DSGVO). Die Regelungsbefugnis ergibt sich aus Artikel 6 Abs. 2 und 3 der DSGVO; hier wird eine Maßnahme zur Gewährleistung einer rechtmäßigen und nach Treu und Glauben erfolgenden Verarbeitung geregelt.

**Zu § 5 (Übermittlung personenbezogener Daten):**

Zu Absatz 1:
Die Grundsätze der Datenverarbeitung sind in Artikel 5 Abs. 1 DSGVO niedergelegt. Nach Artikel 5 Abs. 2 DSGVO ist der Verantwortliche für die Einhaltung der Datenschutzgrundsätze verantwortlich und nachweispflichtig.
Entsprechend dem bisherigen Recht (§ 11 Abs. 3 NDSG) soll die Verantwortlichkeit für die Übermittlung personenbezogener Daten im Falle eines Ersuchens durch eine öffentliche Stelle auf diese übertragen werden. Die Regelungsbefugnis ergibt sich aus Artikel 6 Abs. 2, Abs. 3 DSGVO.

Zu Absatz 2:
Absatz 2 entspricht weitgehend dem bisherigen § 11 Abs. 2 NDSG. Die Regelung ist weiterhin erforderlich, da sich insbesondere bei einer aktenmäßigen Verarbeitung personenbezogener Daten nicht immer sicherstellen lässt, dass eine Trennung nach erforderlichen und nicht erforderlichen Daten mit vertretbarem Aufwand möglich ist. Nur wenn eine solche Trennung einen unvertretbaren Aufwand erzeugen würde, dürfen ausnahmsweise auch nicht für den konkreten Zweck erforderliche Daten übermittelt werden. In diesem Falle ist zusätzlich eine Abwägung mit etwaigen entgegenstehenden Belangen der betroffenen Personen vorzunehmen. Zum Schutz der Rechte der betroffenen Personen unterliegen die nicht erforderlichen Daten dem Verbot einer weiteren Verarbeitung durch die Stelle, an die die Daten übermittelt wurden. Die Regelungsbefugnis ergibt sich aus Artikel 6 Abs. 2 und 3 DSGVO; es werden die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung näher spezifiziert.

Zu Absatz 3:
Absatz 3 regelt, dass die Absätze 1 und 2 nur für Datenverarbeitungen gelten, deren Zulässigkeit sich nach § 3 Satz 1 richtet. Nur für diesen Bereich hat der nationale Gesetzgeber Regelungsbefugnisse nach Artikel 6 Abs. 2 und Abs. 3 DSGVO, die er in einem allgemeinen Gesetz nutzen kann.

**Zu § 6 (Zweckbindung, Zweckänderung):**

Diese Vorschrift enthält die zur Anwendung der Datenschutz-Grundverordnung erforderlichen Ergänzungen im allgemeinen Recht im Hinblick auf den Grundsatz der Zweckbindung (Artikel 5 Abs. 1 b) DSGVO). Sie lässt die Zulässigkeit einer Zweckänderung auf Grund einer Einwilligung (Artikel 6 Abs. 4 Fall 1 DSGVO) und die Feststellung einer zulässigen kompatiblen Zweckänderung nach Artikel 6 Abs. 4 Fall 3 DSGVO unberührt.

Im Wesentlichen erfolgen hier Regelungen über die Zweckbestimmung der Verarbeitung und die Zulässigkeit der Datenverarbeitung zu anderen Zwecken. Von der Regelung erfasst sind nicht nur die Fälle der Weiterverarbeitung zu anderen Zwecken innerhalb der verantwortlichen Stelle, sondern auch die Fälle der Datenübermittlung, soweit diese zu einem anderen als dem Erhebungszweck erfolgt und nicht auf Spezialgesetze gestützt werden kann.

Zu Absatz 1:
Der Zweck einer Datenverarbeitung durch öffentliche Stellen umfasst auch die in Nummer 1 genannten Zwecke zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung, zur Durchführung von Organisationsuntersuchungen und die in Nummer 2 genannten Zwecke zur Ausbildung und Prüfung. Abs. 1 stellt daher ähnlich wie der bisherige § 10 Abs. 3 NDSG klar, dass eine Verarbeitung zu den genannten Zwecken keine zweckändernde Datenverarbeitung ist, sondern diese Zwecke jeder Datenverarbeitung einer öffentlichen Stelle immanent sind und eine diesbezügliche Verarbeitung zulässig ist. Für Ausbildungs- und Prüfungszwecke gilt dies nach Nummer 2 jedoch nur, soweit nicht berechtigte Interessen der betroffenen Person an der Geheimhaltung der Daten überwiegen. Im Gegensatz zum bisherigen § 10 Abs. 3 Satz 2 ist ein „offensichtliches“ Überwiegen nicht mehr erforderlich, womit die Interessen der betroffenen Person gestärkt werden sollen. Insbesondere bei vervielfältigten Prüfungsaufgaben, die von einem größeren Kreis von Prüflingen bearbeitet werden, dürften in der Regel die Interessen der betroffenen Person gegenüber dem Interesse der öffentlichen Stelle überwiegen. Letztere hat dann eine Anonymisierung der personenbezogenen Daten vorzunehmen.
Unter die in Nummer 1 genannten Kontrollbefugnisse fällt auch die parlamentarische Kontrolle.

Die Befugnis für diese Regelung ergibt sich aus Artikel 6 Abs. 2 und 3 DSGVO. Danach dürfen im mitgliedstaatlichen Recht die Zwecke der Verarbeitung festgelegt werden. Dies gilt hier nur für Verarbeitungen nach § 3 Satz 1.

Zu Absatz 2:
Absatz 2 macht von dem in Artikel 6 Abs. 4 Fall 2 DSGVO eröffneten Regelungsspielraum Gebrauch. Danach dürfen die Mitgliedstaaten in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem Zweck, für den die Daten erhoben wurden, vereinbar ist, nationale Regelungen erlassen, soweit die nationale Regelung eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Abs. 1 DSGVO genannten Ziele darstellt. Daneben sind unmittelbar in Artikel 6 Abs. 4 DSGVO zulässige Zweckänderungen geregelt, insbesondere befindet sich der bisher in § 10 Abs. 2 Satz 1 Nr. 1 NDSG geregelte Fall der Einwilligung der betroffenen Person nunmehr dort (Art. 6 Abs. 4 Fall 1 DSGVO). Die im bisherigen § 10 Abs. 2 NDSG zugelassenen Zweckänderungen sollen auch zukünftig als Befugnis für die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle normiert werden, soweit dieses nach der Datenschutz-Grundverordnung weiterhin zulässig ist. Als nicht zulässig erscheint insbesondere die Aufrechterhaltung des bisherigen § 10 Abs. 2 Satz 1 Nr. 2 i.V.m. § 9 Abs. 1 Satz 3 Nr. 1 NDSG, also eine generelle Zulässigkeit einer Zweckänderung, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt. Die mitgliedstaatliche Regelungsbefugnis für die in § 6 Abs. 2 geregelten Tatbestände ergibt sich aus Artikel 6 Abs. 4 Fall 2 DSGVO i.V.m. Artikel 23 Abs. 1 DSGVO.
Im Einzelnen werden die Tatbestände des § 6 Abs. 2 im Schwerpunkt auf folgende Normen der Datenschutz-Grundverordnung gestützt:
Nummer 1: Artikel 6 Abs. 4 Fall 2 i.V.m. Artikel 23 Abs. 1 Buchstaben c) und e)
Nummer 2: Artikel 6 Abs. 4 Fall 2 i.V.m. Artikel 23 Abs. 1 Buchstabe c) und d)
Nummer 3: Artikel 6 Abs. 4 Fall 2 i.V.m. Artikel 23 Abs. 1 Buchstaben i) Fall 2
Nummer 4: Artikel 6 Abs. 4 Fall 2 i.V.m. Artikel 23 Abs. 1 Buchstabe e)

Eine Verarbeitung von personenbezogenen Daten zu einem anderen Zweck als dem, für den die Daten erhoben wurden, ist nach Nr. 1 zulässig, soweit und solange die Datenverarbeitung zur Abwehr einer unmittelbaren Gefahr für die öffentliche Sicherheit oder zur Abwehr von Nachteilen für das Wohl des Bundes oder eines Landes erforderlich ist. Das Wohl des Bundes oder eines Landes umfasst nur wesentliche Interessen dieser Gebietskörperschaften. Das sind solche, die den Bestand und die Funktionsfähigkeit des Staates betreffen. Hierzu zählt vor allem die innere oder äußere Sicherheit des Bundes oder eines Landes, ferner die freundschaftlichen Beziehungen zu einem anderen Staat oder zu supranationalen Organisationen. Das Wohl eines bestimmten Teilbereichs, z.B. der jeweiligen Regierung, ist für sich genommen

nicht geschützt. Allerdings können aufgrund von Funktionsstörungen einzelner Organe dem Wohl des Bundes oder eines Landes Nachteile drohen. Fiskalische Interessen genügen nur dann, wenn dadurch die Funktionsfähigkeit des Staatsapparates oder wichtige Leistungen des Staates in Frage gestellt werden (Simitis, Bundesdatenschutzgesetz, BDSG § 19 Rn. 87-90).

Bei Nummer 4 ist eine Überprüfung der Daten nur dann erforderlich, wenn tatsächliche Anhaltspunkte für eine Unrichtigkeit der Daten sprechen.

In den Nummern 5 und 6 sind Fälle von Zweckänderungen geregelt, die zum Schutz der betroffenen Person zulässig sind. Diese Tatbestände werden auf Artikel 6 Abs. 4 Fall 2 i.V.m. Artikel 23 Abs. 1 Buchstabe i) Fall 1 DSGVO gestützt. Bei Nummer 5 wird die Voraussetzung der mutmaßlichen Einwilligung der betroffenen Person des bisherigen § 9 Abs. 2 Nr. 4 nicht aufrechterhalten, da diese durch die Informationspflichten nach Artikel 13 Abs. 3 und Artikel 14 Abs. 4 DSGVO kompensiert wird. Im Gegensatz zu den Nummer 1 bis 4 gibt es bei den Zweckänderungen nach Nummer 5 und 6 auch keine Ausnahme von der Informationspflicht (vgl. Absatz 5).

Zu Absatz 3:
Ähnlich wie im bisherigen Gesetz (§ 10 Abs. 2 Satz 2 NDSG) soll eine zweckändernde Verarbeitung nach Absatz 2 nicht zulässig sein, wenn die personenbezogenen Daten einem Berufsgeheimnis oder besonderen Amtsgeheimnis unterliegen. Berufsgeheimnisse sind Geheimnisse, die den Angehörigen der in § 203 Abs. 1 StGB genannten Berufsgruppen (u.a. Ärzte, Berufspsychologen, Rechtsanwälte, Ehe-, Erziehungs- oder Jugendberater, Suchtberater, Sozialarbeiter) in Ausübung ihrer Tätigkeit bekannt werden. Besondere Amtsgeheimnisse sind solche Geheimnisse, die über das im Verwaltungsverfahrensrecht geregelte allgemeine Amtsgeheimnis und die dienst- und arbeitsrechtlichen Verschwiegenheitspflichten hinausgehen (wie das Steuergeheimnis, das Post- und Fernmeldegeheimnis oder das Statistikgeheimnis). Die Regelungsbefugnis ergibt sich aus Artikel 6 Abs. 2 und 3 Satz 3 DSGVO, indem geregelt wird, welcher Zweckbindung bestimmte Daten unterliegen. Insofern wird hier eine Ausnahme von der Ausnahme (Absatz 2) vom Grundsatz der Zweckbindung geregelt. Die Zulässigkeit einer Zweckänderung auf der Grundlage einer Einwilligung nach Artikel 6 Abs. 4 Fall 1 DSGVO bleibt hingegen auch hier unberührt, was auch der bisherigen Rechtslage entspricht.

Zu Absatz 4:
Der bisherige § 10 Abs. 4 NDSG wird aufrechterhalten. Der Begriff der „Datensicherung“ wurde durch den Begriff der „Gewährleistung der Datensicherheit“ ersetzt. Der bisher verwendete

Begriff „Datensicherung“ wird im IT- Bereich für Back-Ups und sonstige Maßnahmen der Sicherung gegen den Datenverlust verwendet. Hier hingegen ist Gegenstand der Regelung die Datensicherheit allgemein. Die Bestimmung einer solchen Zweckbegrenzung wird von Artikel 6 Abs. 2, Abs. 3 Satz 3 DSGVO ermöglicht und stellt wiederum eine Ausnahme von der Ausnahme (Abs. 2) vom Grundsatz der Zweckbindung dar. Damit ist auch sichergestellt, dass personenbezogene Daten, die beispielsweise zum Betrieb, zur Wartung und Aufrechterhaltung von IT-Systemen verarbeitet werden, keiner Zweckänderung zugänglich sind.

Zu Absatz 5:

Grundsätzlich besteht nach Artikel 13 Abs. 3 und Artikel 14 Abs. 4 DSGVO eine Informationspflicht des Verantwortlichen vor einer Weiterverarbeitung für einen anderen Zweck. Die Weiterverarbeitung in Art. 13 Abs. 3 und Art. 14 Abs. 4 steht somit immer im Zusammenhang mit einer Zweckänderung. Gemäß Artikel 23 Abs. 1 DSGVO können die Rechte und Pflichten gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5 beschränkt werden, soweit dies erforderlich ist, um die in Artikel 23 Abs. 1 Buchstaben a) bis j) genannten Aspekte sicherzustellen und die Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. In den Fällen des Absatz 2 Nummern 1 bis 4, in denen eine zweckändernde Verarbeitung auf der Grundlage von Artikel 6 Abs. 4 Fall 2 i.V.m. Artikel 23 Abs. 1 zugelassen wurde, wird zur Absicherung der Erfüllung dieser Zwecke normiert, dass eine Information der betroffenen Person nicht erfolgt, soweit und solange der Zweck der Verarbeitung durch eine solche Information gefährdet würde. Erfasst sind die Fallgruppen, in denen die Information zu einer Vereitelung oder ernsthaften Beeinträchtigung des – legitimen – Verarbeitungszwecks führen würde, etwa weil eine verdeckte Ermittlung bekannt würde und die Information dazu genutzt werden könnte, weitere Feststellungen zu vereiteln oder gezielt beeinflussen zu können. Auch die aus der Information zu schlussfolgernden Erkenntnisse über Arbeitsweisen und Methoden der jeweiligen Behörde können zu einer entsprechenden Zweckgefährdung führen.

Die Ausnahme von der Informationspflicht wird auf dieselben oben zu Absatz 2 aufgeführten Buchstaben des Artikels 23 Abs. 1 DSGVO gestützt wie die Zulässigkeit der Zweckänderung. Dass die Gründe für die Ausnahme von der Informationspflicht dokumentiert werden müssen, ergibt sich bereits aus dem Gebot eines rechtsstaatlichen Verwaltungsverfahrens und muss hier nicht im Gesetzestext geregelt werden.

Sobald eine Gefährdung der Verarbeitungszwecke nicht mehr besteht, hat die Information der betroffenen Person zu erfolgen.

**Zu Abschnitt 3 (Rechte der betroffenen Person):**

**Zu § 7 (Beschränkung der Informationspflicht nach Artikel 13 Abs. 1 und 2 und Artikel 14 Abs. 1 bis 3 der Datenschutz-Grundverordnung):**

Die Datenschutz-Grundverordnung sieht in ihren Artikeln 13 Abs. 1 und 2 und Artikel 14 Abs. 1 bis 3 umfängliche Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen bei der Erhebung personenbezogener Daten vor. Auf diese Weise soll ein größtmögliches Maß an Transparenz hergestellt und die betroffenen Personen in die Lage versetzt werden, ihre Rechte umfassend wahrzunehmen. Da es nach der bisherigen Rechtslage keine entsprechenden umfangreichen Informationspflichten gab, bestand bisher auch keine Notwendigkeit, solche Ausnahmen zu regeln.
Das Recht auf Information über die Datenverarbeitung darf nach der Datenschutz-Grundverordnung nur unter engen Voraussetzungen beschränkt werden. Artikel 23 Abs. 1 DSGVO gibt den Maßstab für derartige Beschränkungen vor. Die Beschränkungen in § 7 werden im Schwerpunkt auf folgende Tatbestände des Artikels 23 Abs. 1 gestützt:
§ 7 Nr. 1: Artikel 23 Abs. 1 Buchstaben c) und e)
§ 7 Nr. 2: Artikel 23 Abs. 1 Buchstaben d) und e)
§ 7 Nr. 3: Artikel 23 Abs. 1 Buchstaben e) und i).

Die Verantwortlichen haben zu prüfen, in welchem Umfang und in welchem Zeitraum eine Gefährdung i.S.d. in § 7 geregelten Tatbestände besteht. Soweit und sobald eine Gefährdung nicht mehr vorliegt, ist die entsprechende Information zu erteilen.

Bei § 7 Nr. 1 wird auf die Ausführungen zu § 6 Abs. 2 Nr. 1 verwiesen.

Unberührt bleiben die in Artikel 13 Abs. 4 sowie Artikel 14 Abs. 5 DSGVO normierten Ausnahmen von der Informationspflicht.

**Zu § 8 (Beschränkung des Auskunftsrechts nach Artikel 15 der Datenschutz-Grundverordnung):**

Zu Absatz 1:
In den Fällen, in denen sich eine nach Artikel 15 DSGVO verlangte Auskunft auf die Übermittlung von personenbezogenen Daten an die in Absatz 1 Satz 1 genannten Behörden bezieht, ist vor der Auskunftserteilung eine Stellungnahme dieser Behörden einzuholen. Andere zur

Verfolgung von Straftaten zuständige Stellen i. S. v. Nummer 1 sind insbesondere die Finanzbehörden, die nach § 386 AO bei Verdacht einer Steuerstraftat ermitteln.
Satz 2 regelt, dass eine Stellungnahme der in Nr. 3 genannten Behörden nur eingeholt werden muss, wenn die Erteilung der Auskunft die Sicherheit des Bundes berühren könnte.
Die Verantwortlichen haben die nach Satz 1 eingeholte Stellungnahme bei der Entscheidung, ob Gründe nach Abs. 2 vorliegen, die einer Auskunftserteilung entgegenstehen könnten, zu berücksichtigen. Satz 3 regelt den umgekehrten Fall einer Auskunft über eine Übermittlung von einer Behörde nach Satz 1.
Zweck dieser Regelung ist, dass die betroffene Person nicht über andere Behörden das erfahren soll, was ihr die Sicherheitsbehörden oder Nachrichtendienste nicht direkt mitteilen würden. Die Regelungsbefugnis ergibt sich aus Artikel 23 Abs. 1 Buchstaben a) bis e) DSGVO.

Zu Absatz 2:
Die Regelung entspricht teilweise dem bisherigen § 16 Abs. 4 NDSG. Das Recht auf Auskunft nach Artikel 15 DSGVO darf nur unter den engen Voraussetzungen von Artikel 23 Abs. 1 DSGVO beschränkt werden.
Die Beschränkungen des Auskunftsrechts nach Satz 1 sind identisch mit den Beschränkungen der Informationspflicht in § 7 und werden auf dieselben oben aufgeführten Tatbestände des Artikels 23 Abs. 1 DSGVO gestützt. Bei § 8 Abs. 2 Nr. 1 wird auf die Ausführungen zu § 6 Abs. 2 Nr. 1 verwiesen.
Neu gegenüber der bisherigen Regelung in § 16 Abs. 4 NDSG ist die Regelung in § 8 Abs. 2 Satz 1 Nr. 2. Danach können Auskünfte abgelehnt werden, soweit und solange dies zur Verfolgung von Straftaten und Ordnungswidrigkeiten notwendig ist. Diese Tatbestände fallen grundsätzlich, d. h. wenn sie durch die zuständigen Behörden der Polizei und der Justiz verfolgt werden, in den Anwendungsbereich der Richtlinie (EU) 2016/680. Im Bereich der Datenschutz-Grundverordnung müssen die Auskunftsrechte (und Informationspflichten, s.o. zu § 7) der betroffenen Personen im vergleichbaren Maß wie im Bereich der Richtlinie eingeschränkt werden.

Gefährdet die Auskunftserteilung diese Ziele, muss sie unterbleiben, soweit und solange eine solche Gefährdung besteht. Die Verantwortlichen haben zu prüfen, in welchem Umfang und in welchem Zeitraum eine Gefährdung i.S.d. in Satz 1 geregelten Tatbestände besteht. Soweit und sobald eine Gefährdung nicht mehr vorliegt, ist die entsprechende Auskunft zu erteilen.

Nach Satz 2 kann eine Auskunft auch abgelehnt werden, wenn die Daten ausschließlich zu Zwecken der Gewährleistung der Datensicherheit (zum Begriff s. o. zu § 6 Abs. 4) oder der

Datenschutzkontrolle verarbeitet werden und durch geeignete technische und organisatorische Maßnahmen gegen eine Verarbeitung zu anderen Zwecken geschützt sind und wenn die Erteilung der Auskunft einen unverhältnismäßigen Aufwand erfordern würde.
Hierbei handelt es sich etwa um Protokolldateien und andere automatisierte Ereignisdokumentationen, Datenspiegelungen zur Erhöhung der Verfügbarkeit, Verfahren der Datensicherung oder Zwischenspeicherungen zur Erhöhung der Verarbeitungsgeschwindigkeit, welche die eigentlichen Daten lediglich spiegeln oder kopieren.
Eine Beschränkung des Auskunftsanspruchs nach Artikel 15 DSGVO erfolgt durch die Regelung nicht, denn die im Rahmen von Maßnahmen der Datensicherheit oder Datenschutzkontrolle gespeicherten Daten weichen nicht von den Primärdaten ab, hinsichtlich derer ein umfassender Auskunftsanspruch gemäß Artikel 15 DSGVO besteht.
Damit wird die betroffene Person durch diese klarstellende Regelung nicht wesentlich in ihren Rechten beeinträchtigt. Dies gilt umso mehr, als dass - abweichend vom bisherigen § 16 Abs. 1 Satz 2 NDSG - die Auskunft nur abgelehnt werden darf, wenn die Erteilung der Auskunft einen unverhältnismäßigen Aufwand erfordern würde.

Zu Absatz 3:
Satz 1 der Regelung ist dem bisherigen § 16 Abs. 5 NDSG nachgebildet. Dieser stellt sicher, dass nicht durch die Mitteilung der Gründe, auf die die Ablehnung eines Antrags auf Auskunft gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Satz 2 regelt, dass soweit die Ablehnung der Auskunft nicht nach Satz 1 begründet wird, die Gründe dafür aktenkundig zu machen sind.

Zu Absatz 4:
In Satz 1 wird nunmehr zum Schutz der Rechte der betroffenen Person geregelt, dass die Auskunft auf ihr Verlangen der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde zu erteilen ist, soweit nicht die zuständige oberste Landesbehörde im Einzelfall feststellt, dass durch die Auskunft die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Regelung stellt damit als Maßnahme im Sinne des Artikels 23 Abs. 2 DSGVO sicher, dass die Rechte der betroffenen Person angemessen gewahrt bleiben. Die mögliche Beschränkung der Information an die von der oder dem Landesbeauftragten geleiteten Behörde dient wiederum dem Schutz von in Artikel 23 Abs. 1 DSGVO genannten Zielen (dem Schutz der öffentlichen Sicherheit gemäß Art. 23 Abs. 1 Buchstabe c) und der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten gemäß Art. 23 Abs. 1 Buchstabe d). Aus dem Tatbestand ergibt sich bereits, dass diese Regelung als eine Art Notstandsklausel anzusehen ist, deren Anwendung nur in extremen Ausnahmefällen in Betracht kommt., da es

sich bei der von der oder dem Landesbeauftragten geleiteten Behörde um eine oberste Landesbehörde handelt, deren Inkenntnissetzung nur im absoluten Einzelfall zu einer Gefährdung der Sicherheit des Bundes oder eines Landes führen dürfte. Auch dürfen nur diejenigen Aspekte des Sachverhaltes, die diese Gefährdung verursachen, von der Auskunft ausgenommen werden. Eine Pflicht zur Einholung der Zustimmung der obersten Landesbehörde begründet § 8 Abs.4 nicht. Der Ausnahmefall wird sich der verantwortlichen Stelle vielmehr aufdrängen bzw. die oberste Landesbehörde wird diesen von sich aus dieser gegenüber geltend machen, zumal hier in der Regel auch ein Fall des Abs. 1 vorliegen wird.

Wird der von der oder dem Landesbeauftragten geleiteten Behörde für den Datenschutz eine Auskunft nicht erteilt, so sind die Gründe dafür nach Satz 2 ebenfalls aktenkundig zu machen.

Das Akteneinsichtsrecht aus dem bisherigen § 16 Abs. 3 NDSG wurde gestrichen, da das umfassend in Artikel 15 DSGVO geregelte Auskunftsrecht die Akteneinsicht umfasst.
Es besteht folglich weiterhin die alternative Möglichkeit statt der Erteilung einer Auskunft auch Einsicht in Akten zu gewähren. Insbesondere zum Schutz der berechtigten Interessen der betroffenen Person aber auch in den Fällen, in denen die Erteilung einer Auskunft gegenüber der Gewährung einer Akteneinsicht zu einem unverhältnismäßigen Aufwand beim Verantwortlichen führen würde, besteht weiterhin die Möglichkeit, anstelle der Erteilung einer Auskunft auch eine Akteneinsicht zu gewähren. Der Verantwortliche entscheidet hierüber nach pflichtgemäßem Ermessen. Dies gilt sowohl für Akten in Papierform als auch für elektronisch geführte Akten.

**Zu § 9 (Beschränkung der Benachrichtigungspflicht nach Artikel 34 der Datenschutz-Grundverordnung):**

Das Recht der betroffenen Person auf bzw. die Pflicht der Verantwortlichen zur Benachrichtigung bei einer Verletzung des Schutzes personenbezogener Daten mit voraussichtlich hohem Risiko nach Artikel 34 DSGVO darf nur unter den engen Voraussetzungen von Artikel 23 Abs. 1 DSGVO beschränkt werden. Da es nach der bisherigen Rechtslage keine entsprechende Benachrichtigungspflicht des Verantwortlichen gab, bestand bisher auch keine Notwendigkeit, Ausnahmen dazu zu regeln.

Die Nummern 1 bis 3 entsprechen den Beschränkungen bei der Informationspflicht in § 7 und beim Auskunftsrecht in § 8 und werden auf dieselben Tatbestände des Artikels 23 Abs. 1 DSGVO gestützt. Bei § 9 Nr. 1 wird auf die Ausführungen zu § 6 Abs. 2 Nr. 1 verwiesen.

Zusätzlich kann nach Nummer 4 die Benachrichtigung über die Verletzung personenbezogener Daten unterbleiben, soweit und solange die Benachrichtigung die Sicherheit von automatisierten Informationssystemen gefährden würde. Dieses wird auf Artikel 23 Abs. 1 Buchstabe e) DSGVO gestützt. Die zunehmende Bedeutung der Digitalisierung für die Verwaltung erhöht auch das Risiko, dass eine Einschränkung der Funktionsfähigkeit von automatisierten Informationssystemen zu einer Gefährdung der gesamten Verwaltungstätigkeit führen kann. Das könnte insbesondere der Fall sein, soweit und solange die Benachrichtigung eine Sicherheitslücke offenlegen würde, die das Gesamtsystem auch an anderen Stellen gefährden und somit vor einer abschließenden Behebung nicht bekannt werden sollte. Andernfalls könnte die Benachrichtigung zu einer Gefährdung der IT-Systeme insgesamt führen und ggf. die Funktionsfähigkeit der Verwaltung gefährden. Eine funktionsfähige Verwaltung ist ein sonstiges wichtiges Ziel des allgemeinen öffentlichen Interesses im Sinne des Artikels 23 Abs. 1 Buchst. e DSGVO, vergleichbar mit den dort beispielhaft aufgeführten Zielen.

Gefährdet die Benachrichtigung diese Ziele, muss sie unterbleiben, soweit und solange eine solche Gefährdung besteht. Die Verantwortlichen haben zu prüfen, in welchem Umfang und in welchem Zeitraum eine entsprechende Gefährdung besteht. Soweit und sobald eine Gefährdung nicht mehr vorliegt, hat die entsprechende Benachrichtigung zu erfolgen.

Unberührt bleiben die in Artikel 34 Abs. 3 DSGVO geregelten Ausnahmen von der Benachrichtigungspflicht.

**Zu Abschnitt 4 (Besonderer Datenschutz):**

**§§ 10 bis 12**

Die §§ 10 bis 12 befassen sich mit Datenverarbeitungen, die dem sachlichen Anwendungsbereich der Datenschutz-Grundverordnung unterfallen.

**Zu § 10 (Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen)**

Die Regelungsbefugnis für § 10 ergibt sich aus der Öffnungsklausel des Artikels 88 DSGVO. Dieser überlässt es den Mitgliedstaaten, spezifischere Regelungen zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext zu schaffen. Die Möglichkeit, den Arbeitnehmerdatenschutz – wie bisher in § 24 NDSG – fortzuführen, wird wahrgenommen.

Zu Absatz 1:
Die Regelung des bisherigen § 24 Abs. 1 NDSG wird weitestgehend beibehalten, um den Gleichklang der Vorschriften für beamtete und nicht beamtete Beschäftigte des öffentlichen Bereiches zu gewährleisten. Für die beamteten Beschäftigten gilt vorrangig das Niedersächsische Beamtengesetz, das bzgl. der genannten Vorschriften für die nicht beamteten Beschäftigten für entsprechend anwendbar erklärt wird, soweit tarifvertraglich nichts anderes geregelt ist.

Zu Absatz 2:
Die Regelung des bisherigen § 24 Abs. 2 NDSG wird weitestgehend beibehalten. Sie wurde geschaffen, um den Besonderheiten von Daten aus ärztlichen und psychologischen Untersuchungen und Tests Rechnung zu tragen, die im Bewerbungsverfahren erhoben werden. Im Rahmen der Regelungsoption des Artikels 88 DSGVO soll die Vorschrift fortgelten. Die schriftliche Information nach Satz 2 umfasst nicht solche per E-Mail.

Der bisherige § 24 Abs. 2 Satz 3 NDSG konnte nicht aufrechterhalten werden. Es dürfen keine bereichsspezifischen Regelungen zur Einwilligung wie z.B. die schriftliche Einwilligung getroffen werden. Die Verarbeitung und weitere Verarbeitung ergeben sich aus der Datenschutz-Grundverordnung und den allgemeinen Vorschriften dieses Gesetzes. Im Ergebnis bedeutet dies, dass eine Zweckänderung bei Einwilligung nach der allgemeinen Regelung des Art. 6 Abs. 4 Fall 1 DSGVO möglich ist. Die Regelung des § 6 Abs. 2 NDSG-E zur Zweckänderung ist gemäß § 6 Abs. 3 NDSG-E ausgeschlossen. Der zumindest theoretisch denkbare Fall des Artikels 6 Abs. 4 Fall 3 kann national nicht ausgeschlossen werden.

**Zu § 11 (Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken):**

§ 11 regelt die spezifischen Anforderungen an die Verarbeitung personenbezogener Daten für Forschungszwecke. Die Regelungsbefugnis für § 11 ergibt sich aus Artikel 6 Abs. 2 und 3 in Verbindung mit Artikel 89 DSGVO. Gem. Artikel 89 Abs. 1 DSGVO unterliegt die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken geeigneten Garantien für die Rechte und Freiheiten der Betroffenen gemäß der Datenschutz-Grundverordnung. Geeignete Garantien sind in erster Linie technische und organisatorische Maßnahmen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.

Für die Verarbeitung besonderer Kategorien personenbezogener Daten i. S. v. Artikel 9 Abs. 1 DSGVO für wissenschaftliche oder historische Forschungszwecke ohne Einwilligung der betroffenen Person bedarf es gem. Artikel 9 Abs. 2 Buchstabe j) DSGVO einer nationalen Regelung.
Von der in § 11 geregelten Verarbeitung ist zugleich die Weiterverarbeitung umfasst, da nach Artikel 5 Abs. 1 Buchstabe b) Halbsatz 2 DSGVO eine Weiterverarbeitung für wissenschaftliche oder historische Forschungszwecke nicht als unvereinbar mit den Zwecken, für die die Daten erhoben wurden, gilt. Eine Prüfung der Vereinbarkeit mit dem ursprünglichen Zweck gem. Artikel 6 Abs. 4 Fall 3 DSGVO erübrigt sich daher. Somit sind auch die Regelungen des bisherigen § 25 Abs. 2 NDSG angesichts der Regelung in Artikel 5 Abs. 1 Buchstabe b) Halbsatz 2 DSGVO nunmehr im nationalen Recht obsolet. Die Vorgaben zur Zweckbindung im bisherigen Recht, die für ein Forschungsvorhaben gespeicherten oder übermittelten Daten nur für Zwecke der wissenschaftlichen Forschung verarbeiten zu dürfen (§ 25 Abs. 3 NDSG), werden in der Datenschutz-Grundverordnung abgelöst durch den allgemeinen Zweckbindungsgrundsatz in Artikel 5 Abs. 1 Buchstabe b) DSGVO. Eine zulässige Weiterverarbeitung zu anderen Zwecken nach Artikel 6 Abs. 4 Fall 3 DSGVO durch den Verantwortlichen erscheint in der Regel ausgeschlossen, da es insbesondere regelmäßig an einer Verbindung zwischen den Zwecken i.S.v. Artikel 6 Abs. 4 Fall 3 Buchstabe a) DSGVO fehlen dürfte, daher der Verantwortliche eine Kompatibilität verneinen müsste.

Gegenüber dem bisher geltenden Recht wurde die Regelung – Artikel 89 DSGVO entsprechend – um den Bereich der historischen Forschung ergänzt.

Außerhalb des Bereichs der Verarbeitung von Daten besonderer Kategorien (§ 11 Abs. 4) ergibt sich die grundsätzliche Zulässigkeit der Verarbeitung von Daten zu Forschungszwecken bereits aus der grundrechtlich garantierten Forschungsfreiheit.

Zu Absatz 1:
Die Vorgaben zur Anonymisierung und zur grundsätzlichen Trennung der Hilfsmerkmale von den Einzelangaben stellen geeignete Garantien zur Wahrung der Rechte und Freiheiten der betroffenen Person i.S.v. Artikel 89 Abs. 1 DSGVO dar. Der Begriff der Anonymisierung ist in Artikel 89 Abs. 1 Satz 4 DSGVO beschrieben. Es handelt sich demnach um eine Verarbeitung personenbezogener Daten in einer Weise, bei der die Identifizierung betroffener Personen nicht oder nicht mehr möglich ist.
Eine Anonymisierung ist vorzunehmen, sobald dies nach dem Forschungszweck möglich ist. Die Datenübermittlung von öffentlichen Stellen zu einer Forschungsreinrichtung kann demzufolge nicht anonym erfolgen.

Die Pflicht zur Löschung von Merkmalen, mit denen ein Bezug auf eine bestimmte natürliche Person hergestellt werden kann (bisheriger § 25 Abs. 4, letzter Halbsatz), ergibt sich nunmehr direkt aus Artikel 17 DSGVO. Nach Artikel 17 Abs. 1 Buchstabe a) DSGVO sind die Daten zu löschen, sobald sie nicht mehr notwendig sind. Allerdings gilt Artikel 17 Abs. 1 DSGVO nach Artikel 17 Abs. 3 Buchstabe d) DSGVO u. a. nicht für im öffentlichen Interesse liegende wissenschaftliche oder historische Forschungszwecke gem. Artikel 89 Abs. 1 DSGVO, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.

Zu Absatz 2:
Absatz 2 spezifiziert die Verarbeitung (Übermittlung) personenbezogener Daten im Hinblick auf deren Veröffentlichung, indem zum Schutz der Rechte der betroffenen Person nur im besonderen Ausnahmefall eine personenbezogene Darstellung der Forschungsergebnisse zugelassen wird. Neben der Einwilligung soll dies, wie bisher (§ 25 Abs. 5 NDSG) nur zulässig sein, wenn dies für die Darstellung von Ereignissen der Zeitgeschichte unerlässlich ist. Die Regelungsbefugnis ergibt sich aus Artikel 6 Abs. 2 und Abs. 3 i. V. m. Artikel 89 Abs. 1 DSGVO.

Zu Absatz 3:
Abs. 3 Satz 1 lässt die Übermittlung von personenbezogenen Daten an Empfängerinnen und Empfänger zu wissenschaftlichen und historischen Forschungszwecken zu, auf die die Vorschriften des Niedersächsischen Datenschutzgesetzes keine Anwendung finden, wenn sich diese verpflichten, die Daten ausschließlich für das von ihnen bezeichnete Forschungsvorhaben zu verwenden und die in den Absätzen 1 und 2 normierten Garantien zum Schutz der Rechte der betroffenen Person zu beachten. Diese Regelung folgt dem bisherigen § 25 Abs. 7 Satz 1 NDSG. Sie gewährleistet, dass auch für Datenempfänger außerhalb des Anwendungsbereichs des Niedersächsischen Datenschutzgesetzes die in den Absätzen 1 und 2 normierten Garantien für die Rechte und Freiheiten der betroffenen Person i. S. v. Artikel 89 Abs. 1 gelten.
Nach Satz 2 ist für eine Übermittlung besonderer Kategorien personenbezogener Daten außerdem erforderlich, dass sich die Empfängerin oder der Empfänger verpflichtet, Absatz 4 zu beachten und Schutzmaßnahmen nach § 15 oder eine gleichwertige Maßnahme zu treffen.
Satz 3 entspricht weitgehend dem bisherigen § 25 Abs. 7 Satz 2 NDSG. Die Anzeigepflicht gegenüber der von der oder dem Landesbeauftragten geleiteten Behörde ermöglicht Kontrollmaßnahmen, gegebenenfalls in Zusammenarbeit mit anderen Kontrollinstanzen. Eine Pflicht der von der oder dem Landesbeauftragten geleiteten Behörde zur Reaktion auf die Unterrichtung soll damit nicht begründet werden.

Darüber hinaus gelten die Vorgaben der Datenschutz-Grundverordnung, sofern die Empfängerin oder der Empfänger in deren sachlichen und räumlichen Anwendungsbereich fällt.

Zu Absatz 4:

Artikel 9 Abs. 2 j) DSGVO erlaubt den Mitgliedstaaten, bestimmte Ausnahmen vom Verbot der Verarbeitung besonderer Kategorien von Daten zuzulassen. Artikel 9 Abs. 2 Buchstabe j) DSGVO erfordert, dass eine Forschungsklausel in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Dem wird - neben der Regelung in § 15 – insbesondere durch die nach Satz 1 erforderliche Abwägung zwischen dem öffentlichen Interesse und dem Interesse der betroffenen Person Rechnung getragen. Angesichts der besonderen Sensibilität der Daten muss das Forschungsinteresse in diesem Fall erheblich gegenüber dem Interesse der betroffenen Person überwiegen. Das Ergebnis der Abwägung und dessen Begründung sind nach Satz 2 aufzuzeichnen. Nach Satz 3 ist die oder der Datenschutzbeauftragte nach Artikel 37 DSGVO über die Verarbeitung zu unterrichten.

Es handelt sich bei Absatz 4 um eine zusätzliche Regelung für die Verarbeitung besonderer Kategorien personenbezogener Daten; die Absätze 1 bis 3 sowie Absatz 5 bleiben unberührt.

Zu Absatz 5:

Abs. 5 regelt, unter welchen Voraussetzungen die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Einschränkung der Verarbeitung und Widerspruch nicht bestehen. Die Regelungsbefugnis ergibt sich aus Artikel 89 Abs. 2 DSGVO. Dieser erlaubt es den Mitgliedstaaten, Ausnahmen von den Rechten der betroffenen Person insoweit vorzusehen, als diese Rechte zulässige, im öffentlichen Interesse liegende Forschungsvorhaben voraussichtlich unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind. Die in Artikel 89 Abs. 1 genannten Bedingungen und Garantien für die Rechte und Freiheiten der betroffenen Personen sind dabei zu beachten. Dies entspricht der in der Datenschutz-Grundverordnung angelegten Privilegierung der Forschung. Dabei kommt es allerdings immer auf den Einzelfall an, so muss z. B. das Recht auf Berichtigung das Forschungsvorhaben unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahme für die Erfüllung der Forschungszwecke notwendig sein, was nur in Ausnahmefällen, z. B. in einem bereits sehr weit gediehenen Stadium eines Forschungsvorhabens, der Fall sein dürfte.

**Zu § 12 (Videoüberwachung):**

Aufgrund der Regelungen in Artikel 6 Abs. 1 Satz 1 Buchst. e) i.V.m. Artikel 6 Abs. 2 und 3 DSGVO ist es erforderlich, die bisherige Rechtsgrundlage für die Videoüberwachung (§ 25 a NDSG) zu modifizieren. Die Zwecke, zu denen öffentliche Stellen eine Videoüberwachung durchführen dürfen, werden beibehalten und ergänzt.
Nach Art. 35 Abs. 3 Buchst. c DSGVO ist vor einer systematischen umfangreichen Beobachtung öffentlich zugänglicher Bereiche eine Datenschutz-Folgenabschätzung durchzuführen.

Zu Absatz 1:
Gestützt auf Artikel 6 Abs. 1 e) DSGVO ist die Videoüberwachung und die weitere Verarbeitung der dadurch erhobenen personenbezogenen Daten zulässig zur Wahrnehmung einer öffentlichen Aufgabe der jeweils zuständigen öffentlichen Stelle.
Dass eine „weitere Verarbeitung“ nicht die Weiterverarbeitung zu anderen Zwecken umfasst, ergibt sich bereits aus S. 3.
Zur Wahrnehmung einer öffentlichen Aufgabe der jeweils zuständigen öffentlichen Stelle gehören zumindest mittelbar auch der Schutz der Personen, die dieser Stelle angehören oder sie aufsuchen sowie der Schutz von Sachen, die zu dieser Stelle oder den sie angehörenden oder aufsuchenden Personen gehören. Die Wahrnehmung des Hausrechts dient der Gewährleistung der Funktionsfähigkeit der öffentlichen Stelle und damit zumindest mittelbar deren Aufgabenerfüllung. Zur Wahrnehmung des Hausrechts gehört auch die Kontrolle von Zugangsberechtigungen. Aus Gründen der Rechtsklarheit werden in Satz 2 Nrn. 1-3 diese Teilaspekte öffentlicher Aufgaben ausdrücklich erwähnt.

Die bei der Videoüberwachung entstehenden Bildaufnahmen stellen keine biometrischen Daten dar. Vom Begriff der biometrischen Daten werden nur solche Daten erfasst, die mittels spezieller technischer Verfahren gewonnen werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen (vgl. Art. 4 Nr. 14 DSGVO und Erwägungsgrund 51 zur Datenschutz-Grundverordnung). Insofern fallen diese Daten nicht unter Art. 9 DSGVO. Das bedeutet auch, dass die Regelung in § 12 NDSG keine Rechtsgrundlage für eine entsprechende technische Bearbeitung von Bildaufnahmen darstellt. Auch die Zuordnung der Daten zu einer Person nach Abs. 3 bedeutet nicht, dass es sich um biometrische Daten i.S.v. Art. 4 Nr. 14 DSGVO handelt. Vielmehr kann die Zuordnung rein faktisch erfolgen, z.B. dadurch, dass die Mitarbeiter, die das Dienstgebäude betreten, bekannt sind.
Satz 1 erfordert zu den bereits genannten Voraussetzungen eine Interessenabwägung. Insoweit wird die bisherige Regelung (§ 25 a Abs. 2 Satz 1 NDSG) materiell aufrechterhalten. Damit stellt Satz 1 eine ausdrückliche Befugnis zur Beobachtung öffentlich zugänglicher

Räume mit Hilfe von optisch-elektronischen Einrichtungen (Videoüberwachung) und die weitere Verarbeitung der dadurch erhobenen personenbezogenen Daten zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe dar. Öffentlich zugängliche Räume sind alle Bereiche, die dem öffentlichen Verkehr gewidmet sind oder nach dem Willen des Berechtigten grundsätzlich von jedermann betreten werden können.

Der Hauptanwendungsfall der Regelung ist die Videoüberwachung der öffentlichen Gebäude des Landes, der Kommunen sowie der anderen dem Anwendungsbereich gemäß §§ 1 und 2 unterliegenden Stellen. Wie im bisherigen Recht wird zwischen der Beobachtung, d.h. Erhebung der Daten (bisher § 25 a Abs. 1 NDSG) und der Weiterverarbeitung (bisher § 25 a Abs. 2 NDSG) unterschieden.

Satz 3 entspricht weitgehend der bisherigen Regelung zur zweckändernden Weiterverarbeitung der durch die Videoüberwachung erhaltenen Daten (§ 25 a Abs. 2 Satz 2 NDSG). Wie bisher soll eine Zweckänderung möglich sein, wenn die Verarbeitung der Daten zur Gewährleistung der öffentlichen Sicherheit oder für Strafverfolgungszwecke erforderlich ist. In Angleichung an § 6 Nr. 1 ist nunmehr eine unmittelbare Gefahr für die öffentliche Sicherheit erforderlich. Wie im bisherigen Recht soll abweichend von § 6 Abs. 2 Nr. 2 eine Zweckänderung nur möglich sein, wenn die Verarbeitung für Strafverfolgungszwecke erforderlich ist. Die Regelung in Satz 3 macht von der Öffnungsklausel in Artikel 6 Abs. 4 Fall 2 DSGVO i.V.m. Artikel 23 Abs. 1 Buchstaben c) und d) DSGVO Gebrauch. Die Datenschutz-Grundverordnung gestattet eine Durchbrechung der Zweckbindung i. S. v. Artikel 5 Abs. 1 Buchstabe b) DSGVO, wenn diese in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der öffentlichen Sicherheit oder zur Verfolgung von Straftaten darstellt. Gegenüber der allgemeinen Vorschrift in § 6 Abs. 2 handelt es sich um eine die zulässige Zweckänderung einschränkende Spezialvorschrift für die Videoüberwachung. Die Zulässigkeit der Zweckänderung aufgrund einer Einwilligung der betroffenen Person wie im bisherigen Recht folgt nunmehr auch hier unmittelbar aus Artikel 6 Abs. 4 Fall 1 DSGVO.
Der letzte Halbsatz des Satz 3 erklärt § 6 Abs. 5 für entsprechend anwendbar. Eine Information an die betroffene Person nach Artikel 13 Abs. 3 und Artikel 14 Abs. 4 DSGVO über die Datenverarbeitungen zu einem anderen Zweck nach Satz 4 erfolgt folglich nicht, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde.

Zu Absatz 2:
Wie im bisherigen Recht (§ 25 a Abs. 3 NDSG) ist der Umstand der Videoüberwachung für die betroffenen Personen durch geeignete Maßnahmen erkennbar zu machen. Zudem wird nunmehr bestimmt, dass die Information zum frühestmöglichen Zeitpunkt erfolgen soll. Hierdurch

soll gewährleistet werden, dass betroffene Personen so früh wie möglich von der Tatsache, dass bestimmte Bereiche videoüberwacht werden, Kenntnis nehmen und ihr Verhalten daran ausrichten können. Frühestmöglich bedeutet dabei, dass eine Information möglichst vor dem Betreten videoüberwachter Bereiche erfolgt.
Die Regelung dient der Transparenz des Vorgangs der Videoüberwachung (Artikel 5 Abs. 1 Buchstabe a) DSGVO). Die generellen Informationspflichten der für die Datenverarbeitung Verantwortlichen wurden durch Artikel 13 DSGVO deutlich erweitert und beziehen sich auch auf die bei einer Videoüberwachung verarbeiteten Daten. Auf den Namen und die Kontaktdaten des Verantwortlichen sowie die Möglichkeit, beim Verantwortlichen die Informationen nach Artikel 13 DSGVO zu erhalten, ist hinzuweisen (Hinweisschilder, Internetauftritt etc.). Dabei handelt es sich nicht um eine Beschränkung der Verpflichtung zur Information, sondern um eine Konkretisierung, die erforderlich ist, um in den Fällen der Videoüberwachung die Einhaltung der Vorschriften der Datenschutz-Grundverordnung abzusichern.

Zu Absatz 3:
Als spezifische nationale Bestimmung auf der Grundlage von Artikel 6 Abs. 2, Abs. 3 DSGVO enthält Absatz 3 wie im bisherigen Recht (§ 25 a Abs. 4 NDSG) eine Regelung der Pflicht zur Information der betroffenen Person über die Verarbeitung, soweit durch die Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet werden.
Damit wird angesichts der Eingriffstiefe einer Videoüberwachung über die Anforderungen der Datenschutz-Grundverordnung hinausgegangen, da nach dieser keine (erneute) Information der betroffenen Person, sofern die weitere Verarbeitung zum gleichen Zweck erfolgt, vorgesehen ist. In Satz 2 wird eine entsprechende Geltung von § 7 NDSG angeordnet, der Ausnahmen von der Informationspflicht regelt. Der bisher in § 25 a Abs. 4 Satz 2 Nr. 2 NDSG geregelte Fall des unverhältnismäßigen Aufwands befindet sich nunmehr in Satz 3.

Zu Absatz 4:
Artikel 35 Abs. 3 Buchstabe c) DSGVO schreibt für systematische umfangreiche Überwachungen öffentlich zugänglicher Bereiche, d.h. auch Videoüberwachungen, die Durchführung einer Datenschutz-Folgenabschätzung vor. Dabei ist der Rat der oder des behördlichen Datenschutzbeauftragten einzuholen (Artikel 35 Abs. 2 DSGVO). Artikel 35 Abs. 7 DSGVO regelt die allgemeinen Inhalte der Folgenabschätzung. Absatz 4 konkretisiert die der oder dem behördlichen Datenschutzbeauftragten mitzuteilenden Informationen. Es handelt sich bei den hier genannten mitzuteilenden Informationen um keine abschließende Aufzählung, was durch das Wort „insbesondere“ deutlich wird. Bereits aus dem Zweck der Regelung des Art. 35 DSGVO ergibt sich, dass dem Datenschutzbeauftragten, der nach Art. 35 Abs. 2 konsultiert wird, die im Einzelfall zur Durchführung der Konsultation erforderlichen Informationen (vgl.

auch Art. 35 Abs. 7 DSGVO) zur Verfügung zu stellen sind. Dazu zählen die Eigenart der betreffenden Überwachung, ihres Umfangs, Kontextes und Zwecks, also insbesondere Informationen über die eingesetzten Videoaufzeichnungsanlagen (Bezeichnung, technische Ausstattung, z. B. Videokameras mit/ohne Übertragung, Hersteller, Zahl der Kameras), die räumliche Ausdehnung der Überwachung (z.B. Standort der Anlage mit/ohne Zoom, automatisch/manuell schwenkbar, veränderbar/nicht veränderbar), die Dauer der Aufzeichnung, Maßnahmen zur Kennzeichnung der Videoüberwachung und der erhebenden Stelle, die Gewährleistung der Vertraulichkeit (Wer hat welche Zugriffsrechte auf die aufgezeichneten Daten? Wie werden unbefugte Zugriffe verhindert? Wie wird die Vertraulichkeit beim Transport bzw. der Übermittlung personenbezogener Daten gesichert?), die Protokollierung (Werden Zugriffe auf die aufgezeichneten Daten und Datenübermittlungen automatisch protokolliert? Wie lange werden diese Protokolle aufgehoben? Ist ihre datenschutzgerechte Entsorgung gewährleistet?), die Festlegung der Auswertungskriterien und des berechtigten Personenkreises (z. B. wer wertet wann welche (Protokoll)daten zu welchem Zweck aus) sowie die vorgesehenen Löschroutinen (wann, wer, wie, Vernichtung der Datenträger, Nachweis).
Der bisherige § 25 a Abs. 5 NDSG zur Löschung gespeicherter Daten kann entfallen, da sich das Gebot des unverzüglichen Löschens bereits aus Artikel 5 Abs. 1 Buchstabe e) i.V.m. Artikel 17 der Datenschutz-Grundverordnung ergibt.

**Zu § 13 und § 14:**

§ 13 und § 14 befassen sich mit Datenverarbeitungen, die nicht dem sachlichen Anwendungsbereich der Datenschutz-Grundverordnung unterfallen. Die Verarbeitungen von personenbezogenen Daten zum Zwecke öffentlicher Auszeichnungen und Ehrungen sowie in Begnadigungsverfahren fallen nicht in den Anwendungsbereich des Unionsrechts und damit gemäß Artikel 2 Abs. 2 Buchstabe a) DSGVO nicht in den Anwendungsbereich der Datenschutz-Grundverordnung. Gleichwohl sollen auch für die in diesem Zusammenhang vorgenommenen Datenverarbeitungen die Grundprinzipien der Datenschutz-Grundverordnung und dieses Gesetzes gelten, wofür § 2 Nr. 2 a) und b) Regelungen schafft. Allerdings bedarf es hier spezieller, die Regelungen der entsprechend anwendbaren Datenschutz-Grundverordnung begrenzender Vorschriften.

**Zu § 13 (Öffentliche Auszeichnungen und Ehrungen):**

Die Vergabe öffentliche Auszeichnungen und Ehrungen ist keine Tätigkeit, die in den Anwendungsbereich des Unionsrechts nach Artikel 2 Abs. 2 Buchstabe a DSGVO fällt. Die Verlei-

hung einer staatlichen Auszeichnung ist ein außergerichtlicher Gunstbeweis, den die Ordensverleiherin oder der Ordensverleiher demjenigen gewährt, den sie oder er für auszeichnungswürdig hält. Die Ordensverleihung vollzieht sich ohne Begründungszwang und Überprüfbarkeit in einem rechtlich nur wenig reglementierten Raum. Dieser besondere Charakter der Ordensverleihung begründet spezielle datenschutzrechtliche Regelungen.

Zu Absatz 1:

Abs. 1 regelt die Verarbeitungsbefugnis der vorbereitenden Stelle im Hinblick auf die zur Vorbereitung der Entscheidung erforderlichen Daten und bestimmt zum Schutz der Rechte der betroffenen Personen eine strenge Zweckbindung.

Eine Satz 1 und 2 entsprechende Regelung findet sich auch im bisher geltenden Recht (§ 27 NDSG). Mit Satz 1 wird die Rechtsgrundlage für die Verarbeitung der Daten zu den genannten Zwecken geschaffen. Zur Vorbereitung der Entscheidung sind alle Daten erforderlich, die zur Beurteilung einer in sachlicher und persönlicher Hinsicht bestehenden (Auszeichnungs- oder Ehr-) Würdigkeit der betroffenen Person benötigt werden. Grundsätzlich zulässig ist auch die Verarbeitung von Daten besonderer Kategorien nach Artikel 9 Abs. 1 DSGVO, soweit spezialgesetzliches Recht dem nicht entgegensteht. Die Regelung wurde um den Begriff „Ehrungen“ erweitert, um klarzustellen, dass zum Beispiel auch solche Fälle erfasst werden, in denen ausgewählte Bürgerinnen und Bürger zu staatlichen Empfängen o. ä. geladen werden.

Eine Verarbeitung der Daten ist jedoch nicht zulässig, wenn der Daten verarbeitenden Stelle bekannt ist, dass die betroffene Person ihrer öffentlichen Auszeichnung oder Ehrung oder der damit verbundenen Datenverarbeitung widersprochen hat. Damit wird sichergestellt, dass die Einschränkung der datenschutzrechtlichen Position der betroffenen Person nicht bei einem bekannten entgegenstehenden Willen dieser Person erfolgt. Satz 2 regelt - wie bisher -, dass öffentliche Stellen auf Anforderung der in Satz 1 genannten Stellen die erforderlichen Daten übermitteln dürfen. Dabei dürfte es sich regelmäßig um eine Zweckänderung handeln, die damit für ausnahmsweise zulässig erklärt wird. Die Feststellung der Ehrwürdigkeit der betroffenen Person erfordert eine möglichst umfassende Heranziehung entscheidungsrelevanter Daten, und zwar gerade solcher, die für andere Zwecke erhoben bzw. gespeichert worden sind.

Die Datenverarbeitung unterliegt nach Satz 3 dem Zweckbindungsgrundsatz für die in dieser Regelung genannten Zwecke der öffentlichen Auszeichnungen und Ehrungen, es sei denn, die betroffene Person willigt – nach der Maßnahme – in die Weiterverarbeitung ein. Damit wird klargestellt, dass eine zweckändernde Weiterverarbeitung nur aufgrund einer Einwilligung nach Artikel 6 Abs. 4 Fall 1 DSGVO erfolgen darf. Die Anwendbarkeit des § 6 Abs. 2 wird damit ausgeschlossen, was durch den 2. Halbsatz des Satz 3 klargestellt wird. Durch den Ausschluss einer Verarbeitung zu anderen Zwecken ist auch die kompatible Zweckänderung nach Artikel 6 Abs. 4 Fall 3 DSGVO ausgeschlossen.

Zu Absatz 2:
Absatz 2 sieht eine Durchbrechung des Grundsatzes der erweiterten Anwendbarkeit gemäß § 2 vor. Wie die bisherige Regelung (§ 27 Abs. 2 NDSG) sieht Absatz 2 eine Ausnahme vom Auskunftsrecht nach Artikel 15 DSGVO vor. Erweitert wird diese Regelung um weitere Ausnahmen von neu mit der Datenschutz-Grundverordnung eingeführten Betroffenenrechten. Im Einzelnen besteht eine Ausnahme von der Mitteilungspflicht nach Artikel 19 DSGVO, eine Ausnahme von der Hinweispflicht nach Artikel 21 Abs. 4 DSGVO und eine Ausnahme von der Informationspflicht nach Artikel 13 und 14 DSGVO, wobei der Fall des Artikel 13 DSGVO in der Regel ohnehin kaum einschlägig sein dürfte, da hier eine Erhebung bei der betroffenen Person selten vorkommen dürfte. Verfahren zur Verleihung öffentlicher Auszeichnungen und Ehrungen sind in ihrer Gesamtheit zum Schutz öffentlicher und im Verfahren bekannt werdender persönlicher Interessen vertraulich, gerade auch gegenüber der betroffenen Person. Informations-, Hinweis- und Mitteilungspflichten oder Auskunftsrechte würden dem Wesen öffentlicher Ehrerweisungen widersprechen. Die Ausnahmen sind mit dem wichtigen öffentlichen Interesse an einer tragfähigen Auswahlentscheidung begründet, die eine vollumfängliche – auch die persönliche Integrität der möglicherweise auszuzeichnenden oder zu ehrenden Person umfassenden - Würdigung voraussetzt.

**Zu § 14 (Begnadigungsverfahren):**

Gnadenangelegenheiten sind Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts nach Artikel 2 Abs. 2 Buchstabe a DSGVO fallen. Das Gnadenrecht begründet eine dem Amte des Trägers des Gnadenrechts eigene Befugnis, eine Gestaltungsmacht besonderer Art. Der Begriff der Gnade impliziert, dass eine Verurteilte oder ein Verurteilter bzw. eine sonstige Gnadenempfängerin oder ein sonstiger Gnadenempfänger kein Recht auf Gnade hat. Dieser besondere Charakter des Gnadenrechts begründet spezielle datenschutzrechtliche Regelungen.

§ 14 ist die allgemeine Rechtsgrundlage für die Datenverarbeitung in Gnadensachen. Grundsätzlich gelten auch hier nach § 2 Nr. 2 b) die Regelungen der Datenschutz-Grundverordnung und dieses Gesetzes, um dadurch ein möglichst einheitliches Datenschutzregime zu erhalten und die Rechtssicherheit zu fördern, was auch für den Bereich der Datenverarbeitung in Begnadigungsverfahren sinnvoll ist.
Satz 2 sieht eine Ausnahme von der Informationspflicht (Artikel 13 und 14 DSGVO), der Mitteilungspflicht (Artikel 19 DSGVO) und dem Auskunftsrecht (Artikel 15 DSGVO) vor, so dass für diese Betroffenenrechte keine erweiterte Anwendung der Regelungen der Datenschutz-

Grundverordnung nach § 2 erfolgt. Wie bei § 13 wird auch hier der Fall des Artikels 13 DSGVO ohnehin selten einschlägig sein. Nach der bisherigen Regelung (§ 2 Abs. 8 NDSG) fand das Niedersächsische Datenschutzgesetz auf das Gnadenverfahren mit Ausnahme des Vierten Abschnitts (Landesbeauftragte oder Landesbeauftragter für den Datenschutz) keine Anwendung, somit bestand auch bisher kein Auskunftsrecht.
Die Ausübung des Gnadenrechts ist weder an bestimmte normative Voraussetzungen gebunden, noch erfolgt eine gerichtliche Kontrolle (BVerfGE 25, 352, 361 ff). Die Gnadenträgerin oder der Gnadenträger entscheidet jeden Einzelfall frei, in eigener Verantwortung und ohne Rechtfertigungsdruck gegenüber der Legislative oder Judikative. Dieses überkommene Verständnis der Eigenverantwortlichkeit für Gnadenentscheidungen wäre empfindlich gestört, wenn die Gnadenträgerin oder der Gnadenträger der betroffenen Person Auskunft über die Gründe für den Ausgang der Gnadenentscheidung erteilen bzw. Akteneinsicht gewähren müsste. Insbesondere der dadurch entstehende Rechtfertigungszwang würde die Gnadenträgerin oder den Gnadenträger in ihrer oder seiner Handlungs- und Entscheidungsfreiheit nicht nur unerheblich beeinträchtigen. Dies wäre mit dem Wesen des Gnadeninstituts nicht vereinbar.

Eine Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten findet wie nach dem bisherigen § 2 Abs. 8 NDSG statt.

**Zu § 15 (Schutzmaßnahmen bei der Verarbeitung besonderer Kategorien personenbezogener Daten):**

§ 15 ist eine allgemeine Regelung zur Verarbeitung besonderer Kategorien personenbezogener Daten. In jeder der im Vierten Abschnitt geregelten besonderen Verarbeitungssituationen kommt auch die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikel 9 Abs. 1 DSGVO in Betracht. In diesen Fällen sind immer dem Risiko der Verarbeitung dieser Daten entsprechende Schutzmaßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorzusehen.
Die Verarbeitung personenbezogener Daten besonderer Kategorien ist gemäß Artikel 9 Abs. 1 DSGVO grundsätzlich untersagt. Dies sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
Ausnahmetatbestände zu dem Verbot sind in Artikel 9 Abs. 2 DSGVO geregelt, wobei sich einige Ausnahmen unmittelbar aus Artikel 9 Abs. 2 DSGVO ergeben (siehe Artikel 9 Abs. 2

Buchstaben a), c), e) und f) DSGVO). Soweit die Mitgliedstaaten nach den übrigen Buchstaben des Artikel 9 Abs. 2 DSGVO Ausnahmen regeln dürfen, müssen diese regelmäßig Schutzmaßnahmen für die Daten vorsehen.

Unberührt bleiben die Regelungen in Artikel 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) und Artikel 32 (Sicherheit der Verarbeitung) DSGVO, die für alle Verarbeitungen gelten, somit auch für die Verarbeitung besonderer Kategorien personenbezogener Daten i. S. v. Artikel 9 Abs. 1 DSGVO. Allerdings zeigen die Regelungen des Artikel 9 Abs. 2 DSGVO, dass hier besondere Anforderungen bestehen. Die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ist sowohl bei Artikel 25 DSGVO als auch bei Artikel 32 DSGVO zu beachten. Bei besonders sensiblen Daten müssen die Maßnahmen ausreichend wirkungsvoll sein, insbesondere müssen die Schutzmaßnahmen gemäß Artikel 32 Abs. 1 DSGVO mit angemessen starken Schutzmechanismen umgesetzt werden.
Artikel 25 DSGVO stellt Anforderungen an die Entwicklung und Implementierung von Datenverarbeitungen, um eine wirksame Umsetzung der Datenschutzgrundsätze (z. B. Datenvermeidung und Datensparsamkeit) zu erreichen. Der Verantwortliche hat hierfür geeignete technische und organisatorische Maßnahmen bei der Technikgestaltung in der Entwicklungsphase (sog. „privacy by design“) und geeignete datenschutzfreundliche Voreinstellungen in der Implementierungsphase auszuwählen (sog. „privacy by default“).
Gemäß Artikel 32 Abs. 1 Buchstabe a) DSGVO ist neben der Pseudonymisierung auch die Verschlüsselung personenbezogener Daten vorgesehen. Artikel 32 Abs. 1 Buchstabe b) sieht vor, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen. Artikel 32 Abs. 1 Buchstabe c) verlangt die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Artikel 32 Abs. 1 Buchstabe d) nennt als Maßnahme ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die Maßnahmen nach Absatz 1 und Absatz 2 sollen einen hinreichenden Schutz der Daten vor unsachgemäßer Handhabung gewährleisten. Unsachgemäße Handhabung umfasst hierbei nicht nur Missbrauch und externe Angriffe, sondern darüber hinaus auch unzureichenden Schutz vor menschlichen Fehlhandlungen, organisatorischen Mängeln, technischem Versagen und höherer Gewalt.

Zu Absatz 1:

Absatz 1 setzt das Erfordernis aus Artikel 9 Abs. 2 Buchstaben b), g) und j) DSGVO um, „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ (Buchstabe g und j) bzw. „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ (Buchstabe b) vorzusehen. Auch die zuletzt genannten geeigneten Garantien werden durch angemessene und spezifische Maßnahmen gewährleistet.

Die Nummern 1 bis 3 geben Pflichtmaßnahmen vor, die von den Verantwortlichen bzw. den Auftragsverarbeitern zwingend umzusetzen sind.

Zu Nummer 1:

Die Zuordnung der handelnden Personen zu jeder durchgeführten Aktivität der Datenverarbeitung muss zweifelsfrei festgestellt werden können. Die daraus resultierenden Schutzmaßnahmen (z. B. Protokollierungen) können zwar unbefugte Aktivitäten nicht von vornherein abblocken, sie können aber bewirken, dass zweifelhafte Aktivitäten unterbleiben, weil der „Veranlasser“ damit rechnen muss, zur Rechenschaft gezogen zu werden.

Zu Nummer 2:

Der Zugriff auf die Daten muss für die Aufgabenerfüllung auf das erforderliche Maß beschränkt werden. Die Zugriffsrechte müssen explizit erteilt werden; verboten ist, was nicht ausdrücklich erlaubt worden ist. Für die Erteilung von Zugriffsrechten müssen fachlich zuständige Stellen benannt sein. Die Regelung fordert ein, dass die Zugriffsrechte in dem Umfang beschränkt werden, wie sie für die einzelnen Personen für die ihnen übertragenen Funktionen ausreichend sind; z. B. können für einzelne Funktionen weitreichende, schreibende Rechte (z. B. Dateneingabe, Datenänderung, Datenlöschung, Datenübermittlung) erforderlich und für andere Funktionen lesende Rechte ausreichend sein. Die Erteilung der Zugriffsrechte und die technische Implementierung der Zugriffsrechte sind zu dokumentieren.

Zu Nummer 3:

Die Sensibilisierung muss für alle Personen erfolgen, die lesenden oder schreibenden Zugriff auf die personenbezogenen Daten besonderer Kategorien haben sollen. Sie muss ferner für alle Personen erfolgen, die Zugang zu den Systemen haben sollen, mit denen diese Daten verarbeitet werden (z. B. System- und Datenbankadministratoren). Sie sind darauf hinzuweisen, dass ihre Aufgaben den Umgang mit besonders sensiblen Daten umfassen und sie entsprechende Sicherheitsmaßnahmen zu ergreifen haben, die ihnen von der Dienststelle vorgegeben werden.

Zu Absatz 2:
Zusätzlich zu den sich aus Absatz 1 ergebenden Pflichtmaßnahmen können je nach Risikoeinschätzung weitere Schutzmaßnahmen zu treffen sein, wobei in Absatz 2 Nr. 1 bis 7 einschlägige Beispiele für starke Schutzmechanismen zur Erreichung der Schutzziele des Artikels 32 Abs. 1 DSGVO genannt werden.

Zu Nummer 1:
Durch die Freigabe der Datenverarbeitung im 4-Augen-Prinzip soll die Verbindlichkeit der Dateneingabe, Datenänderung und Datenlöschung sichergestellt werden. Jede IT-gestützte Verarbeitung der Daten ist dadurch – vergleichbar mit der Unterschrift zweier Personen auf einem Dokument –verifizierbar. Diese Schutzmaßnahme soll verhindern, dass unbefugte Zugriffe durch eine einzelne Person möglich sind sowie kritische Verarbeitungsvorgänge ohne Gegenkontrolle abgeschlossen werden. Ziel ist es, das Risiko von Fehlern und Missbrauch zu reduzieren.

Zu Nummer 2:
Mit der 2-Faktor-Authentisierung jedes Zugriffsberechtigten soll die Authentizität der handelnden Personen sichergestellt werden. Die Echtheit und die Zurechenbarkeit der Aktivitäten bei der Datenverarbeitung sind dadurch überprüfbar, indem die Zugriffsberechtigten nachweisen, dass sie tatsächlich diejenigen sind, für die sie sich ausgeben. Der Zugriff auf die Daten darf erst nach besonders strenger Kontrolle bei der Authentisierung der zugreifenden Person freigegeben werden. Dabei werden zwei Authentisierungstechniken kombiniert, wie beispielsweise Passwort (Nachweis erfolgt durch „Wissen“) und personenbezogenes Zertifikat auf einer Chipkarte (Nachweis erfolgt durch „Besitz“).

Zu Nummer 3:
Die hohe Sensibilität der Daten besonderer Kategorien kann es erforderlich machen, dass die Daten nur mit einer Ende - zu Ende - Verschlüsselung elektronisch übermittelt werden dürfen, um die Vertraulichkeit der Daten auf dem Transportweg über das Netz zu gewährleisten. Es handelt sich dabei um eine Schutzmaßnahme, bei der die Verschlüsselung vom Sender der Nachricht vorgenommen wird und die Entschlüsselung erst beim Empfänger der Nachricht erfolgt. Mitwissende Zwischenstationen auf dem Übertragungsweg, an denen die übertragenen Daten im Klartext vorliegen, werden dabei eliminiert.

Zu Nummer 4:
Ziel der verschlüsselten Datenspeicherung ist es, die Möglichkeit der Kenntnisnahme von Informationen durch unbefugte Beteiligte an der Datenverarbeitung mit privilegierten Rechten

(z.B. System- oder Datenbankadministratoren) zu eliminieren und damit die Vertraulichkeit während der Datenspeicherung zu gewährleisten. Bei dieser Schutzmaßnahme dürfen die Daten in einem vernetzten IT-System nur mit Verschlüsselung gespeichert werden.

Zu Nummer 5:
Ziel der Redundanz von Infrastrukturen ist die zusätzliche Bereitstellung von Ressourcen als Reserve, um bei ihrem Ausfall – z. B. infolge technischen Versagens, wegen höherer Gewalt oder infolge eines gezielten Angriffs – die Verfügbarkeit der Daten weiterhin in der benötigten Güte und mit der geforderten Unterbrechungsfreiheit gewährleisten zu können. Zur Erhöhung der Ausfall-, Funktions- und Betriebssicherheit eines IT-Systems, der Energieversorgung und der Datenübertragungseinrichtungen werden diese parallel betrieben, damit bei einem Ausfall einer Komponente die anderen den Dienst gewährleisten können. Damit soll ein Verlust von Daten, die von diesen Systemen abhängen, vermieden werden.

Zu Nummer 6:
Die Daten besonderer Kategorien müssen unversehrt und vollständig gespeichert sein oder übermittelt werden; die Datenverarbeitung muss korrekte Ergebnisse liefern. Um das Ziel der Integrität zu gewährleisten, ist eine angemessene Schutzmaßnahme auszuwählen, die verhindert, dass Daten unbefugt verändert werden oder zumindest die unbefugte Veränderung nachträglich dauerhaft festgestellt werden kann. Geeignet sind dafür beispielsweise elektronische Signaturen, weil sie über die Daten eine eindeutige, kurze Prüfsumme (Hashwert) bilden. Bei jeder Modifikation der Daten ändert sich der Hashwert, sodass bei der Verifizierung der elektronischen Signatur anhand des Vergleichs der Hashwerte erkannt wird, ob eine Manipulation oder eine andere Datenmodifizierung stattgefunden hat.

Zu Nummer 7:
Die Schulung von Personen mit Zugriffs- und Zugangsberechtigung stellt neben der verpflichtend vorzunehmenden Sensibilisierung der mit der Datenverarbeitung beauftragten Personen (Absatz 1 Nr. 3) eine weitere mögliche Schutzmaßnahme dar. Die Notwendigkeit von Schulungen ergibt sich aus den konkret vorliegenden Aufgaben, die den Umgang mit besonders sensiblen Daten zum Gegenstand haben. Ziel dieser Schutzmaßnahme ist es, menschliche Fehlhandlungen – z. B. aus Unkenntnis – zu verhindern.

Zu Absatz 3:
Absatz 3 regelt, wonach sich die Art und der Umfang der Maßnahmen nach Abs.1 und Abs. 2 richten. Die Schutzmaßnahmen müssen in einem vertretbaren Verhältnis zum Risiko der Da-

tenverarbeitung stehen. Für die Risikoeinschätzung sind insbesondere die Eintrittswahrscheinlichkeit potenzieller Gefahren und die erwartete Höhe des Schadens, der bei Eintritt des Gefahrenszenarios verursacht würde, zu berücksichtigen. Dadurch wird sichergestellt, dass die Pflichtmaßnahmen gemäß Abs. 1 in Art und Umfang derart ausgestaltet werden, dass sie das Risiko für die Grundrechte und Interessen der betroffenen Person auf ein akzeptables Maß reduzieren. Ferner wird durch den Bezug auf Abs. 2 erreicht, dass sich die Angemessenheit ausgewählter zusätzlicher Schutzmaßnahmen ebenfalls am Risiko für die Verbindlichkeit, Authentizität, Vertraulichkeit, Verfügbarkeit und Integrität dieser Daten ausrichtet.

Die Vorschriften des Artikels 35 DSGVO zur Datenschutz-Folgenabschätzung und des Artikel 36 zur vorherigen Konsultation bleiben unberührt. Insbesondere bei § 13 und § 14, aber je nach Einzelfall auch bei § 10 und § 11, dürften nicht immer umfangreiche Verarbeitungen i. S. v. Artikel 35 Abs. 3 Buchstabe b) DSGVO vorliegen, so dass eine Datenschutz-Folgenabschätzung im Einzelfall nicht zwingend angezeigt sein muss.

**Zu Abschnitt 5 (Die oder der Landesbeauftragte für den Datenschutz):**

Artikel 51 Abs. 1 DSGVO gibt den Mitgliedstaaten vor, dafür Sorge zu tragen, dass eine oder mehrere unabhängige Aufsichtsbehörden überwachen, dass die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird. In diesem Abschnitt werden die Regelungen der bisherigen §§ 21-23 NDSG an die Vorgaben der Datenschutz-Grundverordnung angepasst.

**Zu § 16 (Aufsichtsbehörde, Rechtsstellung der oder des Landesbeauftragten für den Datenschutz):**

Zu Absatz 1:
Die völlige Unabhängigkeit und Weisungsfreiheit der Aufsichtsbehörden sind unionsrechtlich vorgegeben (Artikel 16 Abs. 2 AEUV, Artikel 52 DSGVO). Die Gewährleistung der völligen Unabhängigkeit der oder des Landesbeauftragten wurde aufgrund des Urteils des Europäischen Gerichtshofs vom 09. März 2010 (C-518/07) bereits mit Gesetz vom 30. Juni 2011 (Nds. GVBl. S. 210) sichergestellt. Inhaltlich erfolgen keine Änderungen gegenüber dem bestehenden Recht.
Die Festlegung des Dienstsitzes in Satz 1 steht in unmittelbarem Sachzusammenhang zu der Errichtung und Ausstattung der Aufsichtsbehörden (Artikel 52 Abs. 4 DSGVO). Die Regelung des bisherigen § 21 Abs. 3 Satz 1 NDSG wird weitestgehend aufrechterhalten.

Artikel 51 Abs. 1 DSGVO verlangt von den Mitgliedstaaten, eine oder mehrere Aufsichtsbehörden für die Überwachung der Anwendung der Datenschutz-Grundverordnung einzurichten. Satz 2 legt die sachliche Zuständigkeit der von der oder dem Landesbeauftragten geleiteten Behörde fest. Die von der oder dem Landesbeauftragten geleitete Behörde ist Aufsichtsbehörde für die Verarbeitung personenbezogener Daten im Anwendungsbereich dieses Gesetzes. Das heißt, sie oder er übt die Aufsicht über die jeweiligen Datenverarbeitungstätigkeiten öffentlicher Stellen aus. Dies gilt sowohl für die Tätigkeiten der in § 1 genannten Stellen, soweit diese in den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung fallen, als auch für die Tätigkeiten öffentlicher Stellen, die in den erweiterten Anwendungsbereich der Datenschutz-Grundverordnung nach § 2 fallen, soweit keine spezielle Regelung besteht. Damit soll gewährleistet werden, dass alle Verarbeitungen öffentlicher Stellen in Niedersachsen nicht nur datenschutzrechtlichen Vorschriften unterliegen, sondern auch deren Einhaltung kontrolliert werden können. Da die parlamentarischen Angelegenheiten des Landtages nicht in den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung fallen, besteht hier auch keine Aufsicht durch die von der oder dem Landesbeauftragten geleitete Behörde.

Nach Artikel 55 Abs. 3 DSGVO sind die Aufsichtsbehörden nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen. Beim Landesrechnungshof als einer Einrichtung mit verfassungsrechtlich garantierter Unabhängigkeit, soweit dessen Mitglieder im Rahmen ihrer richterlichen Unabhängigkeit handeln, sollte die von der oder dem Landesbeauftragten geleitete Behörde diese Unabhängigkeit achten und bei der Ausübung ihrer oder seiner Befugnisse wahren.

Zu Absatz 2:

Nach Artikel 53 Abs. 2 DSGVO muss jedes Mitglied der Aufsichtsbehörde über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Nach Artikel 54 Abs. 1 Buchstabe b) DSGVO sieht jeder Mitgliedstaat durch Rechtsvorschriften die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung vor. Das Erfordernis („soll“) der Befähigung zum Richteramt aus dem bisherigen § 21 Abs. 1 Satz 1 NDSG wird daher in Absatz 2 zulässigerweise aufrechterhalten. Verfügt die oder der Landesbeauftragte über einschlägige Berufserfahrung im Datenschutzrecht, so kann dies die erforderliche Qualifikation, Erfahrung und Sachkunde im Bereich des Schutzes personenbezogener Daten darstellen.

Zu Absatz 3:
Nach Artikel 53 Abs. 1 DSGVO sehen die Mitgliedstaaten ein transparentes Ernennungsverfahren durch das Parlament, die Regierung, das Staatsoberhaupt oder eine unabhängige Stelle, die nach dem Recht des Mitgliedstaates mit der Ernennung betraut wird, vor. Die Mitgliedstaaten haben gemäß Artikel 54 Abs. 1 Buchstabe c) DSGVO zudem die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde zu schaffen. Satz 1 regelt in Durchführung der Artikel 53 Abs. 1 und Artikel 54 Abs. 1 Buchstaben c) und d) DSGVO das Verfahren der Ernennung und die Amtszeit der oder des Landesbeauftragten. Hierzu wird § 21 Abs. 1 Satz 2 NDSG bisheriger Fassung weitestgehend übernommen.

Die Regelung in Satz 2 zur Zulässigkeit einer einmaligen Wiederwahl entspricht den Vorgaben des Artikels 54 Abs. 1 Buchstabe e) DSGVO. Der bisherige § 21 Abs. 1 Satz 3 NDSG wird insofern konkretisiert, dass nur die einmalige Wiederwahl zulässig ist. Die Konsequenz, dass die oder der Landesbeauftragte zu einer weiteren Amtszeit berufen wird, bedarf keiner Regelung im Gesetz.

Satz 3 regelt, dass sich die Amtszeit bis zur Berufung einer Nachfolgerin oder eines Nachfolgers verlängert. Dies steht im Zusammenhang mit dem Regelungsauftrag des Artikels 54 Abs. 1 Buchstabe d) DSGVO und gewährleistet, dass keine Vakanz zwischen zwei Amtszeiten besteht. Um der ausscheidenden amtswaltenden Person eine persönliche Perspektive und Planungssicherheit zu geben, wird die Pflicht zur Weiterführung des Amtes auf höchstens sechs Monate begrenzt.

Die Beendigung des Beschäftigungsverhältnisses der Bediensteten der von der oder dem Landesbeauftragten geleiteten Behörde sowie die sonstigen in Artikel 54 Abs. 1 Buchstabe f) und Artikel 54 Abs. 2 DSGVO genannten Sachverhalte bestimmen sich nach allgemeinen beamten- und arbeitsrechtlichen Grundsätzen, so dass es hierzu Regelungen im Niedersächsischen Datenschutzgesetz nicht bedarf. Insbesondere sind in § 41 Satz 1 BeamtStG i. V. m. § 79 NBG Regelungen für Tätigkeiten nach Beendigung des Beamtenverhältnisses enthalten, die sowohl für die oder den Landesbeauftragten als auch für die Bediensteten, soweit diese sich in einem Beamtenverhältnis befinden, Geltung haben.

Zu Absatz 4:
Das Regelungserfordernis ergibt sich aus Artikel 54 Abs. 1 Buchstabe f) DSGVO im Hinblick auf die Bedingungen zur Beendigung des Beschäftigungsverhältnisses. § 21 Abs. 2 NDSG in der bisherigen Fassung kann aufrechterhalten werden. Für das Ende der Dienstzeit wird dabei – wie bisher – auf den Ablauf der Amtszeit abgestellt.

Zu Absatz 5:

Die Amtszeit der Landesbeauftragten als Aufsichtsbehörde endet nach Artikel 53 Abs. 3 DSGVO mit Ablauf der Amtszeit (Fall 1), mit Rücktritt (Fall 2) oder verpflichtender Versetzung in den Ruhestand (Fall 3). Eine verpflichtende Versetzung in den Ruhestand kommt im Falle einer Dienstunfähigkeit (§ 43 NBG) in Betracht.

Gem. Artikel 53 Abs. 4 DSGVO erfolgt eine Amtsenthebung, wenn das Mitglied der Aufsichtsbehörde (LfD) eine schwere Verfehlung begangen hat (Fall 1) oder die Voraussetzungen für die Wahrnehmung der Aufgaben nicht mehr erfüllt (Fall 2).

Der bislang in § 21 Abs. 1 Satz 5 NDSG enthaltene ausdrückliche Bezug auf die Entlassungsgründe bei einem Richterverhältnis auf Lebenszeit konnte aufgrund der Regelung in Artikel 53 Abs. 4 DSGVO nicht aufrechterhalten werden. Dennoch könnte materiell-rechtlich eine schwere Verfehlung i. S. v. Artikel 53 Abs. 4 Fall 1 DSGVO gegeben sein, wenn Gründe vorliegen, die bei einem Richterverhältnis auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen würden (§§ 94 ff NRiG i. V. m. NDiszG).

Die Voraussetzungen für die Wahrnehmung des Amtes könnten insbesondere dann nicht mehr erfüllt sein (Artikel 53 Abs. 4 Fall 2 DSGVO), wenn ein Fall der Entlassung nach § 22 Abs. 1 Nr. 1, Abs. 2 oder Abs. 3 BeamtStG oder nach § 23 Abs. 1 Satz 1 Nr. 1 oder Nr. 3 BeamtStG vorliegt oder ein Verlust der Beamtenrechte nach § 24 BeamtStG gegeben ist.

Die bislang in § 21 Abs. 1 Satz 5 NDSG geregelte Entlassung auf eigenen Antrag der oder des Landesbeauftragten (§ 23 Abs. 1 Satz 1 Nr. 4 BeamtStG) ist dem Rücktritt gem. Artikel 53 Abs. 3 Fall 2 DSGVO gleichzusetzen. Satz 1 sieht das Amtsenthebungsverfahren durch den Landtag vor, da dieser auch für die Ernennung zuständig ist (actus contrarius). Die Regelungsbefugnis ergibt sich aus Artikel 54 Abs. 1 Buchstabe f) DSGVO im Hinblick auf die Bedingungen zur Beendigung des Beschäftigungsverhältnisses. Zu einer Enthebung kommt es, wenn die oder der Landesbeauftragte eine schwere Verfehlung begangen hat oder wenn sie oder er die Voraussetzung für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt (Artikel 53 Abs. 4 DSGVO). Für die Amtsenthebung ist nach Satz 2 die Mehrheit von zwei Dritteln der Mitglieder des Landtages erforderlich. Gegenüber der Wahl nach Artikel 62 Abs. 2 Niedersächsische Verfassung – dort zwei Drittel der anwesenden Mitglieder, mindestens jedoch die Mehrheit der Mitglieder des Landtages – verlangt die Amtsenthebung eine höheres Quorum. Dadurch wird die oder der Landesbeauftragte in ihrer oder seiner Unabhängigkeit gestärkt und ihre oder seine Bedeutung als Kontroll- und Beratungsorgan unterstrichen.

Neben der Möglichkeit der Amtsenthebung sind aufgrund der Vorgaben des Artikels 53 Abs. 4 DSGVO keine weiteren disziplinarischen Maßnahmen zulässig.

Zu Absatz 6:
Sätze 1 und 2 stellen die dienstrechtliche Personalhoheit der von der oder dem Landesbeauftragten geleiteten Behörde über die Beschäftigten sicher (Artikel 52 Abs. 5 DSGVO). Satz 3 und Satz 4 entsprechen weitestgehend der bisherigen Regelung.

Zu Absatz 7:
Die von der oder dem Landesbeauftragten geleitete Behörde erhält – wie im bisherigen Recht (§ 21 b NDSG) – die Option, Aufgaben der Personalverwaltung durch eine andere öffentliche Stelle wahrnehmen zu lassen. Für die in diesem Zusammenhang erforderliche Verarbeitung von Personalaktendaten ist die Schaffung einer Rechtsgrundlage erforderlich. Auch organisatorische Aufgaben, wie z. B. Poststelle, Botendienst und Beschaffung können im Wege eines Auftrags von einer anderen Stelle wahrgenommen werden, ohne dass es dazu einer gesetzlichen Regelung bedarf. Aufgrund der freiwilligen Übertragungsmöglichkeit ist die Regelung mit den Vorgaben der Datenschutz-Grundverordnung zur völligen Unabhängigkeit der von der oder dem Landesbeauftragten geleiteten Behörde und zu ihrer Personalhoheit weiterhin vereinbar.

Zu Absatz 8:
Gemäß Artikel 52 Abs. 6 DSGVO stellt jeder Mitgliedstaat sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Der Erwägungsgrund 118 der Datenschutz-Grundverordnung stellt klar, dass die Tatsache, dass die Aufsichtsbehörden unabhängig sind, nicht bedeuten soll, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen werden. Die Finanzkontrolle findet ihre Grenzen jedoch in der Unabhängigkeit der Datenschutzaufsicht. Der Landesrechnungshof hat die Rechnungsprüfung bei der von der oder dem Landesbeauftragten geleiteten Behörde daher so durchzuführen, dass die völlige Unabhängigkeit im Sinne des Artikels 52 Abs. 1 DSGVO nicht beeinträchtigt wird.

**Zu § 17 (Aufgaben der Aufsichtsbehörde; Mitwirkung):**

Die Aufgaben der Aufsichtsbehörden sind unter anderem in Artikel 57 und Artikel 59 DSGVO verbindlich vorgegeben. Die Aufgaben der Aufsichtsbehörden decken sich überwiegend mit denen, die der von der oder dem Landesbeauftragten geleiteten Behörde nach dem bisher geltenden Recht zugewiesen wurden.

Zu Absatz 1:

Gem. Artikel 51 Abs. 1 DSGVO erfolgt eine Zuweisung der Aufgaben der Aufsichtsbehörden nach der Datenschutz-Grundverordnung an die von der oder dem Landesbeauftragten geleitete Behörde. Diese Behörde kontrolliert bei Datenverarbeitungen öffentlicher Stellen i.S.v. § 1 NDSG die Einhaltung der Vorschriften der Datenschutz-Grundverordnung, dieses Gesetzes und anderer datenschutzrechtlicher Bestimmungen. Dies gilt auch für die Bereiche, die in den erweiterten Anwendungsbereich der Datenschutz-Grundverordnung nach § 2 fallen, sofern keine speziellen Regelungen bestehen.

Zu Absatz 2:

Absatz 2 enthält einen Restbestand der Regelung im bisherigen § 22 Abs. 4 NDSG, konkret den bisherigen Satz 1. Dieser wird weitestgehend aufrechterhalten, um als Pendant zu den Befugnissen der von der oder dem Landesbeauftragten geleiteten Behörde nach Artikel 58 DSGVO den Behörden und sonstigen öffentlichen Stellen die entsprechenden Mitwirkungspflichten zuzuweisen.

Gem. Artikel 58 DSGVO muss die Aufsichtsbehörde über ausreichende Möglichkeiten verfügen, um die Verantwortlichen ggf. anzuweisen, die erforderlichen Informationen zur Verfügung zu stellen. Artikel 58 Abs. 4 DSGVO gibt den Mitgliedstaaten vor, das hierzu erforderliche Recht im Einklang mit der Charta der Grundrechte der Europäischen Union zu erlassen.

Zu Absatz 3:

§ 22 Abs. 2 NDSG in der bisherigen Fassung wird weitestgehend aufrechterhalten. Artikel 36 DSGVO sieht in Absatz 1 eine Konsultation der Aufsichtsbehörde vor der Datenverarbeitung nur für die Fälle vor, in denen aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. Artikel 36 Abs. 5 DSGVO erlaubt es den Mitgliedstaaten darüber hinaus, die Verantwortlichen zu verpflichten, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren. Im Hinblick auf den Aufbau automatisierter Informationssysteme erscheint eine frühzeitige Einbindung der von der oder dem Landesbeauftragten geleiteten Behörde weiterhin sinnvoll. Es wird wie im bisherigen Recht ein „Unterrichten“ für ausreichend gehalten, was im Rahmen des Artikel 36 Abs. 5 DSGVO zulässig ist, da dieses als ein „Weniger“ in dem Begriff „Konsultieren“ enthalten ist. „Frühzeitig“ ist eine Unterrichtung, wenn diese eine mögliche Reaktion der Aufsichtsbehörde in einem angemessenen Zeitrah-

men und ein Reagieren des Verantwortlichen darauf vor der Inbetriebnahme des automatisierten Informationssystems ermöglicht. Hier wird es auf den Einzelfall ankommen, insbesondere auf die Komplexität und Reichweite des Systems.

Die bisher in § 22 Abs. 1 Satz 4 NDSG geregelte Anhörungspflicht bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften, die Regelungen zum Recht auf informationelle Selbstbestimmung zum Gegenstand haben, ergibt sich nunmehr unmittelbar aus Artikel 36 Abs. 4 DSGVO.

**Zu § 18 (Wahrnehmung der Befugnisse der oder des Landesbeauftragten nach Artikel 58 der Datenschutz-Grundverordnung):**

Artikel 58 Abs. 4 DSGVO gibt den Mitgliedstaaten auf, ein ordnungsgemäßes Verfahren im Einklang mit der Charta festzulegen, nach dem die Aufsichtsbehörden ihre Befugnisse gem. Artikel 58 DSGVO ausüben können.

Zu Absatz 1:
Es erfolgt die Klarstellung, dass die Befugnisse der von der oder dem Landesbeauftragten geleiteten Behörde nach Artikel 58 Absatz 1 bis 3 DSGVO sich nicht nur auf Verstöße gegen die Datenschutz-Grundverordnung beziehen, sondern auch auf Verstöße gegen dieses Gesetz oder andere datenschutzrechtliche Bestimmungen.

Zu Absatz 2:
Absatz 2 führt die Befugnis der von der oder dem Landesbeauftragten geleiteten Behörde im Sinne des bisherigen § 23 NDSG fort Bestehen Anhaltspunkte dafür, dass eine Datenverarbeitung gegen die Datenschutz-Grundverordnung, dieses Gesetz oder andere datenschutzrechtliche Bestimmungen verstößt, so kann sie den Verantwortlichen oder den Auftragsverarbeiter zur Stellungnahme auffordern. Diese Befugnis ist nach Artikel 58 Abs. 1 bis 3 DSGVO nicht vorgesehen, jedoch von der Öffnungsklausel des Artikels 58 Abs. 6 DSGVO gedeckt. Nach Artikel 58 Abs. 6 DSGVO kann jeder Mitgliedstaat vorsehen, dass die Aufsichtsbehörden neben den in Artikel 58 Abs. 1, 2 und 3 DSGVO vorgesehenen Befugnissen über zusätzliche Befugnisse verfügen. Die Möglichkeit zur Einholung einer Stellungnahme stellt eine zweckmäßige zusätzliche Befugnis für die von der oder dem Landesbeauftragten geleiteten Behörde dar. Die Einholung einer Stellungnahme soll der von der oder dem Landesbeauftragten geleiteten Behörde jedoch nicht – wie bisher - verpflichtend vorgeschrieben werden, sondern vielmehr eine zusätzliche Option neben den anderen Befugnissen darstellen. Die Durchführung eines quasi vorgeschalteten Verfahrens eröffnet die ressourcensparende Möglichkeit, dass

festgestellte Verstöße gegen die Vorschriften des Datenschutzes der jeweils zuständigen Rechts- oder Fachaufsichtsbehörde mitgeteilt werden und diese vor der etwaigen Ausübung der Befugnisse nach Artikel 58 Abs. 2 DSGVO unter Setzung einer angemessenen Frist Gelegenheit zur Stellungnahme erhalten.
Durch die Unterrichtung nach Satz 2 wird insbesondere gewährleistet, dass die zuständige Rechts- oder Fachaufsichtsbehörde (bei Angelegenheiten im eigenen Wirkungskreis die Rechtsaufsichtsbehörde und bei Angelegenheiten im übertragenen Wirkungskreis die Fachaufsichtsbehörde) Kenntnis von dem Verstoß erhält, ggf. für Abhilfe sorgen kann und ansonsten vor der Ausübung weitergehender Befugnisse durch die von der oder dem Landesbeauftragten geleiteten Behörde rechtliches Gehör findet. Die Gefahr divergierender Maßnahmen von Datenschutzaufsicht und der Rechts- bzw. Fachaufsicht wird hierdurch reduziert. Sätze 2 und 4 unterfallen der nationalen Organisationshoheit. Die Regelung in Satz 3 erfolgt in Konsequenz zu Satz 1.

Zu Absatz 3:
Die Regelung erweitert die bislang in § 22 Abs. 4 Satz 2 Nr. 3 NDSG normierten Rechte der von der oder dem Landesbeauftragten geleiteten Behörde. Gemäß Artikel 58 Abs. 1 Buchstabe f) DSGVO hat sie nach dem mitgliedstaatlichen Recht Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, zu erhalten. In diesem Sachzusammenhang steht die hier – zulässigerweise - wiederholte Regelung des Artikel 58 Abs. 1 Buchstabe e) DSGVO, nach der die von der oder dem Landesbeauftragten geleiteten Behörde zudem Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten hat.

Absatz 4:
Mit der Regelung in Absatz 4 wird von der Öffnungsklausel des Artikels 83 Abs. 7 DSGVO Gebrauch gemacht. Es wird geregelt, ob und in welchem Umfang gegen Behörden und sonstige öffentliche Stellen Geldbußen verhängt werden können. Es soll sichergestellt werden, dass öffentliche Stellen, die im Rahmen ihrer Tätigkeit im Wettbewerb mit anderen Verarbeitern stehen, gegenüber ihren Mitbewerbern nicht dadurch bessergestellt werden, dass ihnen gegenüber kein Bußgeld verhängt werden kann.

Dass die von der oder dem Landesbeauftragten geleitete Behörde zur Durchsetzung der Befugnisse nach Artikel 58 DSGVO gegenüber juristischen Personen des öffentlichen Rechts und Behörden keine Zwangsmaßnahmen ausüben darf, ergibt sich bereits aus den allgemeinen verwaltungsvollstreckungsrechtlichen Vorschriften (§ 70 Abs. 1 NVwVG i. V. m. § 64 ff. Nds. SOG, insbesondere im Umkehrschluss zu § 64 Abs. 2 Satz 3 Nds. SOG).

**Zu § 19 (Stellungnahme zum Tätigkeitsbericht)**

Artikel 59 DSGVO schreibt als unmittelbar geltendes Recht die Vorlage eines jährlichen Tätigkeitsberichtes durch die Aufsichtsbehörde an das Parlament und die Regierung vor. Eine Übermittlung an andere Behörden könnte geregelt werden, erscheint jedoch nicht erforderlich. § 22 Abs. 3 Satz 1 NDSG in der bisherigen Fassung sah ebenfalls nur eine Vorlage gegenüber dem Landtag vor. Mit § 19 erfolgt – wie bisher in § 22 Abs. 3 Satz 2 NDSG - die Verpflichtung der Landesregierung, zu dem Bericht Stellung zu nehmen. Die Datenschutz-Grundverordnung enthält keine Vorgabe, zu diesem Bericht eine Stellungnahme abzugeben. Dieses liegt jedoch in der mitgliedstaatlichen Entscheidungshoheit. An dem bisherigen Verfahren, das ggf. auch eine Erörterung im Landtag umfasst, soll festgehalten werden.

**Zu § 20 (Aufsichtsbehörde für die Datenverarbeitung außerhalb des Anwendungsbereichs dieses Gesetzes):**

Satz 1 orientiert sich an der bisherigen Regelung des § 22 Abs. 6 NDSG. Nach § 40 BDSG überwachen die nach Landesrecht zuständigen Behörden bei den nichtöffentlichen Stellen die Anwendung der Vorschriften über den Datenschutz. Es wird hier auch auf Artikel 51 DSGVO Bezug genommen, da die Aufsichtsbehörde im Sinne des § 40 BDSG auch Aufsichtsbehörde im Sinne des Artikels 51 Abs. 1 DSGVO ist. Gem. Artikel 62 Abs. 4 Satz 3 Niedersächsische Verfassung kann eine solche Aufgabenübertragung bzgl. der nicht öffentlichen Stellen, aber auch bzgl. der öffentlich-rechtlichen Wettbewerbsunternehmen, durch Gesetz erfolgen.
Satz 2 erklärt § 17 Abs. 1 und § 18 Abs. 1 für entsprechend anwendbar.

**Zu Abschnitt 6 (Schlussvorschriften):**

**Zu § 21 (Ordnungswidrigkeiten):**

Zu Absatz 1:
In Artikel 83 DSGVO sind die Bedingungen und Tatbestände für die Verhängung von Geldbußen gegen Verantwortliche und Auftragsverarbeiter bei Verstößen gegen die Datenschutz-Grundverordnung geregelt.
§ 21 umfasst hingegen rein nationale Tatbestände, die weiterhin neben der Datenschutz-Grundverordnung zulässigerweise geregelt werden dürfen.
§ 21 Abs. 1 greift die bisher geltende Rechtslage auf, nach der Geldbußen auch gegenüber Mitarbeiterinnen und Mitarbeitern öffentlicher Stellen (§ 29 Abs. 1 Nr. 1 i. V. m § 5 NDSG) bzw.

generell gegenüber natürlichen Personen bei Vortäuschung falscher Tatsachen (§ 29 Abs. 1 Nr. 2 NDSG) möglich waren.
Bei beiden Nummern des § 21 Abs. 1 geht es nicht um Verstöße gegen Vorschriften der Datenschutz-Grundverordnung oder andere datenschutzrechtliche Vorschriften; vielmehr gründet der Unrechtsgehalt auf anderen Tatsachen.
Der Unrechtsgehalt in § 21 Abs. 1 Nr. 1 ist weiterhin, dass eine Mitarbeiterin oder ein Mitarbeiter einer öffentlichen Stelle eine Verarbeitung zu einem anderen Zweck als zu demjenigen, der zu ihren oder seinen rechtmäßigen Aufgaben gehört, vornimmt. Es geht somit um Kompetenzüberschreitungen.
Der Unrechtsgehalt in § 21 Abs. 1 Nr. 2 ist in dem Vortäuschen falscher Tatsachen begründet. Täterin oder Täter kann jede natürliche Person sein. Der Tatbestand der Nummer 2 Fall 1 wurde auf das Verschaffen auch für eine andere Person erweitert. Damit ist das bisherige Ungleichgewicht zu Nummer 2 Fall 2, der auch schon bisher die Übermittlung an sich oder eine andere Person umfasst hat, beseitigt. Darüber hinaus ist durch die Formulierung „die im Anwendungsbereich dieses Gesetzes verarbeitet werden“ klargestellt, dass es sich nur um eine Verarbeitung öffentlicher Stellen nach § 1 und § 2 handeln kann.

Zu Absatz 2:
Die mögliche Bußgeldhöhe wird entsprechend dem bisherigen § 29 Abs. 2 NDSG auf bis zu fünfzigtausend Euro beschränkt. Der deutlich höhere Bußgeldrahmen in Artikel 83 Abs. 5 und Abs. 6 DSGVO für Bußgelder gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter im Wirtschaftsbereich, einschließlich Großkonzernen, kann hingegen nicht Maßstab für ein Bußgeld gegenüber Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen bzw. sonstigen natürlichen Personen für rein nationale Tatbestände sein.

Mit dem normierten Bußgeldrahmen sind die in § 21 geregelten Sanktionen wirksam, verhältnismäßig und abschreckend.

**Zu § 22 (Straftaten)**
Die Tatbestände, die nach § 21 bußgeldbewehrt sind, sind nach § 22 strafbewehrt, wenn diese gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht begangen werden. Die Regelung entspricht in wesentlichen Teilen dem bisherigen § 28 NDSG.

Strafrahmen und Versuchsstrafbarkeit sind unverändert geblieben. Die Tat wird nunmehr nur auf Antrag verfolgt, wobei die Antragsberechtigung sich auf die betroffene Person, den Verantwortlichen, den Auftragsverarbeiter und die von der oder dem Landesbeauftragten geleitete Behörde erstreckt.

Mit dem normierten Strafrahmen sind die in § 22 geregelten Sanktionen wirksam, verhältnismäßig und abschreckend.

**Zu § 23 (Übergangsvorschrift):**

Mit § 23 wird eine Übergangsregelung für die zum Zeitpunkt des Inkrafttretens des Gesetzes im Amt befindliche Landesbeauftragte für den Datenschutz geschaffen. Nach Satz 1 gilt die am 24. Mai 2018 im Amt befindliche Landesbeauftragte für den Datenschutz für den Rest ihrer Amtszeit als nach § 16 Abs. 3 Satz 1 berufen. Damit wird insbesondere klargestellt, dass keine erneute Berufung zu erfolgen hat und die Dauer der Amtszeit von 8 Jahren nach § 16 Abs. 3 Satz 1 nicht neu beginnt. Nach Satz 2 richten sich ihre Rechtsstellung sowie ihre Aufgaben und Befugnisse nach den Vorschriften der Datenschutz-Grundverordnung und nach den §§ 16 bis 20.

**Zu Artikel 2 (Änderung des Niedersächsischen Archivgesetzes):**

Zu Nummer 1: Änderung von § 3 (Ermittlung und Übernahme von Archivgut)

Zu a): Änderung von Absatz 1

Durch den geänderten Satz 2 wird von der Öffnungsklausel des Artikels 9 Abs. 2 Buchstabe j der Datenschutz-Grundverordnung Gebrauch gemacht und auch explizit solches Schriftgut in das der Anbietungspflicht unterliegende Schriftgut einbezogen, das besondere Kategorien personenbezogener Daten enthält, deren Verarbeitung nach Artikel 9 Abs. 1 der Datenschutz-Grundverordnung grundsätzlich untersagt ist.
Nach Artikel 9 Abs. 1 der Datenschutz-Grundverordnung handelt es sich dabei um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeiten hervorgehen, sowie um genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung.
Da bereits die Anbietung von Schriftgut ein Verarbeiten von Daten im Sinn der Definition des Artikels 4 Ziffer 2 der Datenschutz-Grundverordnung darstellt, bedarf die Anbietungsverpflichtung von Schriftgut, das diese besonderen Kategorien personenbezogener Daten enthält, einer gesetzlichen, den Anforderungen des Artikels 9 Abs. 2 Buchstabe j der Datenschutz-Grund-verordnung entsprechenden Grundlage im nationalen Recht.

Das Niedersächsische Archivgesetz enthält strenge datenschutzrechtliche Vorgaben für die Nutzung von Archivgut und stellt insbesondere durch die differenzierte Ausgestaltung der Schutzfristen einen angemessenen Ausgleich zwischen den Rechten auf Datenschutz einerseits und auf Informationszugang andererseits her. Es sieht damit angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen betroffener Personen im Sinn des Artikels 9 Abs. 2 Buchstabe j Datenschutz-Grundverordnung vor.

Zu b): Änderung von Absatz 6

Die Ausdehnung der Anwendungsregelung im neu gebildeten Satz 2 auf die dort eingefügten §§ 3 a, 3 b und 6 a stellt sicher, dass deren Regelungsgehalt, insbesondere die Ermächtigungsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten im Sinn des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung und der Ausschluss von Rechten und Pflichten nach der Datenschutz-Grundverordnung, auch Anwendung findet, soweit die in § 7 Abs. 1 genannten Einrichtungen ihr Schriftgut dem Landesarchiv zur Übernahme anbieten. Die übrigen Verweisungen bleiben unberührt.

Zu Nummer 2: §§ 3 a und 3 b (Löschung personenbezogener Daten in Schriftgut und Verarbeitung besonderer Kategorien personenbezogener Daten)

Die Regelung des § 3 a bestimmt, wann der im öffentlichen Interesse liegende Archivzweck im Sinn des Artikels 17 Abs. 3 Buchst. d der Datenschutz-Grundverordnung nicht mehr besteht mit der Folge, dass dem Löschungsverlangen nach Artikel 17 Abs. 1 Buchst. a der Datenschutz-Grundverordnung Rechnung zu tragen ist. Die Vorschrift soll damit sicherstellen, dass die Löschung personenbezogener Daten, die für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, bis zu einer Entscheidung, ob es sich bei dem die betreffenden personenbezogenen Daten enthaltenen Schriftgut um Archivgut handelt, zurückgestellt wird.
Die Regelungsbefugnis für diese Modifikation der Löschungspflicht ergibt sich aus Artikel 6 Abs. 2, Abs. 3 i.V.m. Artikel 17 Abs. 3 Buchst. d der Datenschutz-Grundverordnung, wonach der nationale Gesetzgeber berechtigt ist, spezifischere Bestimmungen darüber zu treffen, wann und unter welchen Umständen im öffentlichen Interesse liegende Archivzwecke einer Löschung personenbezogener Daten entgegenstehen.
Die Festlegung einer Frist von sechs Monaten für die Feststellung der Archivwürdigkeit stellt einen angemessenen Interessenausgleich zwischen den archivrechtlichen Belangen und den Rechten der betroffenen Personen dar.

Die Regelung des § 3 b beruht auf der Öffnungsklausel des Artikels 9 Abs. 2 Buchstabe j der Datenschutz-Grundverordnung und bildet eine Ermächtigungsgrundlage für das Archivieren von Schriftgut, das besondere Kategorien personenbezogener Daten im Sinn des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung enthält.
Neben dem Anbieten von personenbezogenen Daten enthaltenen Schriftguts erfüllt auch das Archivieren von diese Daten enthaltenen Unterlagen den Tatbestand des in Artikel 4 Ziffer 2 Datenschutz-Grundverordnung definierten Merkmals „Verarbeiten“. Um das Landesarchiv auch nach Geltung der Datenschutz-Grundverordnung in die Lage zu versetzen, das von nach § 1 Abs. 1 Satz 1 und Abs. 2 zur Anbietung verpflichteten Stellen angebotene Schriftgut ohne Differenzierung nach bestimmten Datenkategorien als Archivgut übernehmen und archivieren und dadurch eine alle Lebensbereiche umfassende historische Überlieferung abbilden zu können, ist eine ausdrückliche Ermächtigungsgrundlage für die Verarbeitung der in Artikel 9 Abs. 1 Datenschutz-Grundverordnung genannten Datenkategorien im Niedersächsischen Archivgesetz erforderlich. Den Grundrechten und Interessen der betroffenen Personen auf Schutz ihrer Daten wird durch die differenzierte Ausgestaltung der Schutzfristen für die Nutzung von Archivgut hinreichend und abschließend Rechnung getragen. Das Niedersächsische Archivgesetz genügt damit den Anforderungen des Artikels 9 Abs. 2 Buchst. j Datenschutz-Grundverordnung an das die Verarbeitung besonderer Kategorien personenbezogener Daten regelnde nationale Recht.

Die in dem Vorgang des Archivierens stets vorliegende Weiterverarbeitung von zu einem anderen Zweck erhobenen Daten gilt gemäß Artikel 5 Abs. 1 Buchstabe b der Datenschutz-Grundverordnung nicht als unvereinbar mit den ursprünglichen Zwecken der Ersterhebung.

Zu Nummer 3: Änderung von § 5 (Nutzung von Archivgut)

Zu a): Änderung von Absatz 2

Mit den Änderungen werden Begriffsbestimmungen des Niedersächsischen Archivgesetzes dem Sprachgebrauch der Datenschutz-Grundverordnung angepasst. Der bisher verwendete Begriff des „Betroffenen“ wird durch „betroffene Person“ im Sinn des Artikels 4 Ziffer 1 der Datenschutz-Grundverordnung ersetzt.

Zu b): Änderung von Absatz 3

Grund dieser Änderungen ist die aktuelle Novellierung des Bundesarchivgesetzes.

Die Verweisungen in Absatz 3 auf Vorschriften des Bundesarchivgesetzes für die Nutzung von Archivgut, das dem Sozialgeheimnis unterliegende Daten enthält oder nach anderen Rechtsvorschriften des Bundes der Geheimhaltung unterliegt, sowie im Zusammenhang mit Archivgut, das Stellen des Bundes dem Landesarchiv übergeben haben, wurden an das neue Bundesarchivgesetz vom 10. März 2017 (BGBl. I S. 410) angepasst.
Inhaltliche Änderungen sind damit nicht verbunden.

Zu c): Änderung von Absatz 5

Vgl. Begründung zu Nummer 3 Buchstabe a.

Zu Nummer 4: Änderung von § 6 (Recht auf Auskunft und Gegendarstellung)

Zu a): Änderung der Absätze 1 und 2

Absatz 1 fasst die bisherigen Absätze 1 und 3 zusammen und regelt, unter welchen Voraussetzungen die Erteilung der Auskunft nach Artikel 15 der Datenschutz-Grundverordnung abzulehnen ist.
Die mit den in Satz 1 Ziffern 1 bis 3 genannten Ablehnungsgründen einhergehenden Beschränkungen des Auskunftsanspruchs nach Artikel 15 der Datenschutz-Grundverordnung sowie der in Satz 5 enthaltene Ausschluss über § 6 Abs. 1 hinausgehender Ansprüche beruhen auf der Öffnungsklausel des Artikels 89 Abs. 3 der Datenschutz-Grundverordnung.
Diese ermöglicht es den Mitgliedsstaaten, für im öffentlichen Interesse liegende Archivzwecke im nationalen Recht Ausnahmen u.a. von dem Betroffenenrechten des Artikels 15 der Datenschutz-Grundverordnung vorzusehen, soweit die Ausübung dieses Rechts die Verwirklichung von Archivzwecken unmöglich machen oder ernsthaft beeinträchtigen würde.
In Archiven werden Daten nicht zur originären Wahrnehmung öffentlicher Aufgaben erhoben, sondern Daten verarbeitet, die andere öffentliche Stellen zur Erfüllung ihrer Aufgaben nicht mehr benötigen. Aufgabe der Archive ist es, diese Daten langfristig zu sichern und zu erhalten sowie berechtigten Nutzern und betroffenen Personen unter Einhaltung archivgesetzlich festgelegter strenger Datenschutzvorgaben zugänglich zu machen.
Das umfassende Auskunftsrecht gemäß Artikel 15 der Datenschutz-Grundverordnung ginge weit über diese Zielrichtung und die Kernaufgaben öffentlicher Archive hinaus.
So sind bei nicht erschlossenem Archivgut namentliche Bezüge nur mit erheblichem Aufwand recherchierbar. Dieser Umstand, die regelmäßige Durchsicht großer Mengen von Archivgut

zum Zweck der Auskunftserteilung und die in Artikel 15 Datenschutz-Grundverordnung niedergelegten Informationspflichten beeinträchtigten die Funktionsfähigkeit öffentlicher Archive ernsthaft.
Die konkrete Ausgestaltung des Rechts auf Auskunft und Einsichtnahme in § 6 Abs. 1 und Abs. 2 berücksichtigt gleichermaßen die schutzwürdigen Belange betroffener Personen einerseits und die Bedürfnisse des Niedersächsischen Landesarchivs bei der Wahrnehmung seiner Aufgaben andererseits.

Die in den Ziffern 4 und 5 geregelten Gründe für die Ablehnung der Auskunft gehen auf die Öffnungsklausel des Artikels 23 der Datenschutz-Grundverordnung zurück.
Diese Öffnungsklausel erlaubt den Mitgliedsstaaten, durch Rechtsvorschriften Rechte betroffener Personen einzuschränken, wenn dies aufgrund übergeordneter öffentlicher Interessen, u.a. der Aufrechterhaltung der nationalen oder öffentlichen Sicherheit, der Landesverteidigung, der Verfolgung von Straftaten oder aufgrund von Rechten und Freiheiten anderer Personen, erforderlich ist.

Die Sätze 3 und 4 stellen sicher, dass durch die Angabe einer Begründung für die Ablehnung der Auskunft oder Einsichtnahme nicht der der Ablehnung zugrunde liegende Zweck offenbart werden muss.

Infolge der Neufassung von Absatz 1 war eine sprachliche Anpassung in Absatz 2 erforderlich. Die in der neuen Fassung enthaltene Ermächtigung des Landesarchivs, anstelle der Auskunft Einsichtnahme in das Archivgut zu gewähren, steht mit der Datenschutz-Grundverordnung in Einklang.

Zu b): Streichung des bisherigen Absatzes 3

Es handelt sich um eine Folgeänderung zu a).

Zu c): Änderung von Absatz 4

Bei den Änderungen in Absatz 4 handelt es sich zum einen um eine Folgeänderung zu a) und b). Zum anderen werden Begriffsbestimmungen an den Sprachgebrauch der Datenschutz-Grundverordnung angepasst.

Zu Nummer 5: neuer § 6 a (Ausschluss von Rechten und Pflichten nach der Datenschutz-Grundverordnung)

Der neue § 6 a setzt ebenfalls die Öffnungsklausel des Artikels 89 Abs. 3 Datenschutz-Grundverordnung um und schließt die Betroffenenrechte der Artikel 16 Satz 1, 18, 20 und 21 sowie die Mitteilungspflicht nach Artikel 19 der Datenschutz-Grundverordnung aus. Die Ausübung dieser Rechte und Pflichten stünde in erheblichem Maß im Widerspruch zu im öffentlichen Interesse liegenden Archivzwecken.

Gemäß Artikel 16 Satz 1 haben betroffene Personen das Recht, die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.
Eine Berichtigung im Sinn einer die betreffenden Daten verändernden Korrektur würde dem Grundgedanken des Archivwesens, unverfälschte Überlieferungen historischer Zusammenhänge aufzuzeigen, widersprechen. Bei Verwaltungsentscheidungen etwa ließe sich im Fall einer nachträglichen Korrektur nicht mehr nachvollziehen, auf welcher Grundlage die Entscheidungen gefällt wurden. Auch haben Archive praktisch kaum Möglichkeiten, im Nachhinein die Richtigkeit der von anderen Behörden erhobenen Daten zu überprüfen. Öffentliche Archivzwecke und der Schutz des teilweise auch materiell werthaltigen Archivguts stehen einer Veränderung des archivischen Datenbestands lediglich bei Hinzufügen modifizierender Hinweise nicht entgegen.

Artikel 18 Datenschutz-Grundverordnung räumt betroffenen Personen ein Recht auf Einschränkung der Verarbeitung personenbezogener Daten ein.
Eine solche Einschränkung der Datenverarbeitung ist mit Archivzwecken unvereinbar. Denn es ist gerade Aufgabe der Archive, Vorgänge und Zusammenhänge als unverfälschte historische Überlieferungen für die Nachwelt nutzbar zu machen. Eine Einschränkung der Verarbeitung stünde dieser Zielsetzung entgegen, weil ein weiteres Archivieren der betreffenden Daten ausgeschlossen wäre. Den Rechten der betroffenen Personen wird bereits durch die geltenden archivgesetzlichen Bestimmungen, insbesondere durch die Schutzfristen und den Anspruch auf Berichtigung, hinreichend Rechnung getragen.

Artikel 19 der Datenschutz-Grundverordnung sieht eine Mitteilungspflicht der datenverarbeitenden Stelle im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung vor.
Eine Pflicht, sämtlichen Empfängern, denen im Rahmen der Nutzung von Archivgut personenbezogene Daten offengelegt wurden, jede Berichtigung mitzuteilen, stellte wegen des damit

verbundenen erheblichen Aufwands die Funktionsfähigkeit öffentlicher Archive ernsthaft in Frage.

Artikel 20 der Datenschutz-Grundverordnung beinhaltet ein Recht der betroffenen Person auf Datenübertragbarkeit dergestalt, von der datenverarbeitenden Stelle eine elektronische und strukturierte Kopie ihrer Daten in einem gängigen und für die Weiterverarbeitung geeigneten Format anzufordern.
Die Ausübung dieses Rechts hätte zur Folge, dass Archive in nicht unerheblichem Umfang Datenverarbeitungsprozesse durchführen müssten. Die von Artikel 20 Datenschutz-Grundverordnung erfassten Daten müssten, sofern sie bislang nur in analoger Form vorliegen, in ein strukturiertes, gängiges und maschinenlesbares Format übertragen werden, was nicht zu den Kernaufgaben öffentlicher Archive zählt. Auch eine derartige Verpflichtung beeinträchtigte wegen des damit einhergehenden Arbeitsaufwands öffentliche Archivzwecke ernsthaft.

Ein Ausschluss der Verarbeitung personenbezogener Daten infolge eines Widerspruchs einer betroffenen Person in Ausübung ihres Rechts aus Artikel 21 Datenschutz-Grundverordnung schließlich würde ein weiteres Archivieren dieser Daten verhindern und damit die Verwirklichung öffentlicher Archivzwecke im Ergebnis unmöglich machen.

Zu Nummer 6: Änderung § 7 (Archivgut des Landtages, der kommunalen Körperschaften und sonstiger Einrichtungen)

Zu a): Änderung der Überschrift

Die Überschrift trägt nunmehr dem Regelungsgehalt des § 7 Rechnung, der über die ausschließliche Sicherung des Archivgutes des Landtages, der kommunalen Körperschaften und sonstigen Einrichtungen hinausgeht.

Zu b): Absatz 3

Die Aufnahme der §§ 3 a, 3 b und 6 a in die Verweisung des Absatzes 3 Satz 2 gewährleistet die Anwendung dieser Vorschriften, soweit die in § 7 Abs. 1 Satz 1 genannten Einrichtungen selbst Archive unterhalten oder ihr Archivgut an Archive einer anderen in § 7 Abs. 1 Satz 1 genannten Einrichtung abgeben.

**Zu Artikel 3 (Änderung des Niedersächsischen Mediengesetzes):**

Zu Nummer 1:

Zu Absatz 1:

Mit dem neuen § 54 wird klargestellt, dass die Abweichungsbefugnis des Art. 85 Datenschutz-Grundverordnung für sämtliche Anwendungsbereiche zum Tragen kommen soll. Danach können von den Kapiteln II (Grundsätze), III (Rechte der betroffenen Person), IV (Verantwortlicher und Auftragsverarbeiter), V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), VI (Unabhängige Aufsichtsbehörden), VII (Zusammenarbeit und Kohärenz) und IX (Vorschriften für besondere Verarbeitungssituationen) der Datenschutz-Grundverordnung im Hinblick auf die Meinungs- und Pressefreiheit Abweichungen oder Ausnahmen zugelassen werden.

Die Sätze 1 bis 3 übernehmen für den Bereich der Telemedien nahezu wortgleich die Regelungen des bisherigen § 5 BDSG zum Datengeheimnis. Soweit die öffentlich-rechtlichen Rundfunkanstalten, private Rundfunkveranstalter oder Presseunternehmen als Anbieter auftreten, gelten für sie die Datenverarbeitungsregelungen in § 57 Rundfunkstaatsvertrag. Lediglich für Anbieter von Telemedien, die mit den in § 57 Rundfunkstaatsvertrag genannten Stellen vergleichbar sind, bleibt eine Regelungslücke, deren Regelung dem Landesgesetzgeber vorbehalten bleibt. Da die Datenschutz-Grundverordnung von einem weiten Journalismusbegriff ausgeht (siehe Erwägungsgrund 153 der Verordnung), soll auch für diese vergleichbaren Telemedienanbieter das Medienprivileg anwendbar sein. Gedacht ist dabei vor allem an Betreiber von Blogs etc., die also weder als Rundfunkveranstalter firmieren noch in gedruckter Form veröffentlichen. Die Formulierung „vergleichbar“ soll dabei eine Abgrenzung ermöglichen zwischen journalistisch tätigen Personen und den Urhebern aller weiteren Veröffentlichungen, die zwar die Meinungsfreiheit für sich in Anspruch nehmen können, aber nicht dem Medienprivileg unterfallen sollen. Für den Gesetzgeber müssen sie mit den in § 57 Rundfunkstaatsvertrag genannten Stellen vergleichbar sein, also mit den öffentlich-rechtlichen Rundfunkanstalten, mit privaten Rundfunkveranstaltern oder mit Presseunternehmen. Vergleichbarkeit heißt indessen nicht völlige Gleichheit. Gegeben sein sollte also vor allem eine verstetigte und professionelle Arbeitsstruktur.

Die Regelungen dienen dem Ziel der Sicherheit der Datenverarbeitung; der Verantwortliche hat sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind gesetzlich dazu verpflichtet. „Verarbeiten“ ist gemäß Artikel 4 Absatz 2 Datenschutz-Grundverordnung der Oberbegriff für alle denkbaren Formen des datenschutzrechtlich rele-

vanten Umgangs mit Daten. Für journalistische Zwecke wird im Bereich der Verarbeitung personenbezogener Daten die Anwendung der Datenschutz-Grundverordnung generell beschränkt auf deren Kapitel I, VIII, X und XI, die die Datenschutz-Grundverordnung abweichungsfest vorgibt, sowie auf Artikel 5 Absatz 1 Buchst. f, Artikel 24 und 32 Datenschutz-Grundverordnung, die die Festlegung der Aufgaben des für die Datenverarbeitung Verantwortlichen und die Sicherheit der Datenverarbeitung (einschließlich Geheimhaltung) betreffen.

Indem Artikel 5 Absatz 1 Buchst. f, Artikel 24, 32 Datenschutz-Grundverordnung für anwendbar erklärt werden, wird die Rechtslage unter Geltung des sog. Medienprivilegs abgebildet. Presse, Rundfunk und diesen gleichgestellte Medien waren auch bisher bei der Ausübung ihrer journalistischen Tätigkeit insoweit privilegiert, als sie vom geltenden Datenschutzrecht nur die Vorschriften zum Datengeheimnis und zur Datensicherheit beachten mussten und sich bei Verstößen schadensersatzpflichtig machten. Die Aufrechterhaltung dieser Situation wird auch unter Geltung der Grundverordnung für erforderlich gehalten.

Zu Absatz 2:

Die Regelung ist erforderlich, um den Quellenschutz als wesentlichen Bestandteil der Pressefreiheit nicht leerlaufen zu lassen, indem entsprechende Daten zu Quellen auf Anfrage Betroffener herausgegeben werden müssten. Zwar wird grundsätzlich ein Auskunftsanspruch Betroffener normiert. Für den Bereich der journalistischen Verarbeitung personenbezogener Daten sollen subjektive Rechtsansprüche Betroffener bezüglich der Datenverarbeitung im Rahmen der rechtlichen Möglichkeiten jedoch ausgeschlossen werden, wenn bei Abwägung der schutzwürdigen Interessen der Beteiligten der Quellenschutz aus den in § 57 Absatz 2 Satz 2 Nummern1 bis 3 Rundfunkstaatsvertrag genannten Gründen höher zu werten ist. Es bleibt ein Anspruch wie in den Absätzen 3 und 4 des Entwurfs normiert, wonach Gegendarstellungen, Widerrufe, Gerichtsentscheidungen etc. zu zugrundeliegenden personenbezogenen Daten zu nehmen sind und ggf. mit diesen zusammen übermittelt werden müssen.

Absatz 2 des Entwurfs entspricht inhaltlich weitgehend § 57 Absatz 2 Rundfunkstaatsvertrag und beabsichtigt jedenfalls eine inhaltlich gleichlaufende Rechtsfolge. Auf Hinweis der Arbeitsgruppe Rechtsvereinfachung wurden davon sprachlich abweichend die Voraussetzungen für das Auskunftsrecht und die Verweigerungsgründe voneinander getrennt und eine rechtlich transparente Struktur vorgeschlagen: Satz 1 = Recht auf Auskunft; Satz 2 = Verweigerungsgründe; Satz 3 = Modifikation der Verweigerungsgründe durch Interessenabwägung. Anders als im Rundfunkstaatsvertrag („kann verlangen“) wird ein Auskunftsanspruch eingeräumt, weil sich nur dieser mit einem Katalog von Verweigerungsgründen verträgt. Anstelle von „gespeichert, verändert, übermittelt, gesperrt oder gelöscht“ wird von „verarbeiten“ gesprochen, weil davon ausgegangen wird, dass keine der in Artikel 4 Nr. 2 DSGVO genannten „Verarbeitungsmodalitäten“ ausgeschlossen werden soll. Verzichtet wurde auf die Passage „und wird die

betroffene Person dadurch in ihrem Persönlichkeitsrecht beeinträchtigt“. Nach der Regelung wird damit eine Anspruchsvoraussetzung geregelt, ohne dass klar wird, wer das Vorliegen dieser Voraussetzung feststellen soll. In jedem Fall dürfte die Voraussetzung keine beschränkende Funktion haben, da wohl jede Verarbeitung personenbezogener Daten (ohne Einwilligung) einen Eingriff in das Recht auf informationelle Selbstbestimmung bedeutet.

Im Vergleich zu § 57 Rundfunkstaatsvertrag ebenfalls auf Hinweis der Arbeitsgruppe Rechtsvereinfachung sprachlich umgestaltet und damit im Ergebnis vereinfacht wurde die Aufzählung der Verweigerungsgründe. Statt einer enumerativen Aufzählung mit zahlreichen Details und den damit ggf. verbundenen Abgrenzungsproblemen wurden „Rechte oder Interessen Dritter“ und „die journalistische Arbeit“ als zusammenfassende Oberbegriffe gefunden, bei deren Verletzung die Auskunft verweigert werden kann.

Zu den Absätzen 3 und 4:

Im Anwendungsbereich des Medienprivilegs würde das Recht auf freie Meinungsäußerung leerlaufen, wenn Berichtigungs- und Löschungsansprüche vollumfänglich zur Durchsetzung gelangten. So kommt eine Verpflichtung zur Berichtigung oder Löschung bereits veröffentlichter oder zur Veröffentlichung vorgesehener journalistischer Erzeugnisse gemäß den Vorgaben der Datenschutz-Grundverordnung nicht ohne weiteres in Betracht. Das Recht auf informationelle Selbstbestimmung vermittelt gleichwohl einen Anspruch des Betroffenen auf Gewährleistung von Vollständigkeit und Richtigkeit seiner Daten. Ein Ausgleich dieser Interessen wird mit der Verpflichtung zur parallelen Aufbewahrung und Übermittlung erzielt.

Anders als in § 57 Absatz 2 Rundfunkstaatsvertrag werden für Auskunft und Berichtigung zur besseren Strukturierung getrennte Absätze vorgesehen. Zudem wird die Häufung von Nominalisierungen vermieden und klargestellt, dass auf ein bestimmtes Verlangen etwas zu tun ist. Die rechtlich relevante Regelung ist, dass auf Verlangen etwas zu tun ist und nicht, dass man etwas verlangen kann.

Zu Nummer 2:

§ 55 ist an die neuen europarechtlichen Vorgaben anzupassen und Verfahrensfragen in der Zusammenarbeit zwischen der oder dem Landesbeauftragten für Datenschutz und der Landesmedienanstalt sind zu regeln.

**Zu Artikel 4 (Änderung des Niedersächsischen Pressegesetzes):**

Mit § 19 wird klargestellt, dass die Abweichungsbefugnis des Art. 85 Datenschutz-Grundverordnung für sämtliche Anwendungsbereiche zum Tragen kommen soll. Danach können von den Kapiteln II (Grundsätze), III (Rechte der betroffenen Person), IV (Verantwortlicher und

Auftragsverarbeiter), V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), VI (Unabhängige Aufsichtsbehörden), VII (Zusammenarbeit und Kohärenz) und IX (Vorschriften für besondere Verarbeitungssituationen) der Datenschutz-Grundverordnung im Hinblick auf die Meinungs- und Pressefreiheit Abweichungen oder Ausnahmen zugelassen werden.

Die Sätze 1 bis 3 übernehmen für den Bereich der Presse nahezu wortgleich die Regelungen des bisherigen § 5 BDSG zum Datengeheimnis. Um Unsicherheiten für die Praxis zu vermeiden, wurde der bestehende Wortlaut nur geringstmöglich angepasst. Die Regelungen dienen dem Ziel der Sicherheit der Datenverarbeitung; der Verantwortliche hat sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind gesetzlich dazu verpflichtet. „Verarbeiten“ ist gemäß Artikel 4 Abs. 2 Datenschutz-Grundverordnung nunmehr der Oberbegriff für alle denkbaren Formen des datenschutzrechtlich relevanten Umgangs mit Daten. Diese Regelungen sollen entsprechend auch für Hilfsunternehmen gelten. Für journalistische Zwecke wird im Bereich der Verarbeitung personenbezogener Daten die Anwendung der Datenschutz-Grundverordnung generell beschränkt auf deren Kapitel I, VIII, X und XI, die die Datenschutz-Grundverordnung abweichungsfest vorgibt, sowie auf Artikel 5 Abs. 1 Buchst. f, Artikel 24 und 32 Datenschutz-Grundverordnung, die die Festlegung der Aufgaben des für die Datenverarbeitung Verantwortlichen und die Sicherheit der Datenverarbeitung (einschließlich Geheimhaltung) betreffen.

Indem Artikel 5 Abs. 1 Buchst. f, Artikel 24, 32 Datenschutz-Grundverordnung für anwendbar erklärt werden, wird die Rechtslage unter Geltung des sog. Medienprivilegs abgebildet. Presse, Rundfunk und diesen gleichgestellte Medien waren auch bisher bei der Ausübung ihrer journalistischen Tätigkeit insoweit privilegiert, als sie vom geltenden Datenschutzrecht nur die Vorschriften zum Datengeheimnis und zur Datensicherheit beachten mussten und sich bei Verstößen schadensersatzpflichtig machten. Die Aufrechterhaltung dieser Situation wird auch unter Geltung der Grundverordnung für erforderlich gehalten, um das Recht auf freie Meinungsäußerung auch in seiner Ausgestaltungen als Pressefreiheit gewährleisten zu können.

Nicht weiter verfolgt wurden anfängliche Überlegungen, auch Beteiligungsunternehmen der Presse ausdrücklich mit einzubeziehen. Diese waren auch bisher nicht angeführt, ohne dass dies in der Praxis zu Problemen geführt hätte.

Anders als in den Absätzen 2 und 3 der neuen §§ 9c und 57 Rundfunkstaatsvertrag vorgesehen, wurde davon Abstand genommen, gleichartige, aber für den Bereich der Presse bisher nicht bestehende Betroffenenrechte bzw. Verpflichtungen der Presseunternehmen zu begrün-

den. Dies wäre eine Einschränkung der Pressefreiheit, die nicht erforderlich ist. Denn das Medienprivileg für die Presse in § 19 wird durch die sogenannte freiwillige Selbstkontrolle mit „Publizistischen Grundsätzen“ (Pressekodex) des Deutschen Presserates ergänzt. Danach hat jedermann die Möglichkeit, sich in einem einfachen und kostenfreien Verfahren gegen journalistische Inhalte von Printmedien beim Deutschen Presserat zu beschweren. Der Presserat hat verschiedene Sanktionsmöglichkeiten bis hin zu einer öffentlichen Rüge mit Abdruckverpflichtung. Hieraus ergibt sich ein über die gesetzlichen Ansprüche hinausgehender zusätzlicher, in der Praxis relevanter Schutz bei der Verarbeitung journalistischen Zwecken dienender Daten.

Die freiwillige Selbstkontrolle der Presse ist ein wesentliches Instrument zur Gewährleistung der Pressefreiheit, das sich bewährt hat. Sie ist neben den gesetzlichen Regelungen geeignet, den Schutz des Persönlichkeitsrechts des Einzelnen bzw. das Recht auf den Schutz personenbezogener Daten mit der Pressefreiheit in Einklang zu bringen und zugleich eine unabhängige und kritische Berichterstattung zu ermöglichen. Dass insgesamt kein ausreichender Schutz der Persönlichkeitsrechte gewährleistet wäre und in der Vergangenheit nicht hinnehmbare Schutzlücken entstanden sind, ist vor diesem Hintergrund nicht erkennbar.

Ähnliche Erwägungen gelten für den Ausschluss einer staatlichen Datenschutzaufsichtsbehörde (Artikel 51 Datenschutz-Grundverordnung). Für die freie Presse ist eine journalistische Tätigkeit ohne staatliche Einfluss- und Kontrollmöglichkeit von besonderer Bedeutung und angesichts der grundlegenden Aufgaben („Wächteramt“ der Presse) unverzichtbar und auch grundrechtlich geboten. Hiervon geht offenkundig auch Artikel 85 Absatz 2 Datenschutz-Grundverordnung aus, der auch für die staatliche Aufsicht im Medienbereich bei Kapitel VI (Aufsichtsbehörde) eine Einschränkung vorsieht. Eine staatliche Aufsicht ist vorliegend nicht erforderlich, denn der Pressekodex wurde 2001 um Regelungen zum Redaktionsdatenschutz erweitert, um die besondere datenschutzrechtliche Stellung von redaktioneller Arbeit in Einklang zu bringen mit dem Recht des Einzelnen auf informationelle Selbstbestimmung. Über die Einhaltung des Redaktionsdatenschutzes wacht der Deutsche Presserat anstelle von staatlichen Aufsichtsbehörden. Diese Sonderregelung sollen auch unter Geltung der Datenschutz-Grundverordnung beibehalten werden; Artikel 85 Datenschutz-Grundverordnung schließt dies nicht aus. Einer neuen Vorschrift, die ausdrücklich auf den Pressekodex verweist, bedarf es hierfür nicht. Darüber hinaus wäre eine staatliche Überwachung und Aufsicht hinsichtlich der internen Verarbeitung der journalistischen Zwecken dienenden personenbezogenen Daten zudem ein ganz erheblicher Eingriff in die Pressefreiheit. Ein derartiger Eingriff ist bei einer Gesamtabwägung nicht wegen überwiegender Gründe des Persönlichkeitsrechts des Betroffenen erforderlich und wäre deshalb unverhältnismäßig.

Durch den ausdrücklich ermöglichten Ausschluss des Kapitels VI (Unabhängige Aufsichtsbehörden) sind die Rechte aus Kapitel VIII schon tatbestandlich nicht anwendbar. Denn diese

setzen gerade eine solche Aufsichtsbehörde voraus. Dies gilt vor allem für das Recht auf Beschwerde bei einer Aufsichtsbehörde nach Artikel 77 Datenschutz-Grundverordnung, für das Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde nach Artikel 78 Datenschutz-Grundverordnung und auch für die Bußgeldregelung in Artikel 83 Datenschutz-Grundverordnung. Ohne eine solche Aufsichtsbehörde hat der Normadressat keine Stelle, an die er sich wenden kann. Der Verordnungsgeber hat also selbst die Möglichkeit geschaffen, dass das Kapitel VIII gerade zum Schutz der Presse in Teilen keine Anwendung findet.
Demgegenüber ist die Schadensersatzregelung in Artikel 82 Datenschutz-Grundverordnung grundsätzlich anwendbar. Sie kann im Geltungsbereich des Medienprivilegs aber nur dann greifen, wenn eine für die Medien geltende Verpflichtung verletzt worden ist. Dies wird – entsprechend der bisherigen Rechtslage – durch die Sätze 5 und 6 des Entwurfs klargestellt. Da das durch die Sätze 1 und 3 geschützte Datengeheimnis in der Datenschutz-Grundverordnung jedenfalls nicht ausdrücklich und vergleichbar geregelt ist, könnte zweifelhaft sein, ob bei dessen Verletzung die Schadensersatzregelung des Artikel 82 Datenschutz-Grundverordnung greift. Zur Klarstellung wird deshalb die Norm insoweit für entsprechend anwendbar erklärt.

**Zu Artikel 5 (Änderung des Niedersächsischen Ausführungsgesetzes zum Bundesmeldegesetz):**

Zu Nummer 1:
Die Änderung passt den Gesetzestext an die Bestimmung des Begriffs „Verarbeitung“ nach Art. 4 Nummer 2 der Verordnung (EU) 2016/679 an. Die Norm wird in sprachlicher Hinsicht präziser gefasst und es erfolgt eine Anpassung an die Neufassung des Niedersächsischen Kommunalabgabengesetzes.

Zu Nummer 2:
Die Änderung passt den Gesetzestext an die Bestimmung des Begriffs „Verarbeitung“ nach Art. 4 Nummer 2 der Verordnung (EU) 2016/679 an. Dieser definiert die „Verarbeitung“ als „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (…)“ und stellt mithin einen Oberbegriff dar, der auch die „Speicherung“ umfasst.

Zu Nummer 3:
§ 9 kommt in seiner derzeitigen Fassung lediglich eine klarstellende Funktion ohne Regelungsgehalt zu. Bei einer Beibehaltung der Norm müsste zusätzlich zum Verweis auf die (ohnehin

einzuhaltenden) Vorschriften des Bundesmeldegesetzes, des vorliegenden Gesetzes, der aufgrund dieses Gesetzes erlassenen Rechtsvorschriften und des Niedersächsischen Datenschutzgesetzes nunmehr auch ein Hinweis auf die Verordnung (EU) 2016/679 erfolgen. Eine solche Vorschrift widerspräche dem Gebot der Normenklarheit und verhielte sich konträr zu den Bestrebungen des Bürokratieabbaus.

**Zu Artikel 6 (Änderung des Niedersächsischen Rettungsdienstgesetzes):**

§ 11 ist die Datenschutz- und Dokumentationsregelung im NRettDG und enthält in den ersten drei Absätzen spezielle Regelungen über die im Bereich des Rettungsdienstes zu verarbeitenden Daten und die befugten Stellen. Aufgrund der Datenschutz-Grundverordnung ist ein Änderungsbedarf für die ersten drei Absätze nicht erforderlich.
Der Absatz 4 war insbesondere wegen der Ausnahmen in Bezug auf das bisherige Niedersächsische Datenschutzgesetz aufgenommen worden. Solche Ausnahmen gibt es nicht mehr, so dass Absatz 4 gestrichen werden konnte. Dass neben der Datenschutz-Grundverordnung auch das Niedersächsische Datenschutzgesetz anzuwenden ist, braucht nicht bestimmt zu werden. Das ergibt sich aus § 1 Abs. 1 NDSG.

**Zu Artikel 7 (Änderung des Niedersächsischen Brandschutzgesetzes):**

Zu Nummer 1:

Die Aufgabenwahrnehmung der Kommunen und des Landes mit den Feuerwehren, den Feuerwehr-Einsatz-Leitstellen, der Niedersächsischen Akademie für Brand- und Katastrophenschutz sowie den anderen zuständigen Behörden erfordert die Verarbeitung personenbezogener Daten.

Mit Regelungen zur Datenverarbeitung soll zum einen die maximal mögliche Nutzung der landesweit eingeführten Feuerwehrverwaltungssoftware erreicht werden, die nicht nur einen einheitlichen Standard für die Datennutzung bietet und den Aufgabenträgern Statistiken und Übersichten zur Verfügung stellt. Zum anderen erleichtern die Daten den Gemeinden, Landkreisen und dem Land die Abwicklung von Verwaltungsangelegenheiten, wie z. B. Übersicht über Personal und Ausstattung sowie Planung der Aus- und Fortbildung.

Deshalb wird ein neuer „Fünfter Teil – Datenverarbeitung –“ mit den §§ 35 a und 35 b eingeführt. Sie ergänzen die allgemeinen Regelungen des Niedersächsischen Datenschutzgesetzes (NDSG).

Zur Einfügung des § 35 a:

§ 35 a bestimmt die „Verarbeitung personenbezogener Daten aus einsatzbedingter Kommunikation“.

Absatz 1 stellt die Aufzeichnung von Notrufen in den Feuerwehr-Einsatz-Leitstellen (§ 3 Abs. 1 Nr. 4 und § 4) sowie einsatzbedingten Fernmeldeverkehr im Hinblick auf Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes (Recht am eigenen Wort), § 201 StGB und § 4 Abs. 1 NDSG auf eine eindeutige, bereichsspezifische Rechtsgrundlage.

Absatz 2 Satz 1 Nrn. 1 bis 6 legt fest, für welche Zwecke die zur Durchführung des Niedersächsischen Brandschutzgesetzes zuständigen Stellen personenbezogene Daten aus einsatzbedingter Kommunikation (Absatz 2 Satz 1 Nr. 1 bis 6) verarbeiten dürfen.

Die Aufzeichnungen von Anrufen sind, wie die Praxis immer wieder zeigt, insbesondere bei kritischen Einsätzen, für die Dokumentation der Alarmierung und des Einsatzablaufs (Nummer 1) sowie als Grundlage für die Abrechnung von Einsätzen (Nummer 2) notwendig. Gleichermaßen gilt dies zur Vorbereitung oder Durchführung gerichtlicher oder Verwaltungsverfahren (Nummer 3). Aufgezeichnete Daten dürfen zur Erprobung von Änderungen im Verfahren und der Technik sowie zur Beseitigung von Schwachstellen bei der Alarmierung und beim Einsatz im Interesse einer Optimierung der Aufgabenerfüllung durch die Leitstellen und die Gemeindefeuerwehren verarbeitet werden (Nummer 4). Ebenso ist eine Verarbeitung der aufgezeichneten Daten für statistische Zwecke (Nummer 5) zulässig. Auch für die Aus- und Fortbildung der Disponenten in den Leitstellen und der Feuerwehrangehörigen ist die Verarbeitung der Daten statthaft (Nummer 6). Dabei ist der Grundsatz der Erforderlichkeit zu beachten, andererseits ist die Verarbeitung gestattet, wenn betroffene Personen eingewilligt haben.

Die personenbezogenen Daten der Nummern 4 bis 6 sind für die Verarbeitung zu anonymisieren oder pseudonymisieren, es sei denn, dass die Zwecke damit nicht erreicht werden können. Eine Anonymisierung oder Pseudonymisierung ist beispielsweise ausnahmsweise nicht erforderlich, wenn der Zweck der Aus- und Fortbildung entgegensteht und die Interessen der Betroffenen Personen nicht offensichtlich überwiegen (§ 35 a Abs. 2 Satz 2).

Nach Absatz 3 Satz 1 dürfen Daten nach Abs. 2 Satz 1 an

- Polizeibehörden,
- Staatsanwaltschaften, Gerichte,
- Gemeinden, Landkreise, das Land,
- Träger des Rettungsdienstes (§ 3 Abs. 1 des Niedersächsischen Rettungsdienstgesetzes) und
- wirtschaftliche Unternehmen und öffentliche Einrichtungen mit Werkfeuerwehr (§ 16)

übermittelt werden. Dabei ist der Grundsatz der Erforderlichkeit zu beachten. Wenn diese Daten anonymisiert oder pseudonymisiert wurden, dürfen sie auch für wissenschaftliche Zwecke an Forschungseinrichtungen übermittelt werden (§ 35 a Abs. 3 Satz 2).

Zur Einfügung des § 35 b:

§ 35 b regelt die „Verarbeitung personenbezogener Daten von Mitgliedern der Feuerwehren sowie Lehrgangsteilnehmerinnen und Lehrgangsteilnehmern“.

Die zur Durchführung dieses Gesetzes zuständigen Behörden dürfen die für die Feuerwehrbedarfsplanung, Einsatzplanung, Brandschutzerziehung, Brandschutzaufklärung, Mitgliederverwaltung sowie die Lehrgangsplanung und -durchführung personenbezogene Daten der Feuerwehrangehörigen und Lehrgangsteilnehmerinnen und Lehrgangsteilnehmern verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Diese Daten sind für die Wahrnehmung und Umsetzung dieser gesetzlich bestimmten Aufgabenbereiche der zuständigen Behörden unverzichtbar.

Die Einschränkung „soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist “ soll sicherstellen, dass die zur Verfügung gestellten personenbezogenen Daten nur bestimmten Stellen zur Kenntnis gelangen.

Die unter Nrn. 1 bis 8 angeführten Daten (Name, Vornamen, Geburtsdatum und Anschrift, Beruf, akademische Grade, Telefonnummern und andere Angaben über die Erreichbarkeit, Beschäftigungsstelle) sind für die Feuerwehrbedarfsplanung erforderlich.

Nr. 9 (Angaben über die körperliche Tauglichkeit und die Strahlen- und Schadstoffbelastung) erfasst unter anderem den Nachweis über das Tragen von Atemschutzgeräten und Chemikalienschutzanzügen sowie eine etwaige Strahlenbelastung bei Einsätzen.

Die Erfassung des Datums des Eintritts in die Feuerwehr ist für die Berechnung von Dienstzeiten (Beförderungen, Ehrungen) erforderlich (Nr. 10).

Der Name der Feuerwehr wird für die eindeutige Zuordnung der Mitglieder zur Freiwilligen Feuerwehr der Gemeinde oder bei Gliederung in Ortsfeuerwehren zur jeweiligen Ortsfeuerwehr benötigt (Nr. 11).

Die Personalnummer und Dienstausweisnummer werden erfasst, da die Mitglieder einen Dienstausweis erhalten können (Nr. 12).

Die persönliche Ausrüstung, insbesondere die Einsatzschutzkleidung wird erfasst, da sie jedem Mitglied zum persönlichen Gebrauch zur Verfügung gestellt wird (Nr. 13).

Bei der Lehrgangsplanung sind die Lehrgangsvoraussetzungen zu prüfen. Bei Führungslehrgängen sind z. B. andere Lehrgänge vorher zwingend zu absolvieren. Es ist daher erforderlich

die Aus- und Fortbildungslehrgänge, einschließlich der Beurteilungsergebnisse, als Zugangsvoraussetzung zu kennen (Nr. 14).

Dienstgrad und Beförderungen sind für die Erstellung der entsprechenden Urkunden festzuhalten (Nr. 15).

Die Erfassung der Funktion in der Feuerwehr ist für die Gliederung der Feuerwehr in taktische Einheiten entsprechend der Feuerwehrdienstvorschrift 3 (FwDV 3) erforderlich (Nr. 16).

Die Erfassung besonderer Kenntnisse und Fähigkeiten ist für den richtigen Personaleinsatz neben der reinen feuerwehrtechnischen Ausbildung erforderlich (Nr. 17).

Auszeichnungen und Ehrungen sind für die Prüfung weiterer Anträge zu erfassen (Nr. 18).

Einsätze, Dienstzeiten und sonstige geleistete Stunden sind zu erfassen, um die Dienststunden der Mitglieder für Ansprüche nach den §§ 32 bis 35 NBrandSchG nachweisen zu können (Nr. 19).

Die Bankverbindungen sind für die Erstattung von Entschädigungen nach § 33, Schadensersatz nach § 34 sowie der Fahrtkosten- und Zahlung von Aufwandsentschädigungen bei Lehrgangsveranstaltungen erforderlich (Nr. 20).

Die Erfassung des Familienstandes ist für die Prüfung weiterer Anträge erforderlich (Nr. 21).

Die gefahrgeneigte Tätigkeit im Feuerwehreinsatz und im Übungsdienst erfordert es, dass jederzeit Angehörige und Erziehungsberechtigte benachrichtigt werden können (Nrn. 22 und 23).

Zu Nummer 2

Es handelt sich um eine redaktionelle Folgeänderung.

**Zu Artikel 8 (Änderung des Niedersächsischen Gesetzes über das amtliche Vermessungswesen):**

Die aktuelle Fassung des § 3 Abs. 2 Satz 3 lautet: „Zu den Liegenschaften sind Eigentumsangaben zu führen.“ Dieser Satz macht nicht ausreichend deutlich, dass im Liegenschaftskataster die Eigentumsangaben für im Grundbuch gebuchte Grundstücke in Übereinstimmung mit dem Grundbuch geführt werden. Die originäre Zuständigkeit für den Nachweis des Eigentums an Grundstücken liegt bei den Grundbuchämtern.

Nach § 55 Abs. 3 GBO sind Veränderungen der grundbuchmäßigen Bezeichnung des Grundstücks und die Eintragung eines Eigentümers außerdem der Behörde bekanntzumachen, welche das in § 2 Abs. 2 GBO bezeichnete amtliche Verzeichnis führt. Diese im Einklang mit dem Grundbuch eingetragenen Eigentumsangaben werden nach § 5 Abs. 2 NVermG bereitgestellt.

Artikel 16 DSGVO räumt den betroffenen Personen ein Recht auf Berichtigung ein. Danach können diese Personen von den Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten verlangen. Dieses Recht gilt unmittelbar und wird auch nicht von einer Öffnungsklausel umfasst. Somit könnten z.B. Eigentümer bei einer Namensänderung durch Eheschließung die Berichtigung des Liegenschaftskatasters verlangen, mit dem Resultat, dass dadurch im Grundbuch und im Liegenschaftskataster vermeintlich unterschiedliche Eigentümer nachgewiesen werden. Die Führung der Nachweise wird infolgedessen unnötig erschwert.

Durch die Gesetzesänderung wird nun deutlich, dass die Eigentumsangaben im Liegenschaftskataster gemäß § 55 Abs. 3 GBO zwingend in Übereinstimmung mit dem Grundbuch zu führen sind. Die Änderung trägt zur Transparenz bei. Die Rechte der Betroffenen nach Artikel 16 DSGVO werden gewahrt, sie sind jedoch bei dem zuständigen Grundbuchamt geltend zu machen. Die Angaben im Liegenschaftskataster werden nach Berichtigung des Grundbuchs über Datenaustausch aktualisiert, so dass wieder die Übereinstimmung mit dem Grundbuch erreicht wird.

**Zu Artikel 9 (Änderung des Niedersächsischen Statistikgesetzes):**

Die Novellierung dient dem Zweck, das Niedersächsische Statistikgesetz (NStatG) vom 27. Juni 1988 (Nds. GVBl. S.113), zuletzt geändert durch Artikel 8 des Gesetzes vom 16. Dezember 2004 (Nds. GVBl. S. 634) an die am 25. Mai 2016 in Kraft getretene und ab dem 25. Mai 2018 anzuwendende Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Datenverkehr zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung (DSGVO) anzupassen. Die Datenschutz-Grundverordnung enthält Öffnungsklauseln für den nationalen Gesetzgeber, die mit diesem Gesetz ausgefüllt werden, soweit Regelungsbedarfe nicht durch vorrangiges Bundes- oder die ergänzenden Bestimmungen des in Artikel 1 neu gefassten Niedersächsischen Datenschutzgesetzes gedeckt werden.

Zu Nummer 1:

Ein Großteil der amtlichen Statistiken beruht auf EU- und bundesrechtlichen Vorgaben. Die Durchführung dieser Statistiken liegt bei den Landesstatistikbehörden. Allgemeine Regelungen zur Ausführung dieser von EU und Bund angeordneten Statistiken trifft das Bundesstatistikgesetz (BStatG), Es ist deshalb erforderlich die Verweisung in § 1 Abs. 1 Nr. 1 hieran anzupassen. Das NStatG hat insoweit ergänzende Funktion.

Zu Nummer 2:
Der neu eingefügte Absatz korrespondiert mit § 16 Abs. 2 bis 4 des BStatG, zu dem das NStatG ergänzende Regelungen trifft. Er regelt die Übermittlung von Daten in der Zusammenarbeit in umgekehrter Richtung der Zusammenarbeit der Landesstatistikbehörde mit dem statistischen Bundesamt und darüber hinaus mit den statistischen Ämtern der anderen Länder.
Die Ergänzung des § 8 NStatG ist notwendig geworden. Der Landesgesetzgeber kann in landesgesetzlichen Regelungen statistische Erhebungen anordnen. In der Vergangenheit sind Fälle aufgetreten, in denen analog zu einer bundesgesetzlichen Regelung auch landesgesetzliche Regelungen erlassen wurden, wenn die gesetzliche Aufgabe auch in der Zuständigkeit der Länder lag. So hat der Bund z. B. für seinen Aufgabenbereich eine Statistik auf Bundesebene und die Länder jeweils eine spezifische Länderstatistik angeordnet. Im weiteren Verlauf hat sich u. a. aus Gründen der Evaluation des Gesetzesvorhaben, der weiteren Planung, der Auswertung der zu erreichenden Ziele, der Mittelverteilung, etc. die Notwendigkeit ergeben, dass diese Statistiken des Bundes und der Länder, die auf einer ähnlichen gesetzlichen Grundlage beruhen, miteinander koordiniert werden sollten.

Zu diesem Zweck hat sich in der Vergangenheit das Statistische Bundesamt angeboten, eine sog. „koordinierte Länderstatistik“ zu erstellen. Dafür ist es notwendig, dem ausführenden Statistischen Amt die jeweiligen Einzeldaten der Landesstatistik zu übermitteln. Eine Einwilligung der Befragten und Betroffenen liegt regelmäßig nicht vor und kann im Nachhinein auch nicht mehr eingeholt werden.

Während in allen anderen Landesstatistikgesetzen dafür neue Ermächtigungsgrundlagen geschaffen wurden, gab es für Niedersachsen bisher keine Möglichkeit, für eine koordinierte Länderstatistik die erforderlichen Einzeldaten zu liefern.

Ein Verweis auf § 3 BStatG wäre unzureichend, da diese Vorschrift die Aufgaben des Statistischen Bundesamtes beschreibt, aber keine Ermächtigungsgrundlage für die Übermittlung von Einzeldaten darstellt. Insbesondere ist hier nur die Zusammenstellung der Ergebnisse der Lan-

desstatistiken in der erforderlichen sachlichen und regionalen Gliederung und nicht die Übermittlung von Einzeldatensätzen geregelt. Doch häufig wird genau dieses detaillierte Material benötigt, um z.B. bei einer koordinierten Länderstatistik in einer bundesweiten Mehrfachfall-Prüfung Dubletten herauszufiltern.

Auch § 3 Abs. 4 BStatG bietet keine zutreffende Ermächtigungsgrundlage, da hier die Übermittlung von Einzeldaten nur für wissenschaftliche Zwecke erlaubt ist.

**Zu Artikel 10 (Änderung des Niedersächsischen Spielbankengesetzes):**

Zu Nummer 1 (§ 10 d):
Artikel 4 Nr. 7 2. Halbsatz der Datenschutz-Grundverordnung sieht vor, dass in den Fällen, in denen das nationale Recht natürlichen oder juristischen Personen, Behörden, Einrichtungen oder anderen Stellen die Verarbeitung von personenbezogenen Daten und damit deren Zwecke und Mittel vorgibt, der betreffend gesetzlich in die Pflicht Genommene zum „Verantwortlichen“ im Sinne der Datenschutz-Grundverordnung erklärt werden kann.
Aus Gründen des Spielerschutzes, der Spielsuchtbekämpfung, der Gefahrenabwehr u. a. ist der Zulassungsinhaber nach gesetzlichen Vorschriften, wie zum Beispiel nach dem Niedersächsischen Spielbankengesetz, der Niedersächsischen Spielordnung und dem Glückspielstaatsvertrag, verpflichtet, personenbezogene Daten zu verarbeiten.
Mit der Bestimmung des Zulassungsinhabers als Verantwortlichem im Sinne der Datenschutz-Grundverordnung wird dessen Bindung an die datenschutzrechtlichen Vorgaben sichergestellt und dem Sonderfall Rechnung getragen, dass nicht eine selbsterwählte Datenerhebung, sondern eine gesetzlich auferlegte gegeben ist.
Soweit wiederum die niedersächsische Spielbankenaufsicht die betreffenden Daten innerhalb ihrer aufsichtsrechtlichen Aufgabenwahrnehmung weiterverarbeitet, ist diese unmittelbar selber Verantwortliche im Sinne des Artikels 4 Nr. 7 der Datenschutz-Grundverordnung und unterliegt den Vorgaben des Niedersächsischen Datenschutzgesetzes.

Zu Nummer 2 (§ 10 e):
Rein redaktionelle Folgeänderung durch den neu eingefügten § 10 d.

Zu Nummer 3 (§ 11 Nr. 11):
Rein redaktionelle Folgeänderung durch den nach Einfügung des neuen § 10 d neu benannten § 10 e.

**Zu Artikel 11 (Änderung des Gesetzes über das Leichen-, Bestattungs- und Friedhofswesen):**

Zu Nummer 1 (§ 6):
Nach § 6 Abs. 4 Satz 2 des Gesetzes über das Leichen-, Bestattungs- und Friedhofswesen (BestattG) vom 8. Dezember 2005 (Nds. GVBl. S. 381) kann die untere Gesundheitsbehörde Hochschulen und anderen mit wissenschaftlicher Forschung befassten Stellen nach Maßgabe des § 25 des Niedersächsischen Datenschutzgesetzes (NDSG) auf Antrag Einsicht in Todesbescheinigungen gewähren, soweit dies für ein wissenschaftliches Vorhaben erforderlich ist. Die zitierte Vorschrift des § 25 NDSG betrifft die Verarbeitung personenbezogener Daten für Forschungsvorhaben. Diese Thematik ist nunmehr in der Datenschutzgrundverordnung und im Niedersächsischen Datenschutzgesetz an anderer Stelle geregelt. Sie ist hier entbehrlich und wird daher gestrichen.

Zu Nummer 2 (§ 18):
Folgeänderung der Änderung in Nummer 1 (§ 6).

**Zu Artikel 12 (Änderung des Niedersächsischen Gesetzes über Hilfen und Schutzmaßnahmen für psychisch Kranke):**

Zu Nummer 1:
Hierbei handelt es sich um eine redaktionelle Anpassung an die Neufassung des § 6 Abs. 1 NDSG in Verbindung mit der Geltung der Datenschutzgrundverordnung.

Zu Nummer 2:
Mit Abs. 1 Satz 1 macht der Gesetzgeber Gebrauch von der Ausnahmeregelung des Artikels 9 Abs. 2 Buchst. h) Datenschutz-Grundverordnung.

Zu Nummer 3:
§ 35 kann gestrichen werden, da eine entsprechende Regelung im Niedersächsischen Datenschutzgesetz bereits enthalten ist.

Zu Nummer 4:
Mit Satz 2 macht der Gesetzgeber von dem in Artikel 23 Abs. 1 Datenschutz-Grundverordnung verankerten Recht Gebrauch, die Pflichten und Rechte aus Artikel 15 Datenschutz-Grundverordnung zu beschränken. Je nach Krankheitsbild, Stadium der Erkrankung und der damit ver-

bundenen Handlungs- und Verständnisfähigkeit der betroffenen Person kann es aus therapeutischer und medizinischer Sicht notwendig sein, bestimmte Informationen zum Schutz der Person selber oder von Dritten zurückzuhalten. Ein Therapieerfolg kann durch eine vollständige Auskunft, z.B. über den zu erwartenden weiteren Krankheitsverlauf, gefährdet sein. Unter diesen Umständen kann es auch gerechtfertigt sein, Informationen zu Hinweisgebern zu der Erkrankung aus dem näheren Umfeld nicht zu geben. Diese Beschränkung ist nach Artikel 23 Abs. 1 Buchst. i) Datenschutz-Grundverordnung zulässig.

**Zu Artikel 13 (Änderung des Niedersächsischen Maßregelvollzugsgesetzes):**

Zu Nummer 1:
Hierbei handelt es sich um eine redaktionelle Anpassung an die Neufassung des § 6 Abs. 1 NDSG in Verbindung mit der Geltung der Datenschutzgrundverordnung.

Zu Nummer 2:
Mit der Regelung macht der Gesetzgeber Gebrauch von der Ausnahmeregelung des Artikels 9 Abs. 2 Buchst. h) Datenschutz-Grundverordnung.

Zu Nummer 3:
Es handelt sich um eine redaktionelle Anpassung an die Neufassung des § 8 NDSG.

**Zu Artikel 14 (Änderung des Niedersächsischen Schulgesetzes):**

Zu Nummer 1:
Mit der Regelung wird dem Informationsbedürfnis der am Übergang von der Schule in den Beruf beteiligten Agenturen für Arbeit im Rahmen der Durchführung von Maßnahmen am Übergang von der Schule in den Beruf, der Träger der Jugendhilfe in Bezug auf Angebote sozialpädagogischer Hilfen im Rahmen der Jugendhilfe und geeigneter sozialpädagogisch begleiteter Ausbildungs- und Beschäftigungsmaßnahmen sowie der Träger der Grundsicherung für Arbeitsuchende, den sog. Jobcentern, zum Zwecke der Wahrnehmung der Aufgaben nach § 1 Abs. 3 SGB II sowie § 4 Abs. 2 SGB II Rechnung getragen. Soweit die Kenntnis der personenbezogenen Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten für die vorgenannten Leistungsträger erforderlich ist, um die gesetzlichen Aufgaben rechtmäßig, vollständig und in angemessener Zeit erfüllen zu können, soll daher die Datenübermittlung zugelassen werden. In diesem Zusammenhang ist nicht zuletzt die auch von den Partnern des Bündnisses für Duale Berufsausbildung geforderte Intensivierung der Zusammenarbeit zwischen Agentur für Arbeit, Träger der Jugendhilfe, Jobcenter, Schule, Schulbehörden und

Schulträger bei der Unterstützung von Jugendlichen am Übergang zwischen Schule und Beruf im Rahmen einer koordinierten Beratungsstruktur hervorzuheben, die mit der gesetzlichen Regelung unterstützt wird.

Zu Nummer 2:
Es wird eine schulgesetzliche Grundlage für die Datenübermittlung zur Überwachung der Schulpflicht von Schülerinnen und Schülern geschaffen. Absatz 2 regelt dies für den Primarbereich. Satz 1 normiert die Datenübermittlung zwischen Meldebehörde und zuständiger Grundschule, damit letztere aufgrund aktueller Schülerdaten in die Lage versetzt wird, die Schulpflicht der in dem folgenden Jahr erstmals schulpflichtig werdenden oder während ihrer Schulpflicht im Primarbereich zuziehenden Kinder überwachen zu können (Satz 2). In Satz 3 wird vor dem Hintergrund des Grundsatzes der Datenminimierung der Katalog an zu übermittelnden Daten auf das für den Zweck der Überwachung der Schulpflicht erforderliche Maß beschränkt.
Die Regelung in Absatz 3 regelt die Datenübermittlung der abgebenden an die aufnehmende Schule im Falle eines Schulwechsels zur Überwachung der Schulpflicht. Mit den Vorgaben in den Sätzen 2 und 3 wird zur Überwachung der Schulpflicht die Übermittlung der Aufnahmeentscheidung durch die aufnehmende Schule an die abgebende Schule normiert und festgelegt, dass bis zur Übermittlung der Aufnahmeentscheidung der abgebenden Schule die Überwachung der Schulpflicht obliegt. Satz 4 soll sicherstellen, dass im Falle des Schulwechsels einer im Sekundarbereich schulpflichtigen Schülerin oder eines Schülers aus einem anderen Bundesland oder aus dem Ausland die Schulbehörde die für die Überwachung der Schulpflicht erforderlichen Daten erhält. Die abgebende Schule kann in diesen Fällen mangels Gesetzgebungskompetenz nicht zur Datenübermittlung an die aufnehmende Schulen verpflichtet werden. Aufgrund der fehlenden rechtlichen Verpflichtung in § 63 Abs. 2 Satz 1, 2. Halbsatz NSchG zur Festlegung von Schulbezirken im Sekundarbereich I sowie aufgrund des Fehlens einer gesetzlichen Ermächtigung zur Festlegung von Schulbezirken im Sekundarbereich II steht anders als im Primarbereich nicht von vornherein fest, welche Schule die Schülerin oder der Schüler besucht. Aus diesem Grunde wird eine Datenübermittlung an die Schulbehörde vorgesehen, damit diese in die Lage versetzt wird, die Erziehungsberechtigten zu kontaktieren, um den Schulbesuch des schulpflichtigen Kindes zu überprüfen.

Zu Nummer 3:
Folgeänderung.

Zu Nummer 4:
Die Rechte der betroffenen Personen ergeben sich künftig im Falle der Verarbeitung personenbezogener Daten direkt aus der Datenschutz-Grundverordnung. Dies gilt insbesondere auch für das Widerspruchsrecht, das in Artikel 21 DSGVO statuiert ist und unmittelbar gilt. Die bisherige Regelung in Absatz 3 ist damit obsolet. Dass hinsichtlich der Geltendmachung datenschutzrechtlicher Ansprüche die Erziehungsberechtigten für ihre minderjährigen Kinder handeln, bedarf keiner ausdrücklichen Regelung.

Zu Nummer 5:
Folgeänderung.

**Zu Artikel 15 (Änderung des Niedersächsischen Bodenschutzgesetzes):**

Zu Nummer 1:
§ 13 Satz 2 NBodSchG stellt bisher in Abweichung vom allgemeinen Datenschutzrecht die Rechtmäßigkeit der Datenübermittlung sicher, um zu verhindern, dass die Bodenschutzbehörden bei der Erstellung der Altlastenverzeichnisse die bereits bei anderen Behörden (z. B. den Baubehörden) vorhandenen Informationen über schädliche Bodenveränderungen und Altlasten noch einmal auf eigene Kosten erheben müssen. Eine die Zweckbindung überwindende Regelung ist hierfür nicht erforderlich, da die hierfür in § 6 Abs. 2 NDSG vorgesehenen allgemeinen Regelungen in der Regel nicht ausreichend sein werden.
Im Rahmen der bevorstehenden Novellierung des Niedersächsischen Datenschutzgesetzes (NDSG) und des In-Kraft-Tretens der Datenschutz-Grundverordnung muss § 13 Satz 2 NBodSchG entsprechend angepasst werden.

Zu Nummer 2:
Die Regelung in Satz 4 über die Anwendung des Niedersächsischen Datenschutzgesetzes diente ausschließlich der Rechtsklarheit und kann entfallen.

**Zu Artikel 16 (Inkrafttreten):**

Nach Artikel 99 Abs. 2 DSGVO ist die Verordnung ab dem 25. Mai 2018 unmittelbar geltendes Recht in allen Mitgliedstaaten. Deshalb treten mit Satz 1 das neue, die Datenschutz-Grundverordnung ergänzende niedersächsische Datenschutzgesetz sowie die Änderungen in den Fachgesetzen zu diesem Zeitpunkt in Kraft. Gleichzeitig tritt nach Satz 2 das geltende Niedersächsische Datenschutzgesetz außer Kraft.