Entwurf

G e s e t z

zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes

Artikel 1

Niedersächsisches Gesetz über digitale Verwaltung
und Informationssicherheit (NDIG)

I n h a l t s ü b e r s i c h t

Erster Teil

Allgemeines

§ 1

Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes bedeutet:

1. Angriff:

   ein Versuch, die IT-Sicherheit eines Computersystems unbefugt zu beeinflussen,

2. Basisdienst:

   ein fachunabhängiges informationstechnisches Verfahren zur Unterstützung von Verwaltungsaufgaben,

3. Behörde:

   jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt,

4. besondere Kategorien personenbezogener Daten:

   personenbezogene Daten, aus denen die rassische oder 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,

5. elektronische Rechnung:

   eine Rechnung, die in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird, das ihre automatische und elektronische Verarbeitung ermöglicht,

6. Informationstechnik:

   technische Mittel zur elektronischen Verarbeitung oder Übertragung von Informationen,

7. Inhaltsdaten:

   Informationen, die bei einem Telekommunikationsvorgang übertragen werden und um derentwillen die Telekommunikation stattfindet und die keine Verkehrsdaten nach § 3 Nr. 30 des Telekommunikationsgesetzes sind,

8. IT-Sicherheit:

   die Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten,

9. Landesdatennetz:

   eine Kommunikationsinfrastruktur, die eine Verbindung zwischen den lokalen Netzen der damit verbundenen Behörden sowie zu Netzen anderer Verwaltungen ermöglicht und durch das Land oder im Auftrag des Landes betrieben wird,

10. Nutzerkonto:

    eine zentrale Identifizierungskomponente zur einmaligen oder dauerhaften Identifizierung einer natürlichen oder juristischen Person oder einer Personengesellschaft zu Zwecken der Inanspruchnahme von Behördenleistungen,

11. Schadprogramm:

    ein Computerprogramm, das bei Ausführung unbefugt die Vertraulichkeit, Verfügbarkeit oder Integrität der verarbeiteten Daten gefährden kann, oder ein Teil davon,

12. Sicherheitsdomäne:

    ein abgegrenzter Teil der Verwaltung mit einheitlichen Sicherheitsanforderungen oder einheitlicher Sicherheitsadministration,

13. Sicherheitsarchitektur:

    die Gesamtheit der technischen und organisatorischen Maßnahmen für das Landesdatennetz, die zur Abwehr von Gefahren auf dieses dienen,

14. Sicherheitslücken:

die Eigenschaften von Computerprogrammen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Unbefugte gegen den Willen der Berechtigten Zugang zu diesen informationstechnischen Systemen verschaffen oder die Funktion dieser informationstechnischen Systeme beeinflussen können,

15. Sicherheitsvorfall:

ein Ereignis, das die Vertraulichkeit, Verfügbarkeit oder Integrität der verarbeiteten Daten einschränkt oder beseitigt oder einschränken oder beseitigen könnte.

(2) Ein informationstechnisches System ist mit dem Landesdatennetz verbunden, wenn es direkt, über ein untergeordnetes behördeneigenes Netz oder über einen IT-Dienstleister an das Landesdatennetz angeschlossen ist.

§ 2

Die oder der IT-Bevollmächtigte der Landesregierung

[1]Die Landesregierung bestellt eine IT-Bevollmächtigte oder einen IT-Bevollmächtigten. [2]Sie oder er hat den Einsatz der Informationstechnik durch das Land und die Fortentwicklung der digitalen Verwaltung, die ihre geschäftlichen Prozesse durchgehend mithilfe der Informationstechnik durchführt, unter Berücksichtigung der fachlichen und organisatorischen Belange zu koordinieren.

Zweiter Teil

Digitale Verwaltung

§ 3

Geltungsbereich

(1) Dieser Teil gilt für die öffentlich-rechtliche Verwaltungstätigkeit des Landes, der Kommunen sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, soweit nicht besondere Rechtsvorschriften des Landes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten.

(2) Dieser Teil gilt nicht für

1. die Hochschulen in staatlicher Verantwortung und Teile von Behörden des Landes, die mit Forschungsaufgaben betraut und deren informationstechnischen Systeme nicht mit dem Landesdatennetz verbunden sind,
2. die Kirchen, Religionsgesellschaften und Weltanschauungsgemeinschaften sowie ihre Verbände und Einrichtungen,
3. die öffentlich-rechtlichen Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten,
4. die landesunmittelbaren Körperschaften der gesetzlichen Kranken-, Renten- und Unfallversicherung sowie der sozialen Pflegeversicherung,
5. Beliehene,
6. den Norddeutschen Rundfunk und die Niedersächsische Landesmedienanstalt,
7. die Nordwestdeutsche Forstliche Versuchsanstalt,
8. die Schulen im Sinne des Niedersächsischen Schulgesetzes und die Schulen im Sinne des Niedersächsischen Gesetzes über Schulen für Gesundheitsfachberufe und Einrichtungen für die praktische Ausbildung,
9. die den Landesbildungszentren angeschlossenen pädagogischen Bereiche, wenn deren informationstechnische Systeme nicht mit dem Landesdatennetz verbunden sind,
10. die Strafverfolgung, die Verfolgung und Ahndung von Ordnungswidrigkeiten, die Rechtshilfe für das Ausland in Straf-und Zivilsachen und für Maßnahmen des Richterdienstrechts sowie
11. alle Einrichtungen im Sinne des § 1 Abs. 2 des Gesetzes über Tageseinrichtungen für Kinder.

(3) Für

1. das Justizministerium und seinen Geschäftsbereich, soweit diese nicht bereits von den Absätzen 1 und 2 erfasst sind,
2. die Verwaltungstätigkeit nach dem Zweiten Buch des Sozialgesetzbuchs,
3. die Landtagsverwaltung,

4. die Tätigkeit der Finanzbehörden nach der Abgabenordnung und dem Finanzverwaltungsgesetz,

5. den Landesrechnungshof,

6. die Vergabekammer Niedersachsen,

7. die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde,

8. die Wasser- und Bodenverbände,

9. die Realverbände sowie die Forst- und die Jagdgenossenschaften und

10. die Zweckverbände im Sinne des Niedersächsischen Gesetzes über die kommunale Zusammenarbeit sowie den Regionalverband „Großraum Braunschweig“

gilt nur § 10 Abs. 4.

(4) Unabhängig von den Absätzen 1 bis 3 gilt § 6 Abs. 3 und 4 für

1. die niedersächsische Auftraggeber im Sinne des § 98 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) in Bezug auf Aufträge, die in den Anwendungsbereich des Teils 4 des Gesetzes gegen Wettbewerbsbeschränkungen fallen, und

2. die öffentlichen Auftraggeber im Sinne des § 2 Abs. 5 des Niedersächsischen Tariftreue- und Vergabegesetzes in Bezug auf Aufträge, deren geschätzter Auftragswert den jeweils maßgeblichen Schwellenwert gemäß § 106 GWB nicht erreicht.

§ 4

Elektronischer Zugang zur Verwaltung

(1) [1]Die Behörden sind, auch wenn sie nicht Bundesrecht ausführen, verpflichtet, auch einen Zugang für die Übermittlung elektronischer Dokumente zu eröffnen. [2]Dies gilt unabhängig davon, ob die Dokumente mit einer qualifizierten elektronischen Signatur versehen sind.

(2) [1]Die Behörden sind verpflichtet, einen Zugang nach Absatz 1 auch über Nutzerkonten anzubieten. [2]Diese müssen die Bereitstellung und Entgegennahme von Daten zum Zweck der Inanspruchnahme von Behördenleistungen ermöglichen. [3]Sie sind durch technische und organisatorische Maßnahmen gegen den unberechtigten Zugriff Dritter zu schützen [4]Die Behörden sollen die Nutzerkonten bei der Kommunikation in Verwaltungsverfahren nutzen.

(3) Die Behörden sind verpflichtet, einen Zugang nach Absatz 1 auch durch eine De-Mail-Adresse im Sinne des De-Mail-Gesetzes oder einen anderen schriftformersetzenden Dienst anzubieten.

(4) Die Behörden des Landes sind verpflichtet, in elektronisch durchgeführten Verwaltungsverfahren, in denen sie die Identität einer Person aufgrund einer Rechtsvorschrift festzustellen haben oder aus anderen Gründen eine Identifizierung für notwendig erachtet wird, einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes (PAuswG) oder nach § 78 Abs. 5 des Aufenthaltsgesetzes (AufenthG) anzubieten.

§ 5

Elektronische Informationen und Verwaltungsportal

(1) Die Behörden stellen, auch wenn sie nicht Bundesrecht ausführen, über öffentlich zugängliche Netze in allgemein verständlicher Sprache Informationen über ihre Aufgaben, ihre Anschrift, ihre Geschäftszeiten sowie ihre postalische, telefonische und elektronische Erreichbarkeit zur Verfügung.

(2) Die Behörden haben, auch wenn sie nicht Bundesrecht ausführen, über öffentlich zugängliche Netze in allgemein verständlicher Sprache über ihre nach außen wirkende öffentlich-rechtliche Tätigkeit, damit verbundene Gebühren, beizubringende Unterlagen, die zuständige Ansprechstelle und ihre Erreichbarkeit zu informieren sowie erforderliche Formulare bereitzustellen.

(3) Die Informationen nach den Absätzen 1 und 2 sowie nach § 3 Abs. 1 und 2 des E-Government-Gesetzes (EGovG) sind aktuell zu halten.

(4) [1]Die obersten Landesbehörden stellen sicher, dass die Informationen nach Absatz 2 und § 3 Abs. 2 EGovG für die Kommunen elektronisch bereitstehen, soweit diese für die Ausführung von Bundes- oder Landesrecht zuständig sind. [2]Die Kommunen können diese Informationen für Zwecke nach Absatz 2 und § 3 Abs. 2 EGovG verwenden und dabei Ergänzungen vornehmen.

(5) [1]Zur Ausführung des § 1 des Onlinezugangsgesetzes stellt das für zentrale IT-Steuerung zuständige Ministerium ein niedersächsisches Verwaltungsportal bereit und verknüpft es mit dem Portalverbund von Bund und Ländern. [2]Die Behörden bieten ihre Verwaltungsleistungen auch über das niedersächsische Verwaltungsportal an.

§ 6

Elektronische Bezahlmöglichkeiten und Rechnungen

(1) Fallen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens Verwaltungskosten oder sonstige Forderungen an, so muss die Behörde die Einzahlung dieser Verwaltungskosten oder die Begleichung dieser sonstigen Forderungen durch Teilnahme an mindestens einem im elektronischen Geschäftsverkehr üblichen und hinreichend sicheren Zahlungsverfahren ermöglichen, auch wenn nicht Bundesrecht ausgeführt wird.

(2) Die Behörden sollen es ermöglichen, dass Zahlungen nach Absatz 1 so geleistet werden können, dass die Gutschrift sofort bei der empfangenden Behörde erkennbar ist, wenn die Höhe der Verwaltungskosten feststeht und die Verwaltungsleistung erst nach der Zahlung erbracht wird.

(3) Die Auftraggeber nach § 3 Abs. 4 stellen sicher, dass elektronische Rechnungen aufgrund von Aufträgen nach § 3 Abs. 4 nach Maßgabe der Verordnung nach Absatz 4 empfangen und verarbeitet werden können.

(4) [1]Die Landesregierung wird ermächtigt, durch Verordnung Vorschriften zur Ausgestaltung des elektronischen Rechnungsverkehrs zu erlassen. [2]Diese Vorschriften können sich beziehen auf

1. die Art und Weise der Verarbeitung elektronischer Rechnungen,
2. die Anforderungen an elektronische Rechnungen hinsichtlich der von diesen zu erfüllenden Voraussetzungen, den Schutz personenbezogener Daten, das zu verwendende Rechnungsdatenmodell und die Verbindlichkeit der elektronischen Form sowie
3. Ausnahmen für sicherheitsspezifische Aufträge.

§ 7

Nachweise

(1) [1]Wird ein Verwaltungsverfahren elektronisch durchgeführt, so können die vorzulegenden Nachweise, auch wenn nicht Bundesrecht ausgeführt wird, elektronisch eingereicht werden, es sei denn, dass durch Rechtsvorschrift etwas anderes bestimmt ist oder die Behörde für bestimmte Verfahren oder im Einzelfall die Vorlage eines Papieroriginals verlangt. [2]Die Behörde entscheidet nach pflichtgemäßem Ermessen, welche Art der elektronischen Einreichung zur Ermittlung des Sachverhalts zulässig ist.

(2) [1]Die zuständige Behörde kann erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit der Einwilligung der Verfahrensbeteiligten direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen, auch wenn nicht Bundesrecht ausgeführt wird. [2]Zu diesem Zweck dürfen die anfordernde Behörde und die abgebende öffentliche Stelle die erforderlichen personenbezogenen Daten verarbeiten, auch wenn nicht Bundesrecht ausgeführt wird.

§ 8

Elektronische Formulare

[1]Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars, das ein Unterschriftsfeld vorsieht, vorgeschrieben, so wird allein dadurch nicht die Anordnung der Schriftform bewirkt, auch wenn nicht Bundesrecht ausgeführt wird. [2]Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld, auch wenn nicht Bundesrecht ausgeführt wird.

§ 9

Georeferenzierung

(1) Wird ein elektronisches Register, das Angaben mit Bezug zu Grundstücken in Niedersachsen enthält, neu aufgebaut oder überarbeitet, so hat die Behörde in das Register eine bundesweit einheitlich festgelegte direkte Georeferenzierung (Koordinate) auf der Grundlage der Angaben des amtlichen Vermessungswesens (Geobasisdaten) zu dem jeweiligen Flurstück, dem Gebäude oder zu einem in einer Rechtsvorschrift definierten Gebiet aufzunehmen, auf das sich die Angaben beziehen.

(2) Register im Sinne dieses Gesetzes ist ein Verzeichnis, für das Daten aufgrund von Rechtsvorschriften des Landes erhoben oder gespeichert werden.

§ 10

Elektronische Aktenführung

(1) Die Behörden können ihre Akten elektronisch führen.

(2) [1]Die Behörden des Landes sollen neu anzulegende Akten ab dem 1. Januar 2026 elektronisch führen. [2]Jede oberste Landesbehörde stellt ab dem 1. Januar 2023 sicher, dass auf Arbeitsplätzen ihres Geschäftsbereichs, auf denen Verwaltungsleistungen über das Niedersächsische Verwaltungsportal erbracht werden, neu anzulegende Akten elektronisch geführt werden. [3]Bei Vorliegen besonderer Gründe können im Einvernehmen mit

der oder dem IT-Bevollmächtigten der Landesregierung jeweils spätere Termine nach den Sätzen 1 und 2 festgelegt werden. [4]Die oder der IT-Bevollmächtigte der Landesregierung kann das Einvernehmen verweigern, wenn die Terminverschiebung nicht ausreichend begründet ist und durch die Festlegung späterer Termine die flächendeckende Einführung der elektronischen Aktenführung erheblich beeinträchtigt würde.

(3) [1]Wird eine Akte elektronisch geführt, so sind die Einhaltung der Grundsätze der ordnungsgemäßen Aktenführung sowie die Lesbarkeit, die Integrität und Authentizität, die Verfügbarkeit und die Vertraulichkeit der Akte sicherzustellen. [2]Akten oder Aktenteile können weiterhin in Papierform geführt werden, wenn die Anforderungen nach Satz 1 nicht oder nur mit einem unverhältnismäßigen Aufwand erfüllt werden können.

(4) [1]Der Austausch elektronisch geführter Akten innerhalb einer Behörde und zwischen Behörden soll auf elektronischem Wege erfolgen. [2]Die Landesregierung wird ermächtigt, technische Verfahren und Standards für den Austausch zwischen Behörden nach Satz 1 durch Verordnung zu regeln.

(5) Einsichtnahme in eine elektronisch geführte Akte wird gewährt, indem

1. ein Aktenausdruck zur Verfügung gestellt wird,
2. die elektronischen Dokumente auf einem Bildschirm wiedergegeben werden,
3. die elektronischen Dokumente übermittelt werden oder
4. der lesende Zugriff auf den Inhalt der Akte ermöglicht wird.

§ 11

Übertragen und Vernichten von Dokumenten in Papierform

(1) [1]Soweit die Behörden des Landes Akten elektronisch führen, übertragen sie die Dokumente, die in Papierform oder in anderer körperlicher Form vorliegen, erforderlichenfalls in elektronische Dokumente und speichern diese in einer elektronischen Akte. [2]Bei der Übertragung in elektronische Dokumente ist nach dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Dokumenten in Papierform oder in anderer körperlicher Form bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. [3]Von der Übertragung der Dokumente in Papierform oder anderer körperlicher Form in elektronische Dokumente kann abgesehen werden, wenn die Übertragung unverhältnismäßigen Aufwand erfordert.

(2) [1]Sind in Papierform oder in anderer körperlicher Form vorliegende Dokumente nach Absatz 1 übertragen und zur elektronischen Akte genommen worden, so sollen sie vernichtet oder zurückgegeben werden, wenn eine Aufbewahrung aus rechtlichen Gründen nicht erforderlich ist. [2]Für Maßnahmen der Qualitätssicherung kann die Vernichtung von Dokumenten aufgeschoben werden.

(3) Kommunen sowie sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts können in Papierform oder in anderer körperlicher Form vorliegende Dokumente, wenn sie übertragen und zu einer elektronischen Akte nach § 10 Abs. 1 genommen worden sind, vernichten oder zurückgeben, wenn eine Aufbewahrung aus rechtlichen Gründen nicht erforderlich ist. [2]Absatz 2 Satz 2 gilt entsprechend.

§ 12

Basisdienste

(1) [1]Das für die zentrale IT-Steuerung zuständige Ministerium stellt den Behörden Basisdienste

1. für die Zugänge nach § 4 Abs. 1 bis 3,
2. für den elektronischen Identitätsnachweis nach § 18 PAuswG oder nach § 78 Abs. 5 AufenthG,
3. für die Zurverfügungstellung von Informationen und Bereitstellung von Formularen nach § 5 Abs. 1 und 2 dieses Gesetzes sowie § 3 Abs. 1 und 2 EGovG,
4. für das Anbieten von Verwaltungsleistungen über das niedersächsische Verwaltungsportal nach § 5 Abs. 5 Satz 2,
5. für eine Bezahlmöglichkeit nach § 6 Abs. 1 und 2,
6. für den Empfang und die Verarbeitung elektronischer Rechnungen nach § 6 Abs. 3 und
7. für die elektronische Aktenführung nach § 10 unter Berücksichtigung der Vorgangsbearbeitung

bereit. [2]Das für Geoinformation zuständige Ministerium stellt den Behörden einen Basisdienst für die Georeferenzierung bereit. [3]Basisdienste für die in den Sätzen 1 und 2 genannten Funktionen und für andere Funktionen können die Behörden des Landes nur im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung bereitstellen. [4]Das Einvernehmen kann nur verweigert werden, wenn die Zweckmäßigkeit oder Wirtschaftlichkeit nicht erkennbar ist. [5]Die Behörden des Landes können sich bei der Bereitstellung von Basisdiensten Dritter bedienen.

(2) [1]Die Behörden des Landes haben ihre Verpflichtungen nach den §§ 4, 5 Abs. 1 und 2, den §§ 6, 9 und 10 Abs. 2 dieses Gesetzes sowie nach § 2 Abs. 1, § 3 Abs. 1 und 2 und den §§ 4 und 4 a EGovG mit den nach Absatz 1 Sätze 1 und 2 bereitgestellten Basisdiensten zu erfüllen. [2]Im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung können diese Verpflichtungen abweichend von Satz 1 mit einem nach Absatz 1 Satz 3 bereitgestellten Basisdienst oder über ein fachbezogenes informationstechnisches Verfahren erfüllt werden. [3]Das Einvernehmen kann nur verweigert werden, wenn die Zweckmäßigkeit oder Wirtschaftlichkeit des Einsatzes in der Behörde nicht erkennbar ist.

(3) [1]Die Kommunen sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts haben ihre Verpflichtungen nach § 4 Abs. 2 mit dem nach Absatz 1 Satz 1 Nr. 1 bereitgestellten Basisdienst, ihre Verpflichtungen zur Zurverfügungstellung der Informationen nach § 5 Abs. 1 und 2 mit dem nach Absatz 1 Satz 1 Nr. 3 bereitgestellten Basisdienst und ihre Verpflichtungen nach § 9 mit dem nach Absatz 1 Satz 2 bereitgestellten Basisdienst zu erfüllen. [2]Die Basisdienste für

1. die Bereitstellung eines Zugangs über Nutzerkonten, die die Anforderungen nach § 4 Abs. 2 Sätze 2 und 3 erfüllen,
2. die Zurverfügungstellung der Informationen nach § 5 Abs. 1 und 2 dieses Gesetzes und nach § 3 Abs. 1 und 2 EGovG,
3. die Bereitstellung von erforderlichen Formularen nach § 5 Abs. 2 dieses Gesetzes und nach § 3 Abs. 2 EGovG sowie
4. das Anbieten von Verwaltungsleistungen über das niedersächsische Verwaltungsportal nach § 5 Abs. 4 Satz 2

werden den Kommunen und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts kostenfrei zur Nutzung bereitgestellt.

(4) Die Landesregierung wird ermächtigt, durch Verordnung

1. für die vom Land bereitgestellten Basisdienste weitere Nutzungsverpflichtungen und Verpflichtungen zur Bereitstellung zur Nutzung festzulegen und
2. die Ausgestaltung der Basisdienste zu regeln, insbesondere hinsichtlich
   a) der Interoperabilitäts- und Informationssicherheitsstandards,
   b) der Anforderungen, die der Qualitätssicherung dienen,
   c) des Funktionsumfangs und des Inhalts der vom Land bereitgestellten Basisdienste, insbesondere der durch den jeweiligen Dienst zu verarbeitenden personenbezogenen Daten, sowie
   d) der Nutzung der vom Land bereitgestellten Basisdienste.

Dritter Teil

Informationssicherheit

Erster Abschnitt

Gewährleistung der Informationssicherheit

§ 13

Förderung der Sicherheit in der Informationstechnik

(1) [1]Die das Landesdatennetz betreibende Behörde fördert die Sicherheit der Informationstechnik im Landesdatennetz mit Ausnahme des Netzes des Geschäftsbereichs des Justizministeriums. [2]Im Netz des Geschäftsbereichs des Justizministeriums fördert eine vom Justizministerium bestimmte Stelle die Sicherheit der Informationstechnik.

(2) Zu dem Zweck nach Absatz 1 haben die das Landesdatennetz betreibende Behörde und die vom Justizministerium bestimmte Stelle jeweils für ihren Bereich die Aufgabe,

1. Gefahren für die IT-Sicherheit, die durch Sicherheitslücken, Schadprogramme oder Angriffe bestehen, abzuwehren,
2. Informationen über Gefahren für die IT-Sicherheit und über Sicherheitsvorkehrungen zu sammeln, diese auszuwerten, die Sicherheitsrisiken zu analysieren und die gewonnenen Erkenntnisse den Stellen, deren informationstechnischen Systeme mit dem Landesdatennetz verbunden sind, zur Verfügung zu stellen,
3. Sicherheitsvorkehrungen für das Landesdatennetz zu planen,
4. die Zentralstelle für IT-Sicherheit (§ 16 Abs. 1) nach deren Vorgaben zu unterstützen.

(3) Zusätzlich hat die das Landesdatennetz betreibende Behörde, auch für das Netz des Geschäftsbereichs des Justizministeriums, die Aufgabe,

1. sicherheitstechnische Anforderungen an die von den Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden sind, einzusetzende Informationstechnik und an die Verbindung von Netzen und informationstechnischen Systemen mit dem Landesdatennetz zu entwickeln und fortzuschreiben,
2. IT-Sicherheitsprodukte den Stellen, deren informationstechnischen Systeme mit dem Landesdatennetz verbunden sind, bereitzustellen,
3. die für Sicherheit der Informationstechnik Verantwortlichen der Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden sind, in Abstimmung mit der Zentralstelle (§ 16 Abs. 1) zu unterstützen sowie
4. bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme von Stellen, deren informationstechnischen Systeme mit dem Landesdatennetz verbunden sind, in herausgehobenen Fällen zu unterstützen.

(4) Zur Wahrnehmung der Aufgaben nach den Absätzen 2 und 3 betreiben die das Landesdatennetz betreibende Behörde und die vom Justizministerium bestimmte Stelle dem jeweiligen Stand der Technik entsprechende informationstechnische Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme und Angriffe.

§ 14

Vorübergehende und unaufschiebbare Maßnahmen
zur Gewährleistung der IT-Sicherheit

Die oder der IT-Bevollmächtigte der Landesregierung kann gegenüber Behörden und Gerichten des Landes bei einer gegenwärtigen Gefahr für die IT-Sicherheit, die zu einer Gefahr für die IT-Sicherheit bei anderen Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden sind, führen kann, vorübergehende und unaufschiebbare Maßnahmen anordnen, die zur Gewährleistung der IT-Sicherheit erforderlich sind.

§ 15

Sicherheitsverbund, Verpflichtung zu Sicherheitsmaßnahmen

(1) [1]Die Behörden und Gerichte des Landes betreiben ihre informationstechnischen Systeme in einem Sicherheitsverbund. [2]Die Mitglieder des Sicherheitsverbunds haben eine dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene IT-Sicherheit ihrer informationstechnischen Systeme, auch in Hinblick auf andere Mitglieder des Sicherheitsverbunds, zu gewährleisten.

(2) [1]Die Informationssicherheit im Sicherheitsverbund ist von den Behörden und Gerichten des Landes auf der Basis von Risikoanalysen sicherzustellen. [2]Die zur Risikobehandlung erforderlichen technischen und organisatorischen Maßnahmen sind unverzüglich zu veranlassen und regelmäßig zu überprüfen und anzupassen.

(3) Die das Landesdatennetz betreibende Behörde oder eine von ihr beauftragte Stelle hat Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden, aber nicht Mitglied des Sicherheitsverbundes sind, zur Einhaltung von bestimmten Sicherheitsmaßnahmen zu verpflichten, die dem Stand der Informationssicherheit im Sicherheitsverbund entsprechen.

§ 16

Zentralstelle für Informationssicherheit

(1) Bei dem für die zentrale IT-Steuerung zuständigen Ministerium ist eine Zentralstelle eingerichtet, die fortlaufend ein Informationssicherheitslagebild über Bedrohungen und Angriffe erstellt und dieses mit dem Ziel analysiert, Veränderungen der Gefahrenlage zu erkennen, daraus, auch unter Berücksichtigung einer Gesamtschau der Risikoanalysen, Hinweise zur Anpassung der Sicherheitsarchitektur entwickelt sowie Behörden und Gerichte des Landes über Fragen der Sicherheit in der Informationstechnik berät und bei informationstechnischen Sicherheitsvorfällen unterstützt.

(2) Die Behörden und Gerichte des Landes sind verpflichtet, der Zentralstelle informationstechnische Sicherheitsvorfälle in einer von ihr vorgegebenen Form unverzüglich mitzuteilen, wenn diese geeignet sind, auch die Informationssicherheit anderer Sicherheitsdomänen zu beeinträchtigen.

Zweiter Abschnitt

Einsatz von Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit

§ 17

Geltungsbereich, Wahrnehmung der Befugnisse nach diesem Abschnitt

(1) [1]Dieser Abschnitt gilt für die Behörden, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind. [2]Dieser Abschnitt gilt entsprechend für Stellen aus dem Geschäftsbereich des Justizministeriums, die keine Aufgaben der öffentlichen Verwaltung wahrnehmen, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind.

(2) [1]Die das Landesdatennetz betreibende Behörde nimmt die Befugnisse nach diesem Abschnitt für das Landesdatennetz mit Ausnahme des Netzes für den Geschäftsbereich des Justizministeriums wahr. [2]Soweit der Landesrechnungshof, die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde oder die Landtagsverwaltung betroffen ist, ist für die Wahrnehmung der Befugnisse deren Zustimmung erforderlich. [3]Im Netz für den Geschäftsbereich des Justizministeriums werden die Befugnisse nach diesem Abschnitt von einer vom Justizministerium zu bestimmenden Stelle wahrgenommen.

(3) Dieser Abschnitt gilt nicht für Hochschulen und Einrichtungen des Landes, die mit Forschungsaufgaben betraut sind.

§ 18

Allgemeine Bestimmungen

(1) Die Verwendungsbeschränkungen in diesem Abschnitt betreffen nur digitale Daten, die dem Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes unterliegen oder einen Personenbezug aufweisen.

(2) Soweit die Auswertungen nach den §§ 19 bis 22 ein Schadprogramm identifizieren, kann dieses jederzeit beseitigt oder in seiner Funktionsweise gehindert werden.

(3) Personenbezogene Daten, die zum Zweck der Gewährleistung der IT-Sicherheit nach diesem Gesetz ausgewertet werden dürfen, dürfen nicht für andere Zwecke verarbeitet werden.

§ 19

Auswertung von gespeicherten Daten

(1) [1]Zur Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme oder Angriffe sind die Behörden befugt, die auf ihren mit dem Landesdatennetz verbundenen IT-Systemen zum Erkennen und Nachverfolgen von Auffälligkeiten gespeicherten Daten automatisiert auszuwerten. [2]Für die Auswertung nach Satz 1 dürfen ausschließlich die automatisierten Ereignisdokumentationen von

1. Firewall-Systemen und Systemen zum Netzwerkbetrieb,
2. Systemen zur Erkennung und Beseitigung von Schadsoftware,
3. Systemen zur Erkennung von unerwünschten Werbe-, Betrugs- oder schädlichen E-Mails,
4. Servern von Datenbanken, Verzeichnisdiensten und Anwendungen und
5. der Betriebssoftware von Computersystemen

herangezogen werden. [3]Zum Zweck der Auswertung dürfen Daten gemäß Satz 2 zusammengeführt und gemeinsam verarbeitet werden.

(2) [1]Ergibt die automatisierte Auswertung nach Absatz 1, dass zureichende tatsächliche Anhaltspunkte für eine Gefahr nach Absatz 1 Satz 1 nicht bestehen, so sind die Auswertungsergebnisse und gefertigte Kopien von Ereignisdokumentationen nach Absatz 1 Satz 2 unverzüglich zu löschen. [2]Die Speicherung und sonstige Verarbeitung nach dem ursprünglichen Verwendungszweck bleiben hiervon unberührt. [3]Eine Auswertung von Inhaltsdaten im Rahmen des Absatzes 1 ist nur unter den Voraussetzungen des § 22 zulässig. [4]Die Erstellung von personenbezogenen Profilen zur Vorhersage des Nutzungsverhaltens von natürlichen Personen ist untersagt.

§ 20

Erhebung und Auswertung des Datenverkehrs

(1) [1]Zur Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme oder Angriffe sind die Behörden befugt, an eigenen Übergabe- und Knotenpunkten, die mit dem Landesdatennetz verbunden sind, nach auffälligem Datenverkehr zu suchen. [2]Zu diesem Zweck darf der in diesen Übergabe- und Knotenpunkten anfallende Datenverkehr automatisiert erhoben und entschlüsselt werden. [3]Es dürfen

1. Erhebungszeitpunkt, IP-Adresse einschließlich Subnetzmaske, Präfixlänge, Port und Medienzugriffskontrolladresse (Media-Access-Control-Address — MAC-Adresse), vollständiger Domänenname sowie die Kopf- und Statusdaten von Netzwerkpaketen für ein- und ausgehende Verbindungen,

2. für ein- und ausgehende Verbindungen auf Basis des Hypertext-Übertragungsprotokolls (Hypertext Transfer Protocol — HTTP) sowie des verschlüsselten Hypertext-Übertragungsprotokolls (Hypertext Transfer Protokoll Secure — HTTPS) zusätzlich zu Nummer 1 der vollständige einheitliche Ressourcenzeiger (Uniform Resource Locator — URL) und die Kopfdaten (ohne Cookie),

3. für Verbindungen auf Basis des Domain-Name-Service Protokolls (DNS) alle Inhalte der DNS-Anfrage (DNS Query) sowie der DNS-Antwort (DNS Response)

unverzüglich automatisiert ausgewertet werden. [4]Ergänzend zu den Sätzen 1 bis 3 sind die Behörden zur Erkennung und Analyse auffälligen Datenverkehrs eines Verzeichnisdienstes befugt, den Datenverkehr eines Verzeichnisdienstes zu erheben und auszuwerten.

(2) [1]Ergibt die automatisierte Auswertung nach Absatz 1 Satz 3, dass zureichende tatsächliche Anhaltspunkte für eine Gefahr nach Absatz 1 Satz 1 nicht bestehen, so sind die Daten einschließlich der Auswertungsergebnisse unverzüglich zu löschen. [2]Eine Auswertung von Inhaltsdaten im Rahmen des Absatzes 1 ist nur unter den Voraussetzungen des § 22 zulässig.

§ 21

Auswertung ohne Inhaltsdaten

(1) [1]Soweit die automatisierte Auswertung nach § 19 Abs. 1 oder § 20 Abs. 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass bestimmte Daten zur Abwehr von Gefahren im Sinne des § 19 Abs. 1 Satz 1 oder des § 20 Abs. 1 Satz 1 erforderlich sind, dürfen diese weiter einzelfallbezogen automatisiert ausgewertet werden. [2]Für diesen Zweck dürfen diese Daten höchstens sieben Tage gespeichert werden und sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind.

(2) [1]Hat sich aus der weiteren Auswertung nach Absatz 1 ergeben, dass hinreichende tatsächliche Anhaltspunkte für den Verdacht bestehen, dass die Daten nach § 19 Abs. 1 oder § 20 Abs. 1 durch einen Angriff oder ein Schadprogramm verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben, so dürfen die Daten auch nicht automatisiert ausgewertet und entpseudonymisiert werden. [2]Dies gilt nur, soweit und solange die Datenverarbeitung zur Abwehr des Schadprogramms oder Angriffs, zur Abwehr von Gefahren, die von dem Schadprogramm oder Angriff ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder Angriffe erforderlich ist. [3]Die weitere Auswertung nach Satz 1 bedarf der Anordnung der Behördenleitung und einer oder eines weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung nach Satz 3 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. [5]Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen.

(3) Die für die Zwecke der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse sind unverzüglich zu löschen, soweit sie nicht mehr erforderlich sind.

§ 22

Auswertung von Inhaltsdaten

(1) [1]Zur Abwehr von Gefahren für die IT-Sicherheit des Landes durch Sicherheitslücken, Schadprogramme oder Angriffe sind die Behörden befugt, die in § 19 Abs. 1 und § 20 Abs. 1 angefallenen Inhaltsdaten automatisiert nach Hinweisen auf Schadprogramme oder Angriffe unverzüglich auszuwerten. [2]Die für die Zwecke der Auswertung nach Satz 1 erhobenen Daten sowie die Auswertungsergebnisse sind nach ihrer automatisierten Auswertung unverzüglich zu löschen, es sei denn, die nachfolgenden Absätze sehen eine weitere Verwendung vor.

(2) [1]Soweit die automatisierte Auswertung nach Absatz 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass einzelne Daten zum Schutz vor Schadprogrammen oder Angriffen erforderlich sind, dürfen diese für höchstens sieben Tage gespeichert werden. [2]Diese Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies automatisiert möglich ist und sie nicht bereits pseudonym sind. [3]Die weitere, einzelfallbezogene Auswertung der Daten erfolgt nur automatisiert. [4]Die Speicherung nach Satz 1 bedarf der unverzüglichen Genehmigung der Behördenleitung und einer oder eines weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [5]Sofern eine solche Person nicht beschäftigt ist, ist die Genehmigung nach Satz 4 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. [6]Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen.

(3) [1]Eine über die Absätze 1 und 2 hinausgehende, insbesondere nicht automatisierte oder direkt personenbezogene Auswertung der Daten nach Absatz 1 Satz 1 ist nur zulässig, soweit und solange hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass diese durch ein Schadprogramm oder einen Angriff verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben. [2]Dies gilt nur, soweit die Datenverarbeitung

zur Abwehr des Schadprogramms oder Angriffs, zur Abwehr von Gefahren, die von dem Schadprogramm oder Angriff ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist. [3]Die Datenverarbeitung nach Satz 1 bedarf der Anordnung der Behördenleitung und einer oder eines weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung nach Satz 3 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. [5]Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen.

(4) Die für den Zweck der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse sind unverzüglich zu löschen, soweit sie nicht mehr erforderlich sind.

(5) [1]Soweit möglich ist bei der Datenverarbeitung nach dieser Vorschrift technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen oder die geeignet sind, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen, nicht erhoben werden. [2]Werden dennoch aufgrund der Maßnahmen nach den Absätzen 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder besondere Kategorien personenbezogener Daten erlangt, so dürfen diese nicht verwendet werden. [3]Die zum Zweck der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse, die den Kernbereich privater Lebensgestaltung betreffen oder die geeignet sind, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen, sind unverzüglich zu löschen. [4]Dies gilt auch in Zweifelsfällen. [5]Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. [6]Die Dokumentation darf ausschließlich für Zwecke der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung verwendet werden. [7]Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 23

Gewährleistung der Datensicherheit

(1) [1]Die nach den §§ 19 bis 22 erhobenen oder gespeicherten Daten sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme, Veränderung und Verwendung zu schützen. [2]Bei der Umsetzung dieser Maßnahmen ist ein besonders hohes Maß an Datensicherheit zu gewährleisten.

(2) Insbesondere

1. ist organisatorisch sicherzustellen, dass eine Kenntnisnahme der Daten nach den §§ 19 bis 22 durch andere als die dafür bestimmten Personen ausgeschlossen ist,
2. sind die IT-Systeme für Datenverarbeitung nach den §§ 19 bis 22 von den für die üblichen betrieblichen Aufgaben vorgehaltenen IT-Systeme, insbesondere die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben vorgesehenen Speichereinrichtungen, zu trennen,
3. sind besondere Sicherungsmaßnahmen gegen den unberechtigten Zugriff aus anderen Netzen, insbesondere aus dem Internet, zu treffen,
4. sind die personenbezogenen Daten frühestmöglich zu anonymisieren oder zu pseudonymisieren,
5. sind nach dem Stand der Technik als besonders sicher geltende Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit der gespeicherten Daten einzusetzen,
6. sind der Zutritt zu den und der Zugriff auf die Datenverarbeitungsanlagen auf Personen zu beschränken, die durch die jeweilige Behördenleitung hierzu besonders ermächtigt sind, und
7. ist technisch und organisatorisch sicherzustellen, dass der Zugriff auf die Daten nur gemeinsam durch mindestens zwei hierzu besonders ermächtigte Personen erfolgen kann.

(3) [1]Zum Zweck der Datenschutzkontrolle ist jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren von den nach den §§ 19 bis 22 erhobenen oder gespeicherten Daten in einem Protokoll aufzunehmen. [2]Das Protokoll enthält Zeitpunkt und Art des Zugriffs, eine eindeutige Kennung der auf die Daten zugreifenden Personen sowie den Zweck des Zugriffs. [3]Das Protokoll darf ausschließlich zum Zweck der Rechtmäßigkeitskontrolle verwendet werden. [4]Die Einträge in das Protokoll sind zwölf Monate nach ihrer Aufnahme zu löschen.

(4) [1]Der zuständigen Aufsichtsbehörde für den Datenschutz ist einmal im Jahr eine Aufstellung über die nach den §§ 19 bis 22 und 25 erfolgten Verarbeitungen sowie die Dokumentation nach § 26 vorzulegen. [2]Satz 1 gilt nicht für den Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten, soweit sie bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten.

§ 24

Sicherheitskonzept

[1]Eine Behörde darf von den Ermächtigungen der §§ 19 bis 22 nur Gebrauch machen, wenn sie ein Sicherheitskonzept erstellt hat und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen aktenkundig gemacht hat. [2]Das Sicherheitskonzept ist vor jeder Veränderung der eingesetzten technischen Systeme zu aktualisieren und alle zwei Jahre einer Revision zu unterziehen. [3]Für jede Veränderung des Sicherheitskonzeptes gilt Satz 1 entsprechend.

§ 25

Benachrichtigung der betroffenen Personen und Behörden

[1]Die von Maßnahmen nach diesem Gesetz betroffenen Personen und Behörden sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. [2]Die Benachrichtigung kann unterbleiben,

1. solange hierdurch der Ermittlungszweck eines Straf- oder Disziplinarverfahrens oder die IT-Sicherheit gefährdet würde,
2. wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat.

[3]Sofern eine Benachrichtigung unterbleiben soll, bedarf dies der Anordnung der Behördenleitung und einer oder eines weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung nach Satz 3 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. [5]Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen.

§ 26

Dokumentation

[1]Anordnungen und Genehmigungen nach § 21 Abs. 2 Satz 3, § 22 Abs. 2 Satz 4 und Abs. 3 Satz 3 sowie § 25 Satz 3 sind zu dokumentieren. [2]Die Dokumentation darf ausschließlich für Zwecke der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung der Daten verwendet werden. [3]Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 27

Übermittlung personenbezogener Daten

(1) [1]Die Behörden sollen die Daten nach den §§ 21 und 22 übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100 a Abs. 2 der Strafprozessordnung bezeichneten Straftat,
2. an die Polizeibehörden zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person,
3. an die Verfassungsschutzbehörde, wenn tatsächliche Anhaltspunkte dafür bestehen, dass diese zur planmäßigen Beobachtung und Aufklärung eines Beobachtungs- oder Verdachtsobjekts, das auf die Anwendung oder Vorbereitung von Gewalt gerichtet ist, oder zur Erfüllung der Aufgabe nach § 3 Abs. 1 Nr. 2 des Niedersächsischen Verfassungsschutzgesetzes erforderlich sind.

[2]Die Übermittlung nach Satz 1 Nrn. 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. [3]Für das Verfahren nach Satz 1 Nrn. 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. [4]Für die Übermittlung der entsprechenden personenbezogenen Daten nach Satz 1 Nr. 3 gelten die §§ 9 bis 16 des Artikel 10-Gesetzes entsprechend.

(2) [1]Die Behörden können nach §§ 21 und § 22 verarbeitete personenbezogene Daten an die für den Betrieb der Informationstechnik der Behörden zuständigen Stellen oder damit beauftragte Betriebe übermitteln, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die IT-Sicherheit der Behörden erforderlich ist. [2]Die das Landesdatennetz betreibende Behörde und die vom Justizministerium bestimmte Stelle können im Rahmen der Wahrnehmung ihrer Aufgaben nach § 13 Abs. 2 und 3 personenbezogene Daten an die an das Landesdatennetz angeschlossenen Behörden übermitteln, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die IT-Sicherheit der Behörden erforderlich ist.

§ 28

Einschränkung von Grundrechten

Das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes wird durch die §§ 19 bis 22 und 27 eingeschränkt.

Artikel 2

Änderung des Niedersächsischen Beamtengesetzes

Nach § 92 des Niedersächsischen Beamtengesetzes vom 25. März 2009 (Nds. GVBl. S. 72), zuletzt geändert durch Artikel 21 des Gesetzes vom 16. Mai 2018 (Nds. GVBl. S. 66), wird der folgende § 92 a eingefügt:

„§ 92 a

Verarbeitung von Personalaktendaten im Auftrag

(1) [1]Die personalverwaltende Behörde darf gemäß Artikel 28 der Datenschutz-Grundverordnung Personalaktendaten im Auftrag nur für

1. die Bewilligung, Festsetzung oder Zahlbarmachung von Geldleistungen und

2. die automatisierte Erledigung von Aufgaben für Zwecke nach § 88 Abs. 1 Satz 1

verarbeiten lassen. [2]Die personalverwaltende Behörde hat die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den Auftragsverarbeiter regelmäßig zu kontrollieren.

(2) Die Auftragserteilung und die Genehmigung einer Unterauftragserteilung bedürfen der vorherigen Zustimmung der obersten Dienstbehörde.

(3) Eine nicht öffentliche Stelle darf nur beauftragt werden, wenn die Beauftragung der Erfüllung von Aufgaben nach Absatz 1 Satz 1 dient und beim Verantwortlichen sonst Störungen im Geschäftsablauf auftreten können oder der Auftragsverarbeiter die übertragenen Aufgaben erheblich kostengünstiger erledigen kann.“

Artikel 3

Evaluation und Inkrafttreten

(1) Die Landesregierung überprüft zwei Jahre nach Inkrafttreten dieses Gesetzes die finanziellen Auswirkungen der Umsetzung auf die Kommunen.

(2) [1]Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft. [2]Abweichend von Satz 1 tritt

1. Artikel 1 § 6 Abs. 3 und § 12 Abs. 1 Satz 1 Nr. 6 am 18. April 2020,

2. Artikel 1 § 4 Abs. 2 bis 4, § 5 Abs. 2, § 6 Abs. 1 und 2, § 12 Abs. 1 bis 3 am 1. Juli 2021 und

3. Artikel 1 § 5 Abs. 5 am 1. Januar 2023

in Kraft.

Begründung

A. Allgemeiner Teil

I. Anlass, Ziele und Schwerpunkte des Entwurfs

Vor der rasanten Entwicklung der Digitalisierung in Gesellschaft und Wirtschaft kann sich die Verwaltung nicht verschließen. Bürgerinnen, Bürger, Unternehmen und Verbände erwarten, dass die Verwaltung auf den digitalen Wandel reagiert und auch die digitale Abwicklung von Verwaltungsdienstleistungen ermöglicht. Die Förderung der digitalen Verwaltung bedeutet damit einen Ausbau und eine Koordinierung digitaler Prozesse, die zu schnelleren, leistungsfähigeren und effizienteren Verfahren führt.

Eine moderne, digitale Verwaltung bedarf einer gemeinsamen, übergeordneten Zielsetzung und Koordinierung und eines rechtlich verbindlichen Rahmens.

Zu Artikel 1 (Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit):

Der Bundesgesetzgeber hat mit seinem am 1. August 2013 (überwiegend) in Kraft getretenen E-Government-Gesetz (EGovG) vom 25. Juli 2013 (BGBl. I S. 2749) den Abbau bundesrechtlicher Hindernisse beim Einsatz elektronischer Kommunikationsmittel mit der Verwaltung verfolgt. Auch in Niedersachsen sollen die elektronische Kommunikation mit der Verwaltung erleichtert und Land und Kommunen die Möglichkeit eröffnet werden, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten.

Zudem hat der Bundesgesetzgeber mit dem Onlinezugangsgesetz (OZG) vom 14. August 2017 (BGBl. I S. 3122, 3138), das am 18. August 2017 in Kraft getreten ist, Bund und Länder dazu verpflichtet, ihre Verwaltungsleistungen künftig elektronisch über Verwaltungsportale anzubieten. Hiermit ist ein weitreichender Zielrahmen gesetzt, den es auch in Niedersachsen zu beachten gilt. Durch das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) werden die gesetzlichen Vorgaben geschaffen, um die Ziele des Onlinezugangsgesetzes in Niedersachsen vollständig, rechtzeitig und systematisch umzusetzen.

Das vorliegende Gesetz setzt darüber hinaus die Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen (ABl. EU Nr. L 133 S. 1) um. Niedersächsische Auftraggeber Europaweiter Vergabeverfahren werden damit verpflichtet, elektronische Rechnungen ab dem 18. April 2020 empfangen und verarbeiten zu können. Darüber hinaus werden auch Vergabeverfahren im Geltungsbereich des Niedersächsischen Tariftreue- und Vergabegesetzes (NTVergG) ab 10 000 Euro erfasst.

Ein gewichtiger Teil dieses Gesetzes dient der Abwehr von Risiken, die sich aus der Digitalisierung der Verwaltung ergeben. Mit der zunehmenden Digitalisierung der Verwaltung werden umfassend personenbezogene und sonstige zu schützende Daten elektronisch gespeichert und übermittelt. Der Schutz dieser Daten und der zu ihrer Verarbeitung eingesetzten IT-Systeme wird zu einer fundamentalen Anforderung, um die Rechtmäßigkeit, Funktionsfähigkeit und vor allem die Verlässlichkeit der Landesverwaltung sicherzustellen. Diverse Hackerangriffe zeigen, wie schnell inzwischen Systeme infiziert und Informationen in die falschen Hände gelangen können. Den immer ausgereifteren Hackerangriffen kann nur erfolgreich begegnet werden, wenn die Verwaltung angemessene Abwehrmaßnahmen treffen kann. Hierzu bedarf es, insbesondere angesichts der fortschreitenden Digitalisierung der Verwaltung und steigender Bedrohungen aus dem Cyberraum, neuer gesetzlicher Regelungen. Diese Regelungen sind im Bereich der Landesverwaltung zwingend erforderlich, da aktuelle Angriffstechnologien mit den dort etablierten technischen Verfahren – wie portbasierten Firewalls, Virenscannern und Proxies – und im bestehenden Ermächtigungsrechtsrahmen nicht mehr zuverlässig abgewehrt werden können.

Zu Artikel 2 (Niedersächsisches Beamtengesetz):

Im Zusammenhang mit der in Artikel 1 normierten Möglichkeit zur elektronischen Aktenführung soll in die Vorschriften des Niedersächsischen Beamtengesetzes (NBG) eine Bestimmung zur Auftragsverarbeitung von Personalaktendaten eingefügt werden. Für die Digitalisierung von Personalakten durch einen Dritten (sog. Auftragsverarbeitung gemäß der Verordnung [EU] 2016/679 [Datenschutz-Grundverordnung]) bedarf es zwingend einer speziellen Ermächtigungsgrundlage. Durch die Regelung im Niedersächsischen Beamtengesetz wird unter anderem ermöglicht, dass eine öffentliche oder nicht öffentliche Stelle zum Zweck der Übertragung von Papierakten in elektronische Datenbestände Personalakten für die personalverwaltende Behörde einscannt.

II. Auswirkungen auf die Umwelt, den ländlichen Raum und die Landesentwicklung

Negative Auswirkungen auf die Umwelt, den ländlichen Raum und die Landesentwicklungen zeichnen sich aufgrund des Gesetzentwurfs nicht ab. Das Gesetz führt vielmehr zu einer Verbesserung der Situation der Bevölkerung, insbesondere in peripheren ländlichen Räumen, da durch die Förderung der digitalen Verwaltung die Erreichbarkeit von Verwaltungsleistungen verbessert wird und Mobilitätsbedarfe reduziert werden. Dies setzt allerdings ausreichende Bandbreiten der Netzzugänge voraus.

III. Auswirkungen auf die Verwirklichung der Gleichstellung von Frauen und Männern und auf Familien

Die Digitalisierung ist für die zeitlichen und räumlichen Strukturen, die den Alltag von Familien prägen, von großer Bedeutung. Vieles, was früher nur im persönlichen Kontakt erledigt werden konnte, ist nun digital möglich. Mit der Digitalisierung von Verwaltungsverfahren wird Familien ermöglicht, Behördenangelegenheiten ohne zeitliche und räumliche Beschränkungen zu erledigen. Das entspricht einer modernen Familienzeitpolitik und fördert auch die Vereinbarkeit von Beruf und Familie.

IV. Auswirkungen auf Menschen mit Behinderungen

Dieses Gesetz führt zu einer Verbesserung der Situation vieler Menschen mit Behinderungen, indem etwa diejenigen unter ihnen, die in ihrer Mobilität eingeschränkt sind und beim Aufsuchen einer Behörde fremde Hilfe benötigen, zukünftig in mehr Fällen mit der Verwaltung vom heimischen Computer kommunizieren und die Online-Dienste nutzen können. Menschen mit Sehbehinderungen erleiden durch das Gesetz keine Nachteile, da ihre Belange durch das Niedersächsische Behindertengleichstellungsgesetz berücksichtigt sind.

V. Wesentliche Ergebnisse der Gesetzesfolgenabschätzung sowie voraussichtliche Kosten und haushaltsmäßige Auswirkungen des Gesetzes

1. Wirtschaft und Bürgerschaft

Für Bürgerinnen, Bürger, Unternehmen und Verbände außerhalb der Verwaltung sind keine Verpflichtungen mit Kostenfolgen zu erwarten. Für sie werden keine Informationspflichten oder Maßnahmen, die einen Erfüllungsaufwand bedeuten würden, eingeführt.

Durch die Regelungen des Gesetzes sind vielmehr langfristig und insgesamt deutliche Erleichterungen für Bürgerinnen, Bürger, Unternehmen und Verbände zu erwarten. Das Gesetz trägt dazu bei, den Wirtschaftsstandort Niedersachsen weiterhin attraktiv zu halten, da digitale Angebote durchaus einen Standortvorteil darstellen können. Erleichterungen werden nicht nur durch direkte Kostenersparnis (z. B. weniger Portokosten, Vermeidung von Reisekosten und hohen Gebühren) erwartet, sondern vor allem durch Zeitersparnis (schnellere Information, weniger Behördengänge und Wartezeiten), kürzere Dauer bei Antragsverfahren, mehr Transparenz (umfangreichere Informationsangebote) und mehr zeitliche Flexibilität (Dienstleistungen 24 Stunden am Tag, 7 Tage in der Woche verfügbar).

2. Verwaltung

Für die Abschätzung der finanziellen Folgen in der Verwaltung ist zu berücksichtigen, dass bereits gesetzliche Regelungen zur Digitalisierung der Verwaltung bestehen, aus denen sich finanzielle Belastungen herleiten. Von besonderer Bedeutung ist das Onlinezugangsgesetz. § 1 OZG verpflichtet Bund und Länder, bis spätestens Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. § 3 OZG verpflichtet Bund und Länder, Nutzerkonten einzurichten. Das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit trifft Regelungen, um die Verpflichtungen des Onlinezugangsgesetzes für Niedersachsen systematisch umzusetzen. Die im Folgenden aufgeführten Kosten ergeben sich aus diesen durch das Onlinezugangsgesetz veranlassten Regelungen. Auch die Richtlinie 2014/55/EU (zur elektronischen Rechnungsstellung – E-Rechnung), die in § 6 Abs. 3 und 4 NDIG für Niedersachsen gesetzlich geregelt wird, führt zu finanziellen Folgen. Eine Ausnahme hiervon bildet lediglich die Regelung zur elektronischen Aktenführung in § 10 NDIG. Zur Umsetzung des Onlinezugangsgesetzes und auch der Richtlinie 2014/55/EU müssen eingehende Dokumente nachweissicher aufbewahrt werden. Bei bestimmten elektronischen Dokumenten, z. B. elektronisch signierten, kann dies nicht durch Aufbewahrung eines Ausdrucks erfolgen, weil hierdurch die Beweiskraft erheblich reduziert wird. Auf Arbeitsplätzen, auf denen solche Dokumente eingehen, ist also eine elektronische Aktenführung unerlässlich. Das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit sieht allerdings nicht nur auf diesen, sondern auf allen Arbeitsplätzen der Landesverwaltung eine elektronische Aktenführung vor.

E-Government und Informationstechnik prägen die Verwaltung bereits seit langer Zeit. Durch das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit werden diese Prozesse befördert und optimiert, aber nur in wenigen Fällen initiiert. Vielfach sind Verfahren, Organisationen und Basisdienste bereits vorhanden und werden durch das Gesetz angepasst, verbindlich eingeführt oder auf einen bestimmten Nutzerkreis ausgeweitet. Über die Folgen durch das Onlinezugangsgesetz und die Richtlinie 2014/55/EU hinaus sind daher im Verhältnis zu den zahlreichen Anforderungen des Gesetzes nur vergleichsweise geringfügige Mittel zu deren Umsetzung für den Bereich des E-Governments erforderlich. Eine Besonderheit stellt nur die elektronische Aktenführung dar, deren vollständige Einführung entsprechend hohe Investitionen erfordert.

Weiterhin ist von Bedeutung, dass die Landesregierung in ihrer IT-Strategie vom September 2016 eine digitale Verwaltung anstrebt und viele Regelungen des Gesetzentwurfs zur Umsetzung der IT-Strategie beitragen. Bereits mit der IT-Strategie hat die Landesregierung die Notwendigkeit anerkannt, umfassend und fortgesetzt in die Modernisierung der IT der Landesverwaltung investieren zu müssen. Entsprechende Maßnahmen werden daher im Rahmen der verfügbaren Haushaltsmittel einen Ausgabeschwerpunkt des Landeskabinetts darstellen. Dieses Gesetz enthält Verpflichtungen, die zu solchen Ausgaben führen werden. Im Folgenden werden die finanziellen Auswirkungen abgeschätzt und tabellarisch zusammengefasst. Eine genaue Bezifferung der Kosten der jeweiligen

Maßnahmen ist von einer Vielzahl von Faktoren abhängig, die sowohl die technische Entwicklung als auch den zeitlichen Rahmen und die konkrete Ausgestaltung betreffen. Die genaue Bezifferung wird in den Wirtschaftlichkeitsbetrachtungen zu den einzelnen Projekten und Maßnahmen vorzunehmen sein.

Für die Behörden des Landes werden mit diesem Gesetz verschiedene Verpflichtungen geschaffen, die unterschiedliche finanzielle Folgen nach sich ziehen. Auch für Kommunen entstehen Kosten, die aber erheblich geringer ausfallen als für die Behörden des Landes. Hierbei ist zu differenzieren. Einen Großteil der von den Kommunen zu tragenden Kosten ist durch die Richtlinie 2014/55/EU zur E-Rechnung veranlasst und ist somit nicht konnexitätsrelevant. Zudem unterstützt das Land die Kommunen mit der Bereitstellung von Basisdiensten. Die Kosten für Basisdienste können, soweit das Gesetz nicht ausdrücklich etwas anderes vorsieht, auf die nutzenden Behörden umgelegt werden. Es wird im Folgenden aber davon ausgegangen, dass nur eine Umlage der Betriebskosten, nicht der Projektkosten erfolgen wird.

Durch die Regelungen des Gesetzes sind langfristig deutliche Erleichterungen für die Tätigkeiten der Verwaltung zu erwarten. Sie vermindern insbesondere Mehrkosten, die sich ergeben würden, wenn die Verwaltung bei einer zunehmend elektronisch basierten Kommunikation in der Gesellschaft weiterhin die herkömmlichen Arbeitsweisen aufrechterhalten würde. Außerdem werden Mehrkosten verhindert, weil durch zentral bereitzustellende Basisdienste und ihre verbindliche Nutzung kostenintensive Einzellösungen verhindert werden.

Die gesetzlichen Verpflichtungen haben finanzielle Auswirkungen, die im Folgenden vollständig aufgeführt werden. Durch die Umsetzung des Gesetzes werden Voraussetzungen geschaffen, die neben der unmittelbaren Wirkung zahlreiche weitere Chancen zur Verbesserung von Bürgerservices und zur Optimierung von Geschäftsprozessen bieten. So können z. B. elektronisch eingehende Anträge so in die Fachverfahren importiert werden, dass dort sowohl die Erfassung entfallen als auch eine automatische Antragsprüfung erfolgen kann. Zuständige Bedienstete können so bereits nach kurzer Sichtprüfung einen Bescheid erstellen und den Vorgang abschließen. Wenn die Verwaltung diese Chancen nutzen möchte, sind zusätzliche Investitionen erforderlich, etwa zur Verknüpfung von Basisdiensten und individuellen Fachverfahren. Die hierfür erforderlichen Mittel und die resultierenden Einsparungen werden hier nicht dargestellt, weil die Verwaltung selbst entscheiden muss, wann sie welche Optimierungsvorhaben durchführt.

Finanzielle Auswirkungen im Einzelnen:

Im Folgenden werden die Auswirkungen für alle Behörden betrachtet. Soweit erforderlich werden Kosten nach Verwaltungsbereichen differenziert dargestellt (z. B. für die Kommunen). Eine Differenzierung nach Ressorts erfolgt nicht.

Nach § 4 NDIG sind die Behörden verpflichtet, sowohl einen Zugang zur Übermittlung elektronischer Dokumente (z. B. E-Mail-Zugang) und einen Zugang über Nutzerkonten zu eröffnen als auch die Kommunikation mit De-Mail zu ermöglichen und zur Identitätsfeststellung die entsprechenden Funktionen des elektronischen Identitätsnachweises anzubieten (letzteres betrifft nur die Behörden des Landes). Der E-Mail-Zugang ist bereits weitgehend realisiert, sodass hierdurch sowohl beim Land als auch bei den Kommunen keine neuen Kosten entstehen. Damit ist auch der Empfang von Dokumenten mit einer qualifizierten elektronischen Signatur ohne Zusatzkosten möglich. Erst eine Überprüfung der Signatur erfordert zusätzliche IT-Dienste. Diese Dienste können aber im Bedarfsfall über IT-Dienstleister bezogen werden und sind nur in Ausnahmefällen erforderlich, sodass dadurch keine nennenswerten Kosten entstehen.

Für den Zugang über Nutzerkonten, den die Behörden einrichten müssen (auch bereits aufgrund des § 3 OZG), stellt das Niedersächsische Ministerium für Inneres und Sport den Behörden des Landes und den Kommunen nach § 12 NDIG einen Basisdienst zur Verfügung, der bereits heute in einer ersten Ausbaustufe in Betrieb ist. Für den Ausbau zu einem flächendeckenden Dienst werden einmalige Kosten in Höhe von 5 000 000 Euro beim Land und nach Ausbau ab 2023 laufende Kosten von jährlich 400 000 Euro erwartet. Bei Behörden, die diesen Basisdienst nutzen, fallen keine weiteren Kosten für die Bereitstellung von Nutzerkonten an. Sie müssen lediglich regelmäßig den Eingang von Nachrichten über den Nutzerkonto-Basisdienst prüfen und diese gegebenenfalls an die zuständige Stelle weiterleiten, soweit dies nicht bereits automatisch erfolgt. Dies entspricht dem bereits heute üblichen Einsehen von Poststellen-E-Mail-Konten.

Für die Kommunikation mit De-Mail wird eine zentrale Infrastruktur (Gateway) für alle Behörden des Landes zur Verfügung zu stellen sein, die jeweilige Nutzung durch die Behörden ist anlassbedingt. Im kommunalen Bereich ist ein Gateway wohl nicht erforderlich. Die Projektkosten für ein De-Mail-Gateway liegen einmalig bei 600 000 Euro, die jährlichen Betriebskosten nach Ausbau bei 200 000 Euro. Die Bereitstellungskosten durch einen Provider werden mit 200 Euro pro De-Mail-Postfach und pro Jahr angenommen. Es wird erwartet, dass noch 500 De-Mail-Postfächer bei Behörden des Landes und 450 Postfächer im kommunalen Bereich eingerichtet werden müssen. Hierdurch entstehen nach Ausbau jährliche Betriebskosten beim Land von 100 000 Euro und bei den Kommunen von 90 000 Euro. Durch die geringeren Kosten der De-Mail gegenüber der Briefpost ist zudem mit Kostenreduzierungen bei den einzelnen Behörden zu rechnen.

Der elektronische Identitätsnachweis ist bereits als Basisdienst im Niedersächsischen Antragsverwaltungssystem Online realisiert. Dieser Dienst wird gemäß § 12 Abs. 1 NDIG allen Behörden des Landes zur Verfügung gestellt,

weitere Kosten können hierbei durch gegebenenfalls erforderliche Schnittstellenprogrammierungen entstehen. Diese sind im Vergleich jedoch geringer als entsprechende Kosten bei einer jeweils verfahrensbezogenen Integration der elektronischen Identifizierung.

Nach § 5 Abs. 1 NDIG werden die Behörden verpflichtet, Informationen über ihre Aufgaben, ihre Anschrift, ihre Geschäftszeiten sowie postalische, telefonische und elektronische Erreichbarkeiten bereitzustellen. Nach § 5 Abs. 2 NDIG werden die Behörden außerdem verpflichtet, zusätzlich Verfahrensinformationen sowie weitere Informationen im Internet bereitzustellen. Gemäß § 12 Satz 1 Nr. 3 NDIG muss das für IT-Steuerung zuständige Ministerium einen entsprechenden Basisdienst bereitstellen. Die fachlich zuständigen obersten Landesbehörden müssen sicherstellen, dass bei Vollzug von Bundes- oder Landesrecht durch die Kommunen die entsprechenden Informationen über öffentlich zugängliche Netze kostenfrei bereitstehen. Somit müssen die Kommunen lediglich diese Informationen abrufen, in ihre Systeme integrieren und gegebenenfalls um einige wenige, eigene Inhalte ergänzen. Dies sollte einen minimalen Aufwand verursachen. Im Ergebnis sollten keine relevanten Kosten hierfür bei den Kommunen entstehen. Da die Kontaktinformationen nur selten geändert werden und bereits heute meist zur Verfügung stehen, sind nennenswerte Zusatzbelastungen für die Pflege der Daten nicht zu erwarten. Die weiteren Informationen nach § 5 Abs. 2 stehen bereits heute in großen Teilen zur Verfügung, zumeist im Bürger- und Unternehmensservice (BUS) des Landes. Zukünftig muss der BUS als zentraler Bestandteil des niedersächsischen Verwaltungsportals alle Leistungsbeschreibungen vollständig bereitstellen, ergänzt mit behördenspezifischen Informationen. Die Informationen müssen verständlich gestaltet sein. Der hierfür notwendige Personalaufwand beträgt insgesamt 2 000 000 Euro pro Jahr bis 2021. Danach bedarf es einer zentralen Redaktion, um den Datenbestand im BUS korrekt, aktuell, gut lesbar und vollständig zu halten. Die zentrale Redaktion kann auch die einzelnen Behörden bei der Pflege der Daten entlasten. Für die Redaktion werden dauerhaft Kosten von 200 000 Euro pro Jahr erwartet. Durch die bessere und umfassende Information der Bürgerinnen und Bürger, Unternehmen und Verbände im Internet ist gleichzeitig eine Entlastung von Informationsaufgaben über Telefon, durch direktes Gespräch oder Schriftverkehr zu erwarten.

Nach § 5 Abs. 5 NDIG sind die Behörden verpflichtet, ihre Verwaltungsleistungen auch elektronisch anzubieten. Diese Regelung beschreibt den bereits im Onlinezugangsgesetz aufgeführten Zielausbau der digitalen Verwaltung in Hinblick auf das Online-Angebot für Bürgerinnen, Bürger, Unternehmen und Verbände. Teilweise ist dieses Angebot bereits heute vorhanden, insbesondere für Dienstleister in der Wirtschaft aufgrund der Umsetzung der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (ABl. EU Nr. L 376 S. 36). Ansonsten lässt sich diese Regelung durch die Bereitstellung und Entgegennahme von elektronischen Formularen erfüllen, was mithilfe des zentralen Formularservices und der in § 4 NDIG vorgegebenen elektronischen Zugänge durchführbar ist. Der Formularserver stellt aktuell eine große Anzahl an elektronischen Formularen bereit, die unter anderem von den Kommunen kostenfrei genutzt werden können. Viele Verwaltungsbereiche stellen selbst elektronische Formulare bereit, z. B. die Steuerverwaltung oder das Niedersächsische Landesamt für Bezüge und Versorgung. In anderen Bereichen werden noch elektronische Formulare zu erstellen und im Formularserver bereitzustellen sein. Dabei ist zu beachten, dass bei den Behörden durch die Erstellung von elektronischen Formularen nur vergleichsweise geringe Kosten entstehen, die durch die Einsparung von Druckkosten für herkömmliche Formulare kompensiert werden. Alternativen zu Formularen sind Online-Assistenzsysteme, die z. B. durch die einzelnen Schritte eines Antrags führen, dabei auf die bereits erfassten Daten reagieren, Hilfen anbieten und Plausibilitätskontrollen durchführen. Solche Systeme sind zwar aufwändiger als einfache elektronische Formulare, führen aber zu einer höheren Akzeptanz der Online-Angebote. Für den Ausbau von Formularen und Assistenzsystemen werden 20 000 000 Euro pro Jahr bis 2022 erwartet sowie 5 000 000 Euro für das Antragsverwaltungssystem NGovOS. Den Kommunen wird auch hier der Basisdienst kostenfrei zur Verfügung gestellt, weshalb ihnen hierfür keine weiteren Kosten entstehen.

Die schlichte Entgegennahme elektronischer Formulare ohne Änderung der Abläufe sollte allerdings vermieden werden. Elektronisch eingereichte ausgefüllte Formulare sollten vielmehr automatisiert in das jeweilige Fachverfahren der Behörde übernommen werden. In geeigneten Bereichen sollten auch Assistenzsysteme zum Einsatz kommen und mit den Fachverfahren verbunden werden. Dies ist grundsätzlich heute schon möglich. In vielen Teilen der Verwaltung besteht aber noch Umsetzungsbedarf. Der hierfür erforderliche Aufwand ist erheblich, aber nur schwer abzuschätzen. Da § 5 Abs. 5 NDIG diesen wünschenswerten Ausbau nicht vorschreibt, wird auf die Auflistung konkreter Zahlen verzichtet.

§ 6 Abs. 1 und 2 NDIG erfordern den Einsatz eines elektronischen Bezahlverfahrens, das gemäß § 12 Abs. 1 NDIG als Basisdienst bereitgestellt wird. Dieser Basisdienst wurde bereits realisiert und ist für erste Verfahren im Einsatz. Nach aktuellen Abschätzungen fallen für die Einführung elektronischer Bezahlverfahren im Land 700 000 Euro und im kommunalen Bereich 1 150 000 Euro an. Außerdem entstehen Betriebskosten (jährlich 150 000 Euro im Land und 200 000 Euro in den Kommunen nach Ausbau). Diese Kosten erreichen jedoch nicht die Erheblichkeitsgrenze, sodass keine Ausgleichspflicht besteht.

§ 6 Abs. 3 NDIG erfordert ein IT-Verfahren, das E-Rechnungen entgegennehmen und mindestens visualisieren kann. Ab 2019 werden 5 552 000 Euro einmalige und nach Aufbau 600 000 Euro jährliche Kosten für die Landesverwaltung erwartet. Die gleichen Kosten sollten im kommunalen Bereich anfallen, wenn ein zentrales System genutzt wird. Da sie auf der Richtlinie 2014/55/EU basieren, wird hierdurch keine Konnexitätsfolge ausgelöst.

Mit der Einführung der E-Rechnung sind Einsparungen zu erwarten, wenn die vollständige Rechnungsbearbeitung in der Verwaltung elektronisch durchgeführt wird. Dazu müssen die beteiligten Behörden mindestens über ein Vorgangsbearbeitungsmodul zur Zeichnung der sachlichen und rechnerischen Richtigkeit und über eine elektronische Aktenablage verfügen. Einige der eingeführten E-Akte-Systeme verfügen hierüber bereits. Außerdem wird eine Schnittstelle zum Haushaltswirtschaftssystem und idealerweise ein Ressourcenplanungssystem benötigt. Die Kommunen entscheiden selbst im Rahmen der kommunalen Selbstverwaltung, ob ein solches System eingeführt werden soll.

Die in § 9 NDIG vorgeschriebene Georeferenzierung sollte nur zu geringfügigen Kosten führen, da ein Handlungsbedarf nur besteht, wenn Register aufgrund von Rechtsvorschriften des Landes neu aufgebaut oder überarbeitet werden. Zudem gibt es heute ausreichende technische Möglichkeiten, um den Registern die Georeferenzdaten automatisiert hinzuzufügen. Ein größerer personeller Aufwand ist daher nicht zu erwarten.

Die obersten Landesbehörden stellen sicher, dass ab 1. Januar 2023 als Minimalausstattung wenigstens die Arbeitsplätze über eine elektronische Aktenführung verfügen, die Verwaltungsleistungen nach dem Onlinezugangsgesetz erbringen. Hintergrund ist, dass das Onlinezugangsgesetz die Behörden dazu verpflichtet, Dokumente auch elektronisch anzunehmen. Diese müssen auch rechtssicher aufbewahrt werden, um ihre Beweiskraft – z. B. eine elektronische Signatur – zu erhalten. Dies ist nur effektiv durch eine elektronische Aktenführung realisierbar.

Gemäß § 10 Abs. 2 Satz 3 NDIG können die Termine zur Einführung der elektronischen Akte beim Vorliegen besonderer Gründe im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung verschoben werden. Ein besonderer Grund liegt insbesondere dann vor, wenn die erforderlichen Haushaltsmittel nicht zur Verfügung stehen. Somit steht der Zeitpunkt der elektronischen Akteneinführung unter Haushaltsvorbehalt.

Für die Einführungs- und Betriebskosten der elektronischen Aktenführung liegen aus bisherigen Projekten konkrete Zahlen vor. Allerdings ist zurzeit noch unklar, mit welchem E-Akte-System, mit welchen E-Akte-Ausbaustufen und mit welchem Projektverlauf die elektronische Aktenführung umgesetzt werden soll. Daher erfolgt hier eine grobe Kostenabschätzung. Sie beruht allerdings auf den bisherigen Erfahrungen und ähnlichen Abschätzungen anderer Länder und ist insofern von der Größenordnung her belastbar. Pro Nutzerin und Nutzer werden erwartet:

400 Euro für die Beschaffung und Konfiguration von Hard- und Software,

500 Euro für Projektkosten,

600 Euro für Schulung und Einweisung in das E-Akte-System.

Insgesamt entstehen also Einmalkosten in Höhe von 1 500 Euro pro Nutzerin und Nutzer. Dies entspricht bei einem erwarteten Ausbau auf 50 000 Arbeitsplätzen einem Projektvolumen von 75 000 000 Euro. Dabei wird davon ausgegangen, dass der E-Akte-Betrieb im Wesentlichen mithilfe eines einheitlichen E-Akte-Systems gemäß § 12 Abs. 1 Satz 1 Nr. 7 NDIG zentral erfolgt.

Im Betrieb entstehen Kosten für IT-Systeme, Datenspeicherung und Software (80 Euro pro Nutzerin und Nutzer pro Jahr) sowie für organisatorischen und technischen Support (120 Euro pro Nutzerin und Nutzer pro Jahr), bei 50 000 Nutzerinnen und Nutzern also 10 000 000 Euro pro Jahr.

Bei der Ausstattung von Pilotbehörden in einem ersten Schritt fallen zunächst höhere Basiskosten an, z. B. für die Software-Konfiguration, das Serversystem oder den Support. Hierfür werden zusätzlich Einmalkosten von 5 000 000 Euro erwartet. Die Projektkosten für die Einführung der elektronischen Akte werden somit auf insgesamt 80 000 000 Euro geschätzt. Dem stehen vor allem erhebliche Arbeitserleichterungen gegenüber, etwa beim sicheren Abspeichern, Auffinden, Zeichnen und Aussondern von elektronischen Vorgängen und Dokumenten. Allein hieraus ergeben sich Arbeitsentlastungen, die in der Regel 2 bis 3 % der Arbeitszeit ausmachen. Bei entsprechender Geschäftsprozessoptimierung lassen sich mithilfe der elektronischen Akte oft auch wesentlich höhere Arbeitserleichterungen erreichen. Darüber hinaus ermöglicht die elektronische Akte den Bediensteten mehr Flexibilität bei der Arbeitsgestaltung, z. B. durch Telearbeit, und reduziert deren Pendler- und Reisetätigkeit. Sie ist außerdem unabdingbar, um bei einer zunehmend elektronischen Kommunikation weiterhin eine wirtschaftliche Basis für eine ordnungsgemäße Aktenführung zu gewährleisten. Weiterhin ermöglicht die elektronische Akte, andere Vorhaben, etwa die Einführung der E-Rechnung oder die Umsetzung des geplanten Transparenzgesetzes, mit weniger Aufwand durchzuführen.

Da die vollständige E-Akte-Einführung, wie oben beschrieben, unter Haushaltsvorbehalt steht, werden in der weiteren Gesetzesfolgenabschätzung nicht die vollständigen Kosten berücksichtigt. Aufgeführt werden lediglich die Einführungskosten von 5 000 000 Euro und Betriebskosten von 2 000 000 Euro pro Jahr. Dies wird als Minimalausstattung erwartet, um die Rechtsverpflichtungen des Onlinezugangsgesetzes zu erfüllen. Einspareffekte sind auf diese Weise allerdings nicht zu erwarten. § 10 Abs. 4 NDIG sieht vor, dass der Austausch von elektronisch geführten Akten auf elektronischem Weg erfolgen soll. Beim Vorliegen elektronischer Unterlagen stellt die elektronische Übertragung das wirtschaftlichste und schnellste Austauschverfahren dar. Die hierfür erforderlichen Basisdienste sind bereits vorhanden oder werden durch andere Regelungen geschaffen. Zusätzliche Kosten entstehen

somit nicht. Wenn im Ausnahmefall Dokumente in Papierform vorliegen und eine elektronische Übertragung zusätzliche Kosten verursacht, kann auf die elektronische Übertragung verzichtet werden, da die Regelung als Soll-Regelung formuliert ist.

Durch die in § 12 NDIG geregelte zentrale Bereitstellung von Basisdiensten wird sichergestellt, dass die Kosten für die digitale Verwaltung begrenzt bleiben. Die Kosten, die sich aus den in § 12 Abs. 1 NDIG geregelten Basisdiensten ergeben, wurden bereits oben beschrieben.

Der durch das Gesetz vorgesehene Ausbau der IT-Unterstützung, insbesondere in Form von Basisdiensten, erfordert eine Koordination und eine strategische Planung, die auch im weiteren Betrieb fortgeführt werden muss. Sie soll auch bei Organisationsfragen, die bei der Einführung neuer IT-gestützter Prozesse entstehen, unterstützen. Außerdem werden Lenkungs-, Koordinations- und Unterstützungsaufgaben in Projekten anfallen. Hierzu werden mindestens bis 2022 folgende Stellen benötigt (voraussichtlich in dem für zentrale IT-Steuerung zuständigen Ministerium zusätzlich zu bereits vorhandenen Stellen):

	Anzahl	jährliche Kosten in Euro
B 2	1	91 000
A 15	1	76 000
A 13	2	126 000
A 12	2	112 000
A 11	1	51 000
Summe	7	456 000

Die jährlichen personenbezogenen Nebenkosten betragen 170 000 Euro.

Für Lenkungs-, Koordinations- und Unterstützungsaufgaben werden darüber hinaus weitere Beschäftigungsmöglichkeiten im nachgeordneten Bereich, z. B. im IT.Niedersachsen, benötigt. In

- 2019 werden 11 Beschäftigungsmöglichkeiten (856 000 Euro, Nebenkosten 231 000 Euro) und
- ab 2020 zusätzlich 10 Beschäftigungsmöglichkeiten (insgesamt 1 577 000 Euro, 431 000 Euro Nebenkosten jährlich)

benötigt. Die gesamten Personalkosten für Koordinations- und Unterstützungsaufgaben betragen daher 1 713 000 Euro in 2019 und ab 2020 2 634 000 Euro pro Jahr.

Schließlich wird in § 2 NDIG die Funktion der oder des IT-Bevollmächtigten des Landes geregelt. Dies ist erforderlich, weil die Funktionsfähigkeit der IT-Unterstützung in der digitalen Verwaltung eine existentielle Bedeutung erhält. Kosten entstehen hierdurch nicht, weil diese Funktion bereits besteht.

Die §§ 13 bis 16 NDIG regeln die Grundsätze der Informationssicherheit in der digitalen Verwaltung, deren Erfordernis mit dem Ausbau der Digitalisierung des Verwaltungshandelns stark zunimmt. So werden mit dem Onlinezugangsgesetz Bund und Länder verpflichtet, bis spätestens Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten und Nutzerkonten einzurichten. Weiterhin ist die Richtlinie 2014/55/EU zur E-Rechnung umzusetzen. Die Bereitstellung einer sicheren Kommunikation im Sinne des De-Mail-Gesetzes vom 28. April 2011 (BGBl. I S. 666), zuletzt geändert durch Artikel 3 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745), und eines elektronischen Identitätsnachweises sind nach § 4 NDIG verpflichtend. Weitere Anforderungen an die Informationssicherheit entstehen durch die flächendeckende Einführung der elektronischen Akte (§ 10 NDIG), insbesondere wenn die Aufbewahrung von Dokumenten nicht mehr in Papierform erfolgen soll (§ 11 NDIG). Die zentrale Bereitstellung der elektronischen Basisdienste nach § 12 NDIG für die Behörden des Landes und die Kommunen stellen ebenfalls bedeutende Herausforderungen an die Informationssicherheit dar.

Diese digitalisierten Verfahren ersetzen grundlegende Verwaltungsabläufe. Ihre ordnungsgemäße und sichere Funktion wird damit unverzichtbar, um ein gesetzmäßiges Verwaltungshandeln sicherzustellen. Eine Manipulation oder der Ausfall dieser Systeme führt zu einem hohen Schaden, weil der Schutzbedarf – auch aufgrund der Konzentration der Verwaltungsdaten in diesen Verfahren – steigt. Aufgrund ihrer Bedeutung und ihres Umfangs werden sie zudem eine neue Angriffsfläche für Hacker darstellen. Die Gewährleistung der Informationssicherheit ist eine Grundvoraussetzung für die digitale Verwaltung. Eine angemessene angepasste Informationssicherheit ist vor Aufbau derartiger Systeme somit zwingend sicherzustellen.

§ 15 NDIG stellt klar, dass der gemeinsame Sicherheitsverbund im Landesdatennetz eine Vertrauensstellung zwischen den daran angeschlossenen Behörden erfordert. Daher haben diese für eine angemessene Informationssicherheit innerhalb ihrer Organisation und gegenüber den anderen angeschlossenen Behörden zu sorgen. Auf der Basis von Risikoanalysen sind angemessene technische und organisatorische Maßnahmen zu treffen. Dies hat

nach den Regeln des Informationssicherheitsmanagementsystems zu erfolgen. Den Aufbau und Betrieb des ressortübergreifenden Informationssicherheitsmanagementsystems in der niedersächsischen Landesverwaltung beschreibt die Leitlinie zur Gewährleistung der Informationssicherheit in dem Gemeinsamen Runderlass vom 9. November 2016 (Nds. MBl. S. 1193). Die Leitlinie zur Gewährleistung der Informationssicherheit dient der langfristigen Gewährleistung der Informationssicherheit für die unmittelbare Landesverwaltung.

§ 16 NDIG verpflichtet als weiteren Bestandteil des Informationssicherheitsmanagementsystems zum Betrieb einer Zentralstelle, die fortlaufend ein Informationssicherheitslagebild analysiert und Risikoänderungen erkennt, daraus Hinweise zur Anpassung der Sicherheitsarchitektur entwickelt, in Fragen der Sicherheit in der Informationstechnik berät und bei informationstechnischen Sicherheitsvorfällen unterstützt.

Diese Regelungen erfordern die dauerhafte Bereitstellung von Personalressourcen sowie von notwendiger Hard- und Software. Sie führen zu entsprechenden finanziellen Aufwänden. Diese Aufwände würden allerdings auch ohne das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit entstehen und sind somit keine Kostenfolge dieses Gesetzes. Daher werden sie im Folgenden nur nachrichtlich erwähnt.

Für eine angemessene IT-Sicherheit des Landesdatennetzes sind moderne Sicherheitssysteme unverzichtbar. Daher wird in § 13 Abs. 4 NDIG die das Landesdatennetz bereitstellende Behörde verpflichtet, Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme und Angriffe zu betreiben. Diese Aufgaben werden im Rahmen der Bereitstellung des Landesdatennetzes wahrgenommen. Hierfür stehen bereits Mittel zur Verfügung, zusätzliche Kosten werden nicht erwartet.

Der zweite Abschnitt im dritten Teil (§§ 17 bis 28 NDIG) gibt darüber hinaus auch den Behörden die Ermächtigung, Daten zu erheben und automatisiert auszuwerten. Die Regelungen erweitern die Möglichkeiten zur Verbesserung der Informationssicherheit. Es handelt sich soweit um reine Ermächtigungsnormen, ohne zugleich eine Verpflichtung auszusprechen; insofern verhält sich diese Regelung kostenneutral. Anders ist dies, wenn von den Ermächtigungsnormen Gebrauch gemacht wird. Die Kosten sind insofern abhängig von den eingesetzten Systemen und den dafür benötigten Personal- und Sachkosten. Eine valide Schätzung der Kosten ist nur bei Kenntnis dieser Faktoren möglich, hier aber aufgrund der durch das Gesetz nur eingeräumten Möglichkeiten nicht anzustellen. Die Behörden müssen in eigener Bewertung entscheiden, ob und inwieweit sie aufgrund der herrschenden Cybergefahren eigene Sicherheitssysteme aufbauen wollen oder an den von der das Landesdatennetz betreibenden Behörde betriebenen Sicherheitssystemen teilhaben wollen.

Die Kosten für die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts wurden nicht konkret berechnet. Hier werden Kosten in Höhe von 10 % der Kosten für den kommunalen Bereich erwartet.

Gesamtauflistung der erforderlichen Haushaltsmittel (Sachmittel):

Regelung im Gesetz	Bezeichnung	Projektkosten Land in Euro	Projektkosten Kommunen/sonstige öffentl. Stellen in Euro	jährliche Kosten Land nach Ausbau in Euro	jährliche Kosten Kommunen/sonstige öffentl. Stellen nach Ausbau in Euro	Zugrunde liegende Rechtsverpflichtung
§ 4 Abs. 2	Nutzerkonten	5 000 000	0	400 000	0	§ 3 Abs. 2 OZG
§ 4 Abs. 3	De-Mail	600 000	0	300 000	90 000 /9 000	§ 1 Abs. 1 OZG
§ 5 Abs. 1 und 2	Ausbau BUS	2 000 000	0	200 000	0	§ 1 Abs. 1 OZG
§ 6 Abs. 1 und 2	E-Bezahlverfahren	700 000	1 150 000 /115 000	150 000	200 000 /20 000	§ 1 Abs. 1 OZG
§ 6 Abs. 3	E-Rechnung	5 552 000	5 552 000 /555 000	600 000	600 000 /60 000	EU-Richtlinie 2014/55/EU
§ 5 Abs. 1, 2 und 5 sowie	Formularservice/Online-	20 000 000	0	100 000	0	§ 1 Abs. 1 OZG

Regelung im Gesetz	Bezeichnung	Projektkosten Land in Euro	Projektkosten Kommunen/sonstige öffentl. Stellen in Euro	jährliche Kosten Land nach Ausbau in Euro	jährliche Kosten Kommunen/sonstige öffentl. Stellen nach Ausbau in Euro	Zugrunde liegende Rechtsverpflichtung
§ 12 Abs. 1 Nr. 3	Assistenzsysteme					
§ 5 Abs. 5 und § 12 Abs. 1 Nrn. 4 und 5	NGovOS	5 000 000	0	200 000	0	§ 1 Abs. 1 OZG
	Summe Land	38 852 000		1 950 000		
	Summe Kommunen/ sonstige öffentliche Stellen		6 702 000 /670 000		890 000 /90 000	
§ 10 Abs. 1	E-Akte	5 000 000 (Ausbau OZG-Arbeitsplätze)	0	2 000 000 (Ausbau OZG-Arbeitsplätze)	0	§ 1 Abs. 1 OZG

Betriebsmittel fallen erst ab 2019 oder später an und wachsen dem Ausbau entsprechend an. Projektmittel fallen ab 2019 an und sinken zum Ende des Ausbaus.

Für die von den Kommunen zu tragenden Kosten ist daher folgende Kalkulation in Euro vorgenommen worden:

		2019	2020	2021	2022	2023	2024	2025
Projekt	De-Mail	0	0	0	0	0	0	0
Betrieb		0	0	90 000	90 000	90 000	90 000	90 000
Projekt	Bezahlverfahren	200 000	250 000	250 000	250 000	100 000	100 000	0
Betrieb		0	50 000	50 000	100 000	100 000	200 000	200 000
Projekt[1])	E-Rechnung	2 512 000	1 856 000	1 184 000	0	0	0	0
Betrieb[1])		100 000	200 000	500 000	600 000	600 000	600 000	600 000
Summe		**2 812 000**	**2 356 000**	**2 074 000**	**1 040 000**	**890 000**	**890 000**	**890 000**

Wie oben bereits ausgeführt, sind die Kosten für den Bereich E-Rechnung nicht konnexitätsrelevant, weil sie auf der Richtlinie 2014/55/EU basieren. Die verbleibenden Kosten erreichen nicht die Erheblichkeitsgrenze, sodass keine Ausgleichspflicht besteht.

In der Gesetzesfolgenabschätzung wird der Personalbedarf für die Einhaltung der Verpflichtungen beziffert. Durch das vorliegende Gesetz entstehen darüber hinaus neue Möglichkeiten der Geschäftsprozessoptimierung. Da das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit für die Basisdienste wie elektronische Zugänge, Formulare, Bezahlverfahren und Aktenführung sorgt, lassen sich leichter als vorher Geschäftsprozesse durchgängig elektronisch unterstützen. Um das Optimierungspotenzial voll auszuschöpfen, müssen dann

[1]) Kosten werden durch die Richtlinie 2014/55/EU verursacht.

allerdings oft Fachverfahren angepasst und über standardisierte Schnittstellen mit den Basisdiensten verbunden werden. Auch bietet es sich häufig an, Assistenzsysteme einzurichten, mit denen Bürger leichter und weitgehend fehlerfrei Anträge stellen können als mit einfachen elektronischen Formularen. Diese Optimierungen sind für jedes geeignete Verfahren separat durchzuführen und erfordern einen entsprechenden zusätzlichen Aufwand. Es wäre sehr zu begrüßen, wenn möglichst viele entsprechende Vorhaben zur Optimierung durchgeführt werden. Sie sind aber unabhängig vom vorliegenden Gesetz zu planen und mit einer etatreifen Begründung in die Haushaltsanmeldungen einzubringen. Eine Bezifferung von Personalressourcen oder Sachmittel in der Begründung des Niedersächsischen Gesetzes über digitale Verwaltung und Informationssicherheit erfolgt dagegen nicht.

VI. Beteiligung von Verbänden und sonstigen Stellen

- Apothekerkammer
- Architektenkammer Niedersachsen[2])
- Ärztekammer Niedersachsen[2])
- Bund deutscher Finanzrichterinnen und Finanzrichter
- Bund Deutscher Kriminalbeamter – Landesverband Niedersachsen –
- Bund Deutscher Rechtspfleger e. V.
- Bund Niedersächsischer Sozialrichter
- Bundesverband der Justizwachtmeister e. V.
- Christlicher Gewerkschaftsbund Deutschlands – Landesverband Niedersachsen –
- Deutsche Justiz-Gewerkschaft – Landesverband Niedersachsen e. V. –
- Deutsche Rentenversicherung Braunschweig-Hannover[2])
- Deutsche Rentenversicherung Oldenburg-Bremen
- Deutscher Gewerkschaftsbund Bezirk Niedersachsen-Bremen-Sachsen-Anhalt[2])
- Deutscher Hochschulverband – Landesverband Niedersachsen –[2])
- Deutscher Juristinnenbund e. V. – Niedersächsischer Landesverband –
- Handels- und Dienstleistungsverband Osnabrück-Emsland e. V.
- IHK Niedersachsen[2])
- Ingenieurkammer Niedersachsen[2])
- Kassenärztliche Vereinigung Niedersachsen
- Kassenzahnärztliche Vereinigung Niedersachsen[2])
- Katholisches Büro Niedersachsen[2])
- Kommunaler Arbeitgeberverband Niedersachsen
- Konföderation der evangelischen Kirchen in Niedersachsen[2])
- Landesbeauftragte für den Datenschutz Niedersachsen[2])
- Landesbeauftragte für Menschen mit Behinderungen[2])
- Landesverein der Justizwachtmeister Niedersachsen e. V.
- Landesvertretung der Handwerkskammern Niedersachsen[2])
- Landtag Niedersachsen
- Neue Richtervereinigung e. V. – Landesverband Niedersachsen –
- Niedersächsische AOK
- Niedersächsischer Beamtenbund und Tarifunion[2])
- Niedersächsischer Handwerkstag
- Niedersächsischer Landesrechnungshof

[2]) Stellungnahme wurde abgegeben.

- Niedersächsischer Landkreistag[3])

- Niedersächsischer Richterbund

- Niedersächsischer Städte- und Gemeindebund[3])

- Niedersächsischer Städtetag[3])

- Psychotherapeutenkammer[2])

- Unternehmensverbände Handwerk Niedersachsen

- Unternehmerverbände Niedersachsen e. V.

- Verband der Lebensmittelkontrolleure e. V. LV Niedersachsen

- Verband der niedersächsischen Verwaltungsrichterinnen und Verwaltungsrichter e. V.

- Verband der Rechtspfleger e. V.

- Verband kommunaler Unternehmer e. V.[2])

- Verband Mittelständischer Unternehmer in Deutschland e. V.

- Verband Niedersächsischer Strafvollzugsbediensteter

- Vereinigung der Berufsrichter der Arbeitsgerichtsbarkeit im Lande Niedersachsen

Der Deutsche Verein der Blinden und Sehbehinderten in Studium und Beruf e. V. hat eine Stellungnahme ohne Aufforderung abgegeben. In sechs der insgesamt 18 Stellungnahmen wurden keine Anmerkungen abgegeben oder es wurde auf eine Stellungnahme verzichtet (Deutscher Hochschulverband -Landesverband Niedersachsen-, Kassenzahnärztliche Vereinigung Niedersachsen, Konföderation der evangelischen Kirchen in Niedersachsen, Landesvertretung der Handwerkskammern Niedersachsen, Niedersächsischer Beamtenbund und Tarifunion, Psychotherapeutenkammer).

Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD) hat im Rahmen der Verbandsbeteiligung eine umfassende Überarbeitung zahlreicher Regelungen zu den Eingriffsbefugnissen gefordert, da es die tiefgehenden Eingriffsbefugnisse erforderlich machen, diese mit hinreichender Bestimmtheit und Normklarheit zu regeln und das Verfahren zum Grundrechtseingriff so zu gestalten, dass ein angemessener Schutz für die betroffenen Personen hergestellt wird. Viele Forderungen und Hinweise der LfD zum Datenschutz, zur Ausweitung des Kernbereichs privater Lebensgestaltung und der Benachrichtigungspflicht sowie zur Kontrolle wurden übernommen. Nicht berücksichtigt wurde insbesondere die Forderung eines Richtervorbehalts im Rahmen der Auswertung von Inhaltsdaten beim Einsatz von Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit (§§ 21 ff. NDIG). Ausschlaggebend für die Erforderlichkeit des Richtervorbehalts sei einzig und allein die Tatsache, dass die Datenverarbeitung ohne Kenntnis der Betroffenen und damit verdeckt stattfindet. Die hierzu von der LfD vergleichsweise angeführte Kommentarliteratur (Schenke/Graulich/Ruthig/Buchberger BSIG § 5 Rn. 15) bezieht sich auf die Wiederherstellung des Personenbezugs pseudonymisierter Daten gemäß § 5 Abs. 1 Satz 5 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), die die Anordnung des Präsidenten des Bundesamtes und damit keinen Richtervorbehalt enthält. Weil insoweit personenbezogene Daten gespeichert werden, seien nach der zitierten Fundstelle Zweifel angebracht, ob verfassungsrechtlich nicht sogar eine richterliche Entscheidung erforderlich sei analog einem Eingriff durch Telefonüberwachung, zumal die Verwendung personenbezogener Daten nach Absatz 3 ebenfalls keiner richterlichen Entscheidung bedürfe (Schenke/Graulich/Ruthig/Buchberger BSIG § 5 Rn. 15). Die Zweifel werden nicht geteilt. Die Zielrichtung und Eingriffsintensität der Maßnahme erfordern nicht zwingend einen Richtervorbehalt. Besonders das komplexe Stufenmodell, die strenge Zweckbindung, die grundsätzlich automatisierte Datenverarbeitung, der verfolgte Grundsatz der Datenminimierung und die Kontrollmaßnahmen führen zu einer grundrechtsschonenden Umsetzung und letztlich zur Angemessenheit und Verhältnismäßigkeit des Gesetzes. Hinzu kommt, dass Angriffe aus dem Cyberraum eine schnelle Reaktion erfordern, sehr hohe Fallzahlen erwartet werden und eine juristische Spezialisierung auf das Themengebiet erforderlich erscheint. Vergleichbare Eingriffsregelungen in § 5 BSIG und § 16 des Bayerischen E-Government-Gesetzes (BayEGovG) sehen ebenfalls keinen Richtervorbehalt vor.

Zudem kritisiert die LfD auch die Technikneutralität der Vorschriften. Diese ist jedoch erforderlich, um schnell auf neue Bedrohungslagen reagieren zu können. Aufgrund der hohen Flexibilität der Angriffsmöglichkeiten und der schnellen Entwicklung neuer Angriffsmethoden bedarf es einer gesetzlichen Grundlage, mit der auf diese Anforderungen reagiert werden kann.

Die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens schätzt, dass die Digitalisierung des kommunalen Bereichs mit erheblichen Kosten verbunden sein wird. Dabei bezieht sie sich auf Teil A des Hand-

[3]) Eine gemeinsame Stellungnahme wurde durch die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsen abgegeben.

lungsplans „Digitale Verwaltung und Justiz“ („OZG-Handlungsplan“) des Niedersächsischen Ministeriums für Inneres und Sport. Sie halten eine Beteiligung des Landes an der Finanzierung für erforderlich. Die Landesregierung erwartet ebenfalls hohe Kosten im kommunalen Bereich und plant Schritte zur finanziellen Unterstützung der Kommunen bei der Umsetzung des „OZG-Handlungsplans“. Größere Änderungen am Gesetz zur Vermeidung finanzieller Belastungen fordern die kommunalen Spitzenverbände nicht. Auch führen sie keine konkreten Regelungen des Niedersächsischen Gesetzes über digitale Verwaltung und Informationssicherheit auf, die zu übermäßigen finanziellen Belastungen führen würden.

Die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens weist auf den Geltungsbereich des Onlinezugangsgesetzes hin und sieht hier einen Dissens mit der Gesetzesbegründung. Der Anwendungsbereich des Onlinezugangsgesetzes wird aus Ihrer Sicht so verstanden, dass es die Kommunen nur für den Vollzug von Bundesgesetzen direkt verpflichtet. Da der Bund den Ländern unmittelbar keine Aufgaben zuweisen darf, können Bundesgesetze nur im Rahmen einer landesrechtlichen Aufgabenübertragung vollzogen werden. In einem solchen Fall müssten auch die notwendigen Mittel durch das Land gemäß Artikel 57 Abs. 4 der Niedersächsischen Verfassung bereitgestellt werden. Der Anwendungsbereich des Onlinezugangsgesetzes befindet sich aktuell in der Diskussion und ist umstritten. Mehrere Länder vertreten hierzu die Auffassung einer direkten Verpflichtung der Kommunen durch das Onlinezugangsgesetz. Mit dem Bundesministerium für Inneres, Bau und Heimat (BMI) laufen derzeit Gespräche, in denen die jeweiligen Positionen sondiert werden. Je nach Ausgang dieser Gespräche wird gegebenenfalls eine Neubewertung notwendig sein. Die bei den Kommunen durch dieses Gesetz veranlassten Kosten sind so gering, dass sie die Erheblichkeitsschwelle nicht erreichen. Dies gilt unabhängig davon, ob das Onlinezugangsgesetz für die Kommunen gilt oder nicht.

Die Landesarbeitsgemeinschaft Industrie- und Handelskammer Niedersachsen betont, dass es zu einer systematischen und einheitlichen Umsetzung des Onlinezugangsgesetzes insbesondere bei dem Nutzerkonto kommen muss. Die Infrastruktur muss so geplant und eingerichtet werden, dass eine verlässliche Erreichbarkeit gegeben ist. Bis dahin muss eine Einreichung auf klassischem Wege erhalten bleiben. Bestehende und geplante IT-Lösungen müssen vollumfänglich unterstützt werden und eine hohe Kompatibilität zu Systemen des Bundes muss gewährleistet werden. Dies ist in Niedersachsen auch beabsichtigt.

Aufgrund ihrer teilweise selbstverwaltenden Tätigkeit und der Finanzierung über Mitgliedsbeiträge fordern die Architektenkammer, die Landesvertretung der Handwerkskammern Niedersachsen, die Landesarbeitsgemeinschaft Industrie- und Handelskammer Niedersachsen und die Ingenieurkammer eine Ausnahme vom Geltungsbereich. Hingegen wird der Einbezug von der Ärztekammer begrüßt. Durch eine Herausnahme aus dem Geltungsbereich würde das gemeinsame Online-Angebot für Bürgerinnen, Bürger, Unternehmen und Verbände reduziert, was zu wenig Verständnis führen würde. Ohnehin ist davon auszugehen, dass die Kammern, soweit sie Aufgaben des Landes wahrnehmen, das Onlinezugangsgesetz berücksichtigen müssen. Da auch den Kammern Basisdienste zur Verfügung gestellt werden und deren Umfang an Verwaltungsleistungen begrenzt ist, bleibt die Belastung der Kammern durch das Gesetz gering. Der Geltungsbereich wurde daher nicht verändert.

Der Deutsche Verein der Blinden und Sehbehinderten (DVBS) sowie die Landesbeauftragte für Menschen mit Behinderungen fordern einen stärkeren und verpflichtenden Einbezug der Barrierefreiheit in den Gesetzesentwurf, der im Entwurf gegebene Verweis einer Umsetzung durch das geplante Niedersächsische Behindertengleichstellungsgesetz (NBGG) sei nicht ausreichend. Insbesondere Kommunikation, Dokumente, aber auch Basisdienste, vor allem die elektronische Akte, müssten barrierefrei ausgestaltet werden.

Die Barrierefreiheit stellt einen wesentlichen Aspekt bei der Neugestaltung der digitalen Landschaft dar. Mit dem geplanten Niedersächsischen Behindertengleichstellungsgesetz und der darin enthaltenen Umsetzung der Richtlinie (EU) 2016/2102 werden bereits wesentliche Aspekte gesetzlich geregelt, die auch in diesem Gesetz berücksichtigt werden müssen. So sind gemäß § 9 a Abs. 1 Satz 1 NBGG Webseiten und mobile Anwendungen, einschließlich der für die Beschäftigten bestimmten Angebote im Intranet, barrierefrei zu gestalten. Dies gilt auch für die dort abrufbaren Formulare nach § 5 Abs. 2. Die bereitzustellenden Informationen nach § 5 Abs. 1 und 2 werden voraussichtlich ebenfalls über Webseiten und mobile Anwendungen zu veröffentlichen sein, weshalb auch hier bereits das Niedersächsische Behindertengleichstellungsgesetz zu berücksichtigen sein wird. Ebenso werden voraussichtlich viele weitere Anwendungen mithilfe von Webseiten umzusetzen sein.

Wenn eine Regelungslücke besteht, sollen die übrigen Systeme – soweit technisch möglich – natürlich ebenfalls barrierefrei ausgestaltet werden. Soweit hierfür eine zusätzliche Regelung für erforderlich gehalten wird, sollte diese im Niedersächsischen Behindertengleichstellungsgesetz erfolgen. Hierdurch würde eine Zersplitterung der Regelungen vermieden. Inwieweit hier eine Regelungslücke besteht, ist aktuell nicht absehbar.

Zu Artikel 2 des Entwurfs enthielten die Stellungnahmen folgende Aussage:

Der Deutsche Gewerkschaftsbund lehnt die Beauftragung nicht öffentlicher Stellen für die Auftragsverarbeitung ab und fordert, dass nur öffentliche Stellen die Digitalisierung übernehmen dürfen. Dieser Forderung kann nicht gefolgt werden. Die Digitalisierung der Verwaltung ist nur mit erheblichen personellen Ressourcen zu bewältigen, sodass auch die Beauftragung nicht öffentlicher Stellen unabdingbar ist.

Die LfD begrüßt die aufgrund ihrer Empfehlungen zu § 92 a Abs. 1 NBG vorgenommen Umformulierungen sowie die getroffene Regelung zur Kontrolle hinsichtlich der Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den Auftraggeber.

Sie schlägt vor, dass die Beauftragung nicht öffentlicher Stellen nur erfolgen darf, wenn weder die eigene noch andere öffentliche Stellen die Aufgabe vergleichbar wahrnehmen können. Diese Beschränkung wird als zu weitgehend betrachtet und im Hinblick auf die Aufgabenerfüllung bei der Digitalisierung als nicht sinnvoll angesehen. Insbesondere werden die Beschränkungen in § 92 a Abs. 3 NBG als ausreichend angesehen.

Darüber hinaus bemängelt die LfD, dass nach dem Gesetzestext unklar sei, wann ein Geschäftsablauf als gestört betrachtet werden kann. Eine Störung des Geschäftsablaufs dürfte eintreten, wenn die Aufgaben der personalverwaltenden Behörde aufgrund des mit der Digitalisierung verbundenen erheblichen Personaleinsatzes nicht mehr ordnungsgemäß wahrgenommen werden können. Es kommt dabei nicht auf einen Vergleich mit der alten Rechtslage an, vielmehr hat ein Vergleich der Geschäftsgänge mit bzw. ohne Beauftragung einer nicht öffentlichen Stelle als Auftragsverarbeiter stattzufinden.

Der von der LfD weiterhin als wesentlich angesehene Notfallplan bei der Beauftragung von nicht öffentlichen Stellen wird nicht als zwingend erforderlich erachtet. Die Verantwortlichkeit der Datenverarbeitung und Aufgabenerfüllung verbleibt bei der personalverwaltenden Behörde. Sie hat die notwendigen Vorkehrungen zu treffen, damit im Fall einer eventuellen Insolvenz einer beauftragten nicht öffentlichen Stelle die Aufgabenwahrnehmung gewährleistet ist. Zu diesem Zweck kann es sich empfehlen, einen Notfallplan aufzustellen.

Die Ansicht der LfD, dass § 107 Abs. 6 Satz 2 des Niedersächsischen Kommunalverfassungsgesetzes (NKomVG) gegenüber § 92 a NBG spezifischer ist und diesen insoweit verdrängt, wird nicht gefolgt. Bei der Aufgabenübertragung in § 107 Abs. 6 Satz 2 NKomVG handelt es sich um eine Delegation, mit der die Aufgabe als eigene übertragen werden kann. Dies führt zu einer geänderten Zuständigkeit und Verantwortlichkeit. Demgegenüber sieht § 92 a NBG die Aufgabenübertragung nur im Sinne eines Mandats vor. Zuständigkeit und Verantwortlichkeit verbleiben bei der personalverwaltenden Behörde. Da § 107 Abs. 6 Satz 2 NKomVG damit gegenüber § 92 a NBG nicht als speziellere Norm betrachtet werden kann, ist eine Einschränkung des Anwendungsbereichs des § 92 a Abs. 3 NBG nicht gegeben.

Entgegen der Auffassung der Arbeitsgemeinschaft der Kommunalen Spitzenverbände wird die Notwendigkeit einer weiteren Öffnung der Regelung in § 92 a Abs. 3 NBG nicht gesehen. Die Regelung stellt lediglich geringfügige rechtliche Anforderung an die Beauftragung einer nicht öffentlichen Stelle. Wenn diese nicht erfüllt sind, stellt sich die Beauftragung einer nicht öffentlichen Stelle als nicht zielführend dar. Soweit etwa die Digitalisierung von Personalakten – wie von der Arbeitsgemeinschaft der Kommunalen Spitzenverbände vorgetragen – durch die Verwaltungen selbst in aller Regel nur mit unverhältnismäßig hohen und zumeist nicht verfügbaren Personalressourcen realisierbar ist, dürfte darin bereits eine Störung des Geschäftsablaufs liegen, die dazu berechtigt, einen privaten Dienstleister mit der Verarbeitung zu beauftragen.

Auf die weiteren vorgetragenen Anmerkungen der Verbände wird in den Ausführungen im besonderen Teil der Begründung des Gesetzentwurfs eingegangen.

B. Besonderer Teil

Zu Artikel 1 (Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit):

Vorbemerkung:

Gesetzliche Regelungen zum E-Government wurden bereits auf Bundesebene durch das E-Government-Gesetz sowie durch entsprechende Ländergesetze in Baden-Württemberg, Bayern, Berlin, Bremen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Saarland, Sachsen, Schleswig-Holstein und in Thüringen erlassen. Entwürfe für Regelungen zur elektronischen Verwaltung liegen aus Brandenburg, Hessen und Sachsen-Anhalt vor. Das vorliegende Gesetz und seine Begründung orientieren sich am Bundesgesetz und seiner Begründung, sofern keine landesspezifischen Besonderheiten zu beachten sind. Grund dafür ist das Bestreben, möglichst einheitliche Regelungen im Bundesgebiet zu schaffen, da das Bundesgesetz erkennbar auch bei anderen Landesgesetzen Pate stand. Eine Rechtszersplitterung kann damit weitestgehend vermieden werden. Im Übrigen sind die Regelungen sowie die Begründung an das in Baden-Württemberg geltende Gesetz angelehnt, sowie teilweise an Regelungen der anderen oben genannten Bundesländer, um einen möglichst hohen Gleichklang der gesetzlichen Regelungen zu erreichen.

Zum Ersten Teil (Allgemeines):

Zu § 1 (Begriffsbestimmungen):

§ 1 enthält Begriffsbestimmungen, um eine einheitliche Auslegung der Begriffe zu gewährleisten und zur Vermeidung von Wiederholungen im Gesetzestext. Des Weiteren dient diese Vorschrift zur Erläuterung von Rechtsbegriffen, die für das Verständnis der Paragrafen und zur Anwendung dieses Gesetzes erforderlich sind.

Die Erläuterung des Behördenbegriffs dient ausschließlich der Klarstellung und entspricht § 1 Abs. 4 des Niedersächsischen Verwaltungsverfahrensgesetzes (NVwVfG).

Im Gesetz wird der Begriff Informationstechnik (IT) verwendet als jedes technische Mittel zur elektronischen Verarbeitung oder Übertragung von Informationen. Dieser Begriff entspricht dem heutigen Sprachgebrauch. Der Definition entsprechend umfasst der Begriff auch technische Mittel zur Übertragung von Informationen, also auch die Kommunikationstechnik.

Die Definition der besonderen Kategorien personenbezogener Daten wurde aus Artikel 9 Abs. 1 der Datenschutz-Grundverordnung (im Folgenden: DSGVO) wortgleich übernommen und ist ebenso auszulegen.

Als Definition der digitalen Verwaltung wird die „Speyerer Definition“ des E-Government von Reinermann/Lucke 2002 zugrunde gelegt, die Electronic Government als „die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mithilfe von Informations- und Kommunikationstechniken über elektronische Medien“ bezeichnet. Der Begriff „digitale Verwaltung“ und die leicht geänderte Definition werden verwendet, um dem heute üblichen Wortlaut in Fachkreisen und Politik zu entsprechen. Im Übrigen wird im Gesetz weiterhin der Begriff „elektronisch“ statt „digital“ genutzt, weil dieser in einigen Definitionen (z. B. E-Mail, E-Akte) weiter stark verbreitet ist und eine Abänderung zu Irritationen führen würde.

Die Definition für das Landesdatennetz bestimmt dieses als eine elektronische Kommunikation, die zwischen den damit verbundenen lokalen Netzen der Behörden sowie damit verbundenen Netzen anderer Verwaltungen ermöglicht und durch das Land oder im Auftrag des Landes betrieben wird. Die lokalen Netzwerke der Behörden gehören nach dieser Definition nicht zum Landesdatennetz. Auch die Netzwerke der Landkreise und kommunalen Datenzentralen, die als eigene Netze dieser Organisationen betrieben werden und über einen Übergabepunkt an das Landesdatennetz angeschlossen sind, gehören nicht zum Landesdatennetz. Sie sind aber in vielen Fällen gemäß Absatz 2 mit dem Landesdatennetz verbunden. Das Landesdatennetz dient damit als gemeinsames Netz der Übertragung von Daten in Schriftform, technischen Informationen und Programmteilen sowie der Übermittlung von Sprach- und Videodaten im Rahmen der Telefonie und sonstiger Nutzung. Nicht verbunden mit dem Landesdatennetz sind IT-Systeme, die nur über das Internet erreichbar sind. Netze von Verwaltungen außerhalb Niedersachsens einschließlich des Verbindungsnetzes zwischen den Landesdatennetzen sind im Sinne dieses Gesetzes nicht mit dem Landesdatennetz verbunden.

Die Definition der elektronischen Rechnung wurde aus Artikel 2 Abs. 1 der Richtlinie 2014/55/EU übernommen.

Die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens erbittet eine Legaldefinition des Begriffs „Gefahrenabwehr“ oder zumindest eine Verweisung auf das Polizeirecht. Dies wird als entbehrlich angesehen. Im Rahmen der Verbandsbeteiligung wurde durch die Bezugnahme mehrerer Stellungnahmen deutlich, dass die Herleitung des Begriffs ausreichend verdeutlicht wurde. Einer weiteren Klarstellung bedarf es somit nicht.

Zu § 2 (Der oder die IT-Bevollmächtigte der Landesregierung):

Der zunehmende Einsatz der IT auf dem Weg in die digitale Verwaltung erfordert ein besonders hohes und weiter wachsendes Maß an ressortübergreifender Koordination. Auch bedarf es einer intensiven Abstimmung mit dem Bund und den anderen Ländern, etwa im Rahmen des IT-Planungsrats Bund/Länder. Zu diesem Zweck hat die Landesregierung die Position einer oder eines IT-Bevollmächtigten der Landesregierung auf Staatssekretärsebene

eingerichtet. Die Position wurde erstmalig zum 1. Januar 2006 mittels Kabinettsbeschluss geschaffen und besetzt. Sie oder er wird auch als „Chief Information Officer“ oder kurz „CIO“ bezeichnet. Aufgrund der besonderen Bedeutung der Position wird diese nunmehr gesetzlich geregelt. Sie oder er soll den IT-Einsatz im Land gestalten und die Fortentwicklung der digitalen Verwaltung steuern. Zudem sind Veränderungsprozesse zur Digitalisierung und die Einführung entsprechender Verfahren zuerst organisatorisch zu betrachten und gegebenenfalls zu optimieren, um sie anschließend zu digitalisieren. Die Regelung ist auch deshalb erforderlich, weil dem oder der IT-Bevollmächtigten in diesem Gesetz bestimmte Aufgaben zugeordnet werden. Bei diesen Aufgaben gilt es insbesondere, eine Zersplitterung der IT-Strukturen sowie eine einheitliche Umsetzung zu vermeiden. Hierzu sollen ihr oder ihm umfassende Rechte gegenüber Behörden des Landes eingeräumt werden.

Die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens erbittet, von Anfang an in die Planung und Entwicklung der digitalen Verwaltung durch die IT-Bevollmächtigte oder den IT-Bevollmächtigten einbezogen zu werden, und fordert eine gesetzliche Verankerung. Im Rahmen der vertrauensvollen Zusammenarbeit ist eine Beteiligung der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens geplant. Eine gesetzliche Regelung hierzu erscheint jedoch entbehrlich.

Zum Zweiten Teil (Digitale Verwaltung):

Zu § 3 (Geltungsbereich):

Zu Absatz 1:

Absatz 1 Satz 1 regelt den Geltungsbereich des Zweiten Teils für Behörden des Landes, für die Kommunen und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Zu den Behörden des Landes gehören insbesondere alle obersten Landesbehörden sowie deren nachgeordnete Behörden, mithin die unmittelbare Landesverwaltung. Die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sind Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Diese werden vom Geltungsbereich dieses Teils des Gesetzes erfasst, jedoch unterliegen sie nicht den erhöhten Verpflichtungen, die dieser Teil des Gesetzes für die Behörden des Landes vorsieht. Die Formulierung orientiert sich an § 1 Abs. 1 NVwVfG. Der Behördenbegriff wird in § 1 Nr. 3 definiert und ist identisch mit § 1 Abs. 4 NVwVfG.

Eine Herausnahme der Kammern aus dem Teil des Gesetzes konnte grundsätzlich nicht erfolgen, da diese wichtige Verwaltungsaufgaben wahrnehmen und häufig der direkte Kontakt zu den Bürgerinnen und Bürgern besteht. Sie stellen damit in etlichen Verfahren die Schnittstelle zu den Bürgerinnen und Bürgern dar, sodass eine Herausnahme der Kammern in einem E-Government-Gesetz schwere Nachteile mit sich bringen würde. Gerade hier sind die Informationspflichten besonders wichtig und die Zugänge häufig genutzt. Eine Herausnahme würde daher auch eine Entwertung dieses Teils des Gesetzes und seines Zwecks bedeuten. Deutlich wird dies auch an den anderen E-Government-Gesetzen, die bereits in Kraft sind. Dabei wurden die Kammern nur in wenigen Einzelfällen ausgenommen, nicht aber in Gänze.

In diesem Teil des Gesetzes sind Regelungen aufgeführt, die einen Eingriff in die kommunale Selbstverwaltung bedeuten. So wird geregelt, welche elektronischen Zugänge zu eröffnen sind. Außerdem ist die Bereitstellung von Informationen und Verwaltungsleistungen über ein niedersächsisches Verwaltungsportal vorgeschrieben. Zur Umsetzung dieser Verpflichtungen ist teilweise die Nutzung von gemeinsamen Basisdiensten vorgegeben. Nur durch diese Verpflichtungen kann sichergestellt werden, dass Bürgerinnen, Bürgern, Unternehmen und Verbänden Online-Dienste nach einheitlichen oder zumindest ähnlichen Standards angeboten werden, was für eine Akzeptanz dieser Angebote unerlässlich ist. Außerdem sind diese Verpflichtungen erforderlich, um die vom Onlinezugangsgesetz vorgegebene Verknüpfung mit dem Portalverbund zu realisieren. Die Regelungen, insbesondere die Verpflichtung zur Nutzung bestimmter Basisdienste, ermöglichen es zudem, die digitale Verwaltung so kostensparend wie möglich einzuführen. Aufwändige IT-Systeme müssen nur einmal entwickelt und bereitgestellt werden. Sie stehen dann den Behörden des Landes und allen Kommunen zur Verfügung.

Die Eingriffe in die kommunale Selbstverwaltung wurden auf das erforderliche Maß beschränkt. So werden den Kommunen Basisdienste nur vorgeschrieben, wenn dies zum Erreichen der aufgeführten Ziele erforderlich ist. Im Übrigen steht es ihnen frei, die vom Land bereitzustellenden Dienste zu nutzen oder eigene zu verwenden. Auch gibt es keine Regelungen, die in die behördeninternen Abläufe durch Vorgaben eingreifen. Zum Beispiel beschränken sich die Verpflichtungen zur elektronischen Aktenführung auf die Behörden des Landes. Ebenso werden keine Vorgaben in Hinblick auf die Ablauf- oder Aufbauorganisation im kommunalen Bereich getroffen. Auch eine Änderung der Aufgabenbereiche erfolgt nicht.

Dieser Teil gilt ausschließlich für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden. Der Begriff wird wortgleich verwendet wie im Niedersächsischen Verwaltungsverfahrensgesetz. Fiskalisches oder privatrechtliches Handeln ist somit vom Anwendungsbereich nicht erfasst. Die Einbeziehung der Fiskalverwaltung und des privatrechtlichen Handelns wird auch ohne Verpflichtung erwartet. Synergieeffekte sind nur denkbar, wenn alle Formen des Handelns einbezogen sind. Die Einbeziehung der Kommunen war erforderlich, da diese das Gros an Verwaltungsaufgaben tragen und die durch diesen Teil des Gesetzes initiierten Vereinfachungen gerade in dem Zusammenwirken mit den Kommunen zum Tragen kommen. Eine Ausnahme für den kommunalen Bereich wäre daher wenig sinnvoll, insbesondere würde es den Austausch zwischen den Kommunen deutlich erschweren. Die Rechtsetzung

(Rechtsverordnungen, Satzungen und Verwaltungsvorschriften) durch die Exekutive ist auch erfasst, da es sich ebenso um eine Verwaltungsaufgabe handelt (so zum Bundesrecht: Schoch, Informationsfreiheitsgesetz, 2009, § 1 Randnummer 86; Ziekow, Verwaltungsverfahrensgesetz, 3. Auflage 2013, § 29 Randnummer 31).

Dieser Teil des Gesetzes umfasst die Verwaltungstätigkeit und beschränkt diese nicht auf das Handeln mit Außenwirkung, sodass auch die behördeninterne Verwaltungstätigkeit von dem Geltungsbereich erfasst ist. Auch der Landesrechnungshof und seine nachgeordneten Prüfungsämter unterfallen diesem Teil des Gesetzes als eine Behörde des Landes, soweit diese als Verwaltungsbehörde tätig wird. Übt der Landesrechnungshof keine Verwaltungstätigkeit aus, etwa wenn er als Organ der externen Finanzkontrolle tätig wird, so ist dieser Teil des Gesetzes nicht anwendbar. Auch für die Gerichte findet dieser Teil des Gesetzes keine Anwendung, soweit sie als Judikative tätig werden, da sie in diesen Fällen keine Verwaltungstätigkeit ausüben.

Ebenso ist die Verwaltungstätigkeit des Landtags und der oder des LfD erfasst. Sie sind insoweit Behörden des Landes.

Auf juristische Personen des bürgerlichen Rechts ist der Teil des Gesetzes im Grundsatz nicht anwendbar, da sie keine Verwaltungstätigkeit ausüben. Anders ist dies jedoch bei Beliehenen, wie z. B. öffentlich bestellten Vermessungsingenieurinnen und Vermessungsingenieuren, sofern sie hoheitliche Tätigkeiten wahrnehmen. Notarinnen und Notare sind dagegen nicht vom Geltungsbereich dieses Teils des Gesetzes umfasst, da sie rechtspflegerisch tätig werden und somit keine Verwaltungstätigkeit ausüben.

Gemäß Absatz 1 gilt das Gesetz, soweit besondere Rechtsvorschriften des Landes keine inhaltsgleichen oder entgegenstehenden Bestimmungen enthalten. Hierdurch wird deutlich, dass dieser Teil des Gesetzes grundsätzlich ein lex generalis ist. Spezialgesetzliche Regelungen werden vom vorliegenden Teil des Gesetzes nicht berührt. Dieser wird vielmehr von diesen spezielleren, den besonderen, Vorschriften verdrängt.

Das Niedersächsische Verwaltungsverfahrensgesetz wird von diesem Teil des Gesetzes bei inhaltsgleichen oder entgegenstehenden Bestimmungen verdrängt, da es als allgemeines Gesetz nicht vorgeht. Das Niedersächsische Verwaltungsverfahrensgesetz gilt jedoch dann uneingeschränkt, wenn Behörden vom Anwendungsbereich dieses Teils des Gesetzes ausgenommen sind.

Dieser Teil des Gesetzes wird vom Fachrecht verdrängt, wenn das Fachrecht inhaltsgleiche, also gleichlautende, Regelungen enthält, aber auch dann, wenn entgegenstehende Vorschriften vorhanden sind. Dies ist unter anderem dann der Fall, wenn das Fachrecht die Anwendung dieses Teils des Gesetzes ausschließt, es abweichende Regelungen oder abschließende weitergehende Regelungen enthält. Dies gilt auch für geringfügige Abweichungen.

Dieser Teil des Gesetzes ist nicht auf das Wahlrecht anwendbar. Wahlorgane (Wahlleitungen, Wahlausschüsse und Wahlvorstände) sind keine Behörden, die öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen.

Auch die Innungen und Kreishandwerkerschaften, z. B. die Handwerksinnungen, sind von diesem Teil des Gesetzes nicht erfasst. Sie sind zwar Körperschaften des öffentlichen Rechts, unterliegen aber nicht der Aufsicht des Landes, sondern der Aufsicht der Handwerkskammern.

Zudem weist die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens in ihrer Stellungnahme darauf hin, dass es insbesondere bei Samtgemeinden zu Umsetzungsproblemen kommen kann, da meist nur diese über einen Internetauftritt verfügen. Es kommt maßgeblich darauf an, dass die Informationen im Internet abrufbar sind. Nach dem Recht der interkommunalen Zusammenarbeit sowie im Verhältnis der Mitgliedsgemeinden zu Samtgemeinden können gemäß § 98 Abs. 1 Satz 2 NKomVG Aufgaben mit entlastender Wirkung auf die Samtgemeinden übertragen werden. Eine Wahrnehmung ist insoweit auch weiterhin durch die Samtgemeinde möglich und es bedarf grundsätzlich keines eigenen Internetauftritts der Mitgliedsgemeinden.

Zu Absatz 2:

In Absatz 2 wird festgelegt, für welche Bereiche der Zweite Teil keine Anwendung findet. Danach gilt er nicht für die staatlichen Hochschulen und die nicht an das Landesdatennetz angeschlossenen, mit Forschungsaufgaben betrauten Dienststellen in IT-Betreuung der Hochschulen, um den Besonderheiten von Forschung und Lehre gerecht zu werden. Ebenso sind die von den Hochschulen gemäß den Vereinbarungen mit dem Kultusministerium geführten Kompetenzzentren für die Lehrkräftefortbildung ausgenommen. Dies gilt auch für die sonstigen Forschungseinrichtungen, die nicht an das Landesdatennetz angeschlossen sind. Darunter fallen z. B. die Materialprüfungsanstalten, die organisatorisch und technisch eng mit den Universitäten verbunden sind und auch keine zentralen Dienste des IT.Niedersachsen nutzen.

Zudem sind die Vorschriften dieses Teils in Anlehnung an § 2 Abs. 1 NVwVfG nicht anwendbar für die Tätigkeit der Kirchen, der Religionsgesellschaften und Weltanschauungsgemeinschaften sowie ihrer Verbände und Einrichtungen.

Die öffentlich-rechtlichen Kreditinstitute und öffentlich-rechtlichen Versicherungsanstalten wurden ebenfalls aus dem Geltungsbereich herausgenommen. Hierzu gehört zum einen die „Norddeutsche Landesbank – Girozentrale“, da sie von den beiden Ländern Niedersachsen und Sachsen-Anhalt getragen wird und damit sonst mehrere Landesgesetze Anwendung finden würden. Zum anderen sind die niedersächsischen Sparkassen auszunehmen,

da für diese bereits bundesrechtliche Sonderregelungen zu den IT-Anforderungen bestehen. Die übrigen öffentlich-rechtlichen Kreditinstitute und öffentlich-rechtlichen Versicherungsanstalten stehen in einem Wettbewerb zu privatrechtlich organisierten Banken und Versicherungen und sind in erster Linie unternehmerisch tätig.

Der Teil findet keine Anwendung auf die der Rechtsaufsicht des Ministeriums für Soziales, Gesundheit und Gleichstellung unterstehenden landesunmittelbaren Körperschaften der gesetzlichen Kranken-, Renten- und Unfallversicherung sowie der sozialen Pflegeversicherung. Dies betrifft folgende landesunmittelbare Körperschaften: AOK-Die Gesundheitskassen für Niedersachsen, Pflegekasse bei der AOK - Die Gesundheitskasse für Niedersachsen, BKK EWE, BKK Pflegekasse der BKK EWE, BKK Public, Pflegekasse BKK Public, BKK Landesverband Mitte, Kassenärztliche Vereinigung Niedersachsen, Kassenzahnärztliche Vereinigung Niedersachsen, Medizinischer Dienst der Krankenversicherung Niedersachsen, Gemeinde-Unfallversicherungsverband Hannover, Braunschweigischer Gemeinde-Unfallversicherungsverband, Gemeinde-Unfallversicherungsverband Oldenburg, Feuerwehr-Unfallkasse Niedersachsen, Landesunfallkasse Niedersachsen, Deutsche Rentenversicherung Oldenburg-Bremen und Deutsche Rentenversicherung Braunschweig-Hannover.

Ferner gilt der Teil des Gesetzes nicht für Beliehene, um Abgrenzungsschwierigkeiten zwischen dem hoheitlichen und dem privatrechtlichen Handeln zu vermeiden. Auch der Norddeutsche Rundfunk als Landesrundfunkanstalt der Freien und Hansestadt Hamburg und der Länder Niedersachsen, Mecklenburg-Vorpommern und Schleswig-Holstein soll vom Anwendungsbereich ausgenommen sein, um dessen besonderer Stellung, insbesondere hinsichtlich der Trägerschaft, gerecht zu werden. Die Erwähnung in diesem Teil des Gesetzes dient der Klarstellung, er ist aber ohnehin ausgenommen, weil er den Hauptsitz in Hamburg hat und somit die Gesetze Hamburgs ausschlaggebend sind. Auch die Niedersächsische Landesmedienanstalt fällt nicht in den Geltungsbereich, da sie bei verfassungsrechtlicher Betrachtung so gravierende Übereinstimmungen in Stellung und Funktion mit dem NDR aufweist, dass eine Herausnahme angezeigt ist. Die Nordwestdeutsche Forstliche Versuchsanstalt als Behörde, die von den Ländern Niedersachsen, Hessen, Sachsen-Anhalt und Schleswig-Holstein durch Staatsvertrag gegründet wurde, ist ebenfalls vom Geltungsbereich ausgenommen, da sie aufgrund ihrer Struktur und Organisation einen besonderen Status hat, der zu berücksichtigen ist. Weiterhin wurden die Schulen aus dem Geltungsbereich herausgenommen, um deren besonderer Stellung und den Anforderungen an diese Behörden gerecht zu werden. Erfasst sind von dieser Ausnahme die öffentlichen Schulen und die Schulen in freier Trägerschaft sowie die Schulen, für die das Niedersächsische Gesetz über Schulen für Gesundheitsfachberufe und Einrichtungen für die praktische Ausbildung gilt. Zum Schulbereich der Landesbildungszentren zählen auch die angeschlossenen weiteren pädagogischen Bereiche, soweit sie nicht über einen Zugang zum Landesdatennetz verfügen. Sie werden daher ebenfalls ausgenommen.

Die Architektenkammer fordert in ihrer Stellungnahme, dass sie entweder keine Nutzerkonten einführen muss oder das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit sich lediglich auf Behörden mit mehr als 50 Mitarbeiterinnnen und Mitarbeitern beschränkt. Auch die Ingenieurkammer Niedersachsen erbittet eine Ausnahme vom Anwendungsbereich des Gesetzes, da sie in weiten Teilen keine Pflichtkammer wie viele andere Kammern ist. Durch eine Herausnahme aus dem Geltungsbereich würde das gemeinsame Online-Angebot für Bürgerinnen, Bürger, Unternehmen und Verbände reduziert, was zu wenig Verständnis führen würde. Bei den Nutzerkonten handelt es sich um ein Kernelement aus § 3 OZG, mit dem sich Nutzer für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können. Eine Begrenzung ist nicht vorgesehen. Somit bleibt die Nutzung eines Nutzerkontos beim Anbieten von Verwaltungsleistungen verpflichtend. Da auch den Kammern der Basisdienst zum Nutzerkonto bereitgestellt wird, ist der Aufwand für die Einführung und den Betrieb gering.

Der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens erscheinen die Ausnahmen vom Geltungsbereich unverständlich. So sollten gerade die Schulen einbezogen werden, um viele Serviceleistungen auch digital erbringen zu können und Einsparungen herbeizuführen. Auch sollte ein Abgleich mit Teil A des Handlungsplans „Digitale Verwaltung und Justiz“ („OZG-Handlungsplan“) erfolgen. Die Digitalisierung bedarf einer schrittweisen Umstellung. Um die Verwaltungen nicht zu überfordern, wurden zunächst verschiedene Bereiche vom Geltungsbereich des Gesetzes ausgenommen. Diese sollen jedoch auch zeitnah digitalisiert werden.

Zu Absatz 3:

Hinsichtlich der Nummern 1 bis 10 des Absatzes 3 gilt nur die Regelung zum Austausch von Dokumenten in § 10 Abs. 4, da diese im Hinblick auf die Umstellung auf den elektronischen Rechtsverkehr notwendig ist.

Nummer 1 legt fest, dass für das Justizministerium und seinen Geschäftsbereich lediglich § 10 Abs. 4 gilt, sofern nicht ein Bereich überhaupt nicht vom Geltungsbereich des Zweiten Teils erfasst ist oder nicht bereits eine noch weitergehende Ausnahme in Absatz 2 vorgesehen ist. Hierdurch sollen Doppelstrukturen vermieden werden. Zudem wird hiermit der besonderen verfassungsrechtlichen Form und der institutionellen Unabhängigkeit Rechnung getragen. Nummer 2 legt fest, dass die Verwaltungstätigkeit nach dem Zweiten Buch des Sozialgesetzbuchs ebenso vom Anwendungsbereich ausgeschlossen ist.

Der Ausschluss für die Verwaltungstätigkeit nach dem Zweiten Buch des Sozialgesetzbuchs umfasst auch die mit der Grundsicherung für Arbeitssuchende verbundenen Aufgaben der Sozialversicherung, die als Annex der Leis-

tungserbringung wahrgenommen werden. Damit wird sichergestellt, dass der besonderen Form der Mischverwaltung nach Artikel 91 e Abs. 1 des Grundgesetzes Rechnung getragen wird. Zugleich wird durch die einheitliche Regelung für das gesamte Zweite Buch des Sozialgesetzbuchs der gebotene Gleichklang zwischen gemeinsamen Einrichtungen und zugelassenen kommunalen Trägern gewährleistet. Zu berücksichtigen ist, dass einige fachgesetzliche Regelungen des E-Government-Gesetzes des Bundes jedoch mittelbar auch im Zweiten Buch des Sozialgesetzbuchs gelten, etwa die Änderungen im Ersten und Zehnten Buch des Sozialgesetzbuchs. Da es sich im Ersten Buch des Sozialgesetzbuchs um den allgemeinen Teil und beim Zehnten Buch des Sozialgesetzbuchs um allgemeine Vorschriften zum Sozialverwaltungsverfahren handelt, wirken Änderungen hier grundsätzlich auch in den übrigen Büchern. Des Weiteren gibt es auch noch einige unmittelbar für das Zweite Buch des Sozialgesetzbuchs angeordnete Regelungen im E-Government-Gesetz des Bundes; die Bereichsausnahme in Nummer 2 gilt nur für die Regelungen dieses Teils des Gesetzes.

Nummer 3 sieht eine Ausnahme für die Landtagsverwaltung vor, um ihrer besonderen verfassungsrechtlich gewährleisteten Stellung gerecht zu werden.

In Nummer 4 ist eine Ausnahme hinsichtlich der Tätigkeit der Finanzbehörden nach der Abgabenordnung und dem Finanzverwaltungsgesetz geregelt. Grund für diese Ausnahme aus dem Geltungsbereich ist zum einem, dass bereits zahlreiche Regelungen in den Fachgesetzen vorhanden sind und kostenträchtige Doppelstrukturen oder Vorgaben vermieden werden müssen. Zudem würde ein solches Vorgehen auch anderen Landesgesetzen entsprechen, wodurch auch hier das Ziel, ein möglichst hoher Gleichklang bei den verschiedenen Landesgesetzen, erreicht werden kann.

Nummer 5 sieht eine weitere Ausnahme für den Landesrechnungshof vor. Der Landesrechnungshof ist aufgrund seiner besonderen verfassungsrechtlichen Funktion und seiner institutionellen Unabhängigkeit aus dem Anwendungsbereich dieses Teils des Gesetzes ausgenommen. Darüber hinaus wäre eine isolierte Einbeziehung nur des Verwaltungsbereichs des Landesrechnungshofs angesichts des Interesses an einer möglichst abgestimmten Einführung elektronischer Abläufe innerhalb des Landesrechnungshofs ineffektiv und unwirtschaftlich. Vielmehr sollten die notwendigen Abstimmungsmaßnahmen - in Ansehung der Vorgaben des Gesetzes und der für die Landesverwaltung vorgesehenen Umsetzungsmaßnahmen - vom Landesrechnungshof im Rahmen seines Rechts zur Selbstorganisation in eigener Verantwortung durchgeführt werden können. Dabei steht außer Frage, dass der Landesrechnungshof sich den Veränderungen, die aus der mit dem Teil des Gesetzes beabsichtigten Einführung der elektronischen Akte in der Landesverwaltung und den weiteren damit verbundenen Regelungen resultieren, nicht verschließen, sondern seine Tätigkeit hieran ausrichten wird. Auch der Landesrechnungshof hat ein großes Interesse, den mit diesem Teil des Gesetzes angestrebten Prozess sehr eng zu begleiten. Allein die Tatsache, dass die Prüfungstätigkeit intensiven Kontakt mit den Ressorts erfordert, bedingt eine Entwicklung in möglichst weitgehendem Gleichklang. Dies gilt nicht nur in inhaltlicher, sondern auch in zeitlicher Hinsicht.

In Nummer 6 ist die Vergabekammer Niedersachsen ausgenommen. Auch sie nimmt ihre Tätigkeit gemäß § 157 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) unabhängig und in eigener Verantwortung wahr und handelt daher gerichtsähnlich.

Mit Nummer 7 wird die von der oder dem LfD geleitete Behörde ausgenommen, da sowohl die oder der LfD als auch die Behörde für den Datenschutz verfassungsrechtlich eine unabhängige Stellung einnehmen (Artikel 62 Abs. 3 der Niedersächsischen Verfassung) als auch nach der Datenschutz-Grundverordnung diese völlige Unabhängigkeit vorgegeben ist. Zudem handelt es sich bei der oder dem LfD um ein Verfassungsorgan. Insoweit ist sie oder er wie der Landesrechnungshof und der Landtag ebenfalls auszunehmen.

Nummer 8 sieht zusätzlich eine Ausnahme für die Wasser- und Bodenverbände und Nummer 9 für die Realverbände, Forst- und Jagdgenossenschaften vor, da diese Verbände teilweise ehrenamtlich geführt werden und sich aus den Beiträgen ihrer Mitglieder finanzieren. Die Regelungen in diesem Teil des Gesetzes würden daher eine starke Belastung für diese Verbände bedeuten, obgleich dies aufgrund ihrer Stellung und ihres Hintergrundes nicht gefordert werden kann. Die Wasser- und Bodenverbände erfassen alle in Betracht kommenden Verbände der Wasserwirtschaft und damit auch die Deich- und Unterhaltungsverbände.

Nummer 10 sieht eine Ausnahme für Zweckverbände wegen starker finanzieller Belastung vor. Zweckverbände können auch ehrenamtlich geführt werden und durch eine Verbandsumlage der Mitglieder, die auch Privatpersonen sein können, finanziert werden.

Zu Absatz 4:

Absatz 4 trifft für § 6 Abs. 3 und 4 eine abweichende Bestimmung des Geltungsbereichs. § 6 Abs. 3 dient der Umsetzung der Richtlinie 2014/55/EU in niedersächsisches Recht.

Da diese Richtlinie verbindlich für alle öffentlichen Auftraggeber und Auftraggeber im Sinne der Richtlinie gelten muss, durften die in den vorstehenden Absätzen aufgeführten Ausnahmen nicht für § 6 Abs. 3 und 4 gelten. Die Richtlinie war für alle öffentlichen Auftraggeber, insbesondere auch für Konzessionsgeber und Sektorenauftraggeber umzusetzen, aus diesem Grund wurde in Nummer 1 Bezug auf die entsprechenden Vorschriften im Gesetz gegen Wettbewerbsbeschränkungen genommen. Es wird zudem klargestellt, dass die Verpflichtung nur für niedersächsische Auftraggeber gilt, die als Aufraggeber nach § 98 GWB einzustufen sind.

Darüber hinaus sollen die Vorschriften des § 6 Abs. 3 und 4 auch für Aufträge unterhalb des EU-Schwellenwertes gelten. Anknüpfend an den Auftraggeberbegriff des Niedersächsischen Tariftreue- und Vergabegesetzes aus § 2 Abs. 5 NTVergG sind die z. B. Konzessionsgeber nicht erfasst. Eine Ausweitung in Niedersachsen erscheint in diesem Bereich nicht sinnvoll und sollte sich an dem bekannten Auftraggeberbegriff orientiert werden. Insoweit war eine Differenzierung im persönlichen Anwendungsbereich erforderlich.

Das katholische Büro Niedersachsen erbat in seiner Stellungnahme die Klarstellung der Nichtanwendbarkeit der Vorschriften zur elektronischen Rechnung aus § 6 Abs. 3 und 4 auf die Kirchen. Sofern die Kirchen unter den in der EU-Richtlinie 2014/55/EU genannten Auftraggeberbegriff fallen, ist eine Ausnahme vom Anwendungsbereich nicht möglich. Hinsichtlich des weiteren Anwendungsbereichs soll auch weiterhin an dem gewählten Anwendungsbereich festgehalten werden, um die elektronische Rechnung für Auftragnehmer möglichst umfassend zugänglich zu machen und eine zu große Rechtszersplitterung zu vermeiden.

Zu § 4 (Elektronischer Zugang zur Verwaltung):

Zu Absatz 1:

Diese Regelung ist erforderlich, um ein einheitliches Verfahren hinsichtlich der Kommunikation mit der Verwaltung herzustellen, auch wenn durch die Behörden kein Bundesrecht ausgeübt wird. Der Zusatz „auch wenn sie kein Bundesrecht ausführen“ stellt an dieser Stelle und im Folgenden jeweils klar, dass dieses Gesetz nicht in den Wirkungsbereich des E-Government-Gesetzes des Bundes eingreift. Gemäß § 1 Abs. 2 EGovG gilt das E-Government-Gesetz nämlich auch für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen. Aus diesem Grund ist die Vorschrift auch nahezu identisch mit § 2 Abs. 1 EGovG, sodass auf die Begründung zu diesem Bundesgesetz abgestellt wird:

„Mit dieser Vorschrift wird das Ziel A.1 der Nationalen E-Government-Strategie umgesetzt, wonach der Zugang allen in Betracht kommenden Nutzern eines Dienstes ermöglicht wird.

Absatz 1 verpflichtet die Behörden, neben den allgemein üblichen Zugängen zur Verwaltung (z. B. Posteingang für papierbasierte Eingänge, persönliches Erscheinen), auch einen Zugang für die elektronische Kommunikation zu eröffnen. Dies wird in den meisten Behörden bereits gelebt. Es soll jedoch umfassend die Möglichkeit eröffnet werden, mit jeder Behörde elektronisch in Kontakt treten zu können, und zwar grundsätzlich in jeder Angelegenheit.

Der Wortlaut der Regelung orientiert sich an § 3a Absatz 1 VwVfG.

Nach § 3a Absatz 1 VwVfG ist Voraussetzung für die Übermittlung elektronischer Dokumente, dass der Empfänger hierfür einen Zugang eröffnet hat. Eine Verpflichtung von Behörden zur Eröffnung des Zugangs ergibt sich aus dieser Regelung jedoch nicht, sondern es bedarf eines ausdrücklichen oder konkludenten Akts. Bei Behörden wird in der öffentlichen Angabe einer E-Mail-Adresse, z. B. in Briefköpfen oder auf der Internetseite, eine konkludente Eröffnung des Zugangs gesehen. Satz 1 sieht nunmehr diese Verpflichtung zur Eröffnung eines Zugangs vor.

Im einfachsten Fall erfolgt die Eröffnung des Zuganges durch die Bereitstellung eines E-Mail-Postfaches der Behörde. Hat eine Behörde ein E-Mail-Postfach, so erfüllt sie bereits die Verpflichtung im Sinne des Satzes 1. Darüber sollte jede Behörde verfügen, um eine für Bürgerinnen und Bürger, Unternehmen und Verbände einfach handhabbare elektronische Kommunikation zu gewährleisten. Mit jedem einfachen E-Mail-Postfach können in technischer Hinsicht elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen sind, empfangen werden. Soweit eine Behörde also ein E-Mail-Postfach hat, kann sie qualifiziert elektronische signierte Dokumente empfangen.

Jedoch ist die Verpflichtung zur Eröffnung eines Zuganges z. B. auch dann erfüllt, wenn eine Behörde ein elektronisches Gerichts- und Verwaltungspostfach (EGVP) oder ein anderes Verfahren oder andere spezielle Verfahren oder Portallösungen einrichtet, über das ihr elektronische Dokumente übermittelt werden können. Satz 2 verpflichtet die Behörden, auch solche Dokumente anzunehmen, die mit einer qualifizierten elektronischen Signatur versehen sind.

Absatz 1 legt lediglich fest, dass ein Zugang für die Übermittlung elektronischer Dokumente eröffnet werden muss, dabei erfolgt keine Festlegung auf ein bestimmtes Verfahren. Die Regelung ist daher technikoffen gestaltet.

Durch das Wort „auch“ wird das sogenannte Multikanalprinzip abgesichert. Das bedeutet, dass eine Behörde nicht ausschließlich elektronisch erreichbar sein darf, sondern den Zugang für die papierbasierte Eingänge nach wie vor offen halten muss. Nicht alle Personen wollen E-Government-Angebote nutzen oder sind hierzu in der Lage. Grundsätzlich sollen Bürgerinnen, Bürger, Unternehmen und Verbände frei wählen können, auf welche Weise sie mit der Verwaltung in Kontakt treten. Elektronische Informations-, Kommunikations- und Transaktionsangebote der Verwaltung treten als ein zusätzlicher Service neben die etablierten Zugänge (insbesondere persönliche Vorsprache, Telefon oder Brief).“

Elektronische Eingänge sollen gegenüber solchen in Papierform grundsätzlich weder bevorzugt noch benachteiligt werden. Vorzüge, die sich durch die elektronische Bearbeitung ergeben, etwa Zeitersparnis, können jedoch berücksichtigt werden. Die Gleichstellung elektronischer und papiergebundener Kommunikation dient der Umsetzung des Ziels A.4 der Nationalen E-Government-Strategie: („Geeignete Verwaltungsangelegenheiten lassen sich über das Internet abschließend elektronisch erledigen“).

Das oben beschriebene Multikanalprinzip, nachdem Bürgerinnen, Bürger, Unternehmen und Verbände wählen können, welchen Zugang zur Verwaltung sie nutzen, bezieht sich nicht nur auf die Freiheit, zwischen persönlichem Erscheinen, papierbasierten und elektronischen Zugang wählen zu können. Vielmehr ist es erforderlich, auch verschiedene elektronische Zugänge anzubieten. Nur wenn möglichst einfache und zugleich ausreichend sichere Verfahren in Hinblick auf Authentizität und Vertraulichkeit zur Verfügung stehen, findet die digitale Verwaltung eine ausreichende Akzeptanz. Dies ist nicht durch ein einziges Verfahren zu erreichen, sondern erfordert je nach Anforderung verschiedene Verfahren, die in diesem Paragrafen geregelt sind.

Zu Absatz 2:

Absatz 2 beinhaltet in Satz 1 die Verpflichtung der Behörden, einen nach Absatz 1 vorgesehenen Zugang über Nutzerkonten anzubieten. Nutzerkonten sind heute in der Wirtschaft das mit großem Abstand häufigste Verfahren, um Geschäftsprozesse im Internet mit Kunden abzuwickeln. Fast in jedem Online-Verfahren von Unternehmen gibt es für Kunden die Möglichkeit, sich zu registrieren und mindestens durch Angabe von persönlichen Daten, die per E-Mail zu bestätigen sind, zu identifizieren. Das so entstandene Nutzerkonto kann dauerhaft für die Abwicklung von unterschiedlichen Geschäftsprozessen verwendet werden. Nutzerkonten bieten auch für die öffentliche Verwaltung die Möglichkeit, Verwaltungsverfahren mit ihren „Kunden“ abzuwickeln. Sie ermöglichen eine hohe Akzeptanz, weil das Verfahren aus der Wirtschaft bekannt ist und meist einfach einzurichten ist. Darüber hinaus bieten sie auch die Möglichkeit eines „Rückkanals“, also der Übermittlung von Daten der Verwaltung an die Nutzerkonto-Personen.

Bei einem Nutzerkonto handelt es sich gemäß § 1 Nr. 10 um eine zentrale Identifizierungskomponente zur einmaligen oder dauerhaften Identifizierung von einer natürlichen oder juristischen Person oder einer Personengesellschaft zu Zwecken der Inanspruchnahme von Behördenleistungen. Ein Nutzerkonto-Basisdienst erfordert zunächst eine einmalige Registrierung und Identifizierung. Die Identifizierungsmethode hängt vom Sicherheitsniveau ab, für das das Nutzerkonto genutzt werden soll, und kann von einer einfachen Bestätigung der Registrierung per E-Mail bis zu einer Identifizierung per Personalausweis reichen (durch Vorlage in der Behörde oder elektronisch mit der eID-Funktion des Personalausweises). Die Form der Identifizierung wird nicht geregelt und lässt den Behörden die Freiheit, diese den Erfordernissen entsprechend zu gestalten. Es besteht auch die Möglichkeit, z. B. zunächst nur eine einfache Identifizierungsmethode anzubieten und später weitere Methoden hinzuzufügen. Nach der Registrierung wird das Nutzerkonto über eine Internetseite mit Login-Funktion genutzt, auf der z. B. Kennung und Passwort eingegeben werden, gegebenenfalls ergänzt durch weitere Identifizierungsmechanismen. Nach der Identifizierung muss der Zugang gemäß Satz 2 ermöglichen, dass Daten zur Abwicklung von geschäftlichen Prozessen bereitgestellt und entgegengenommen werden können. Der Zugang über das Nutzerkonto muss also mindestens über eine elektronische Zwischenablage – ähnlich wie ein elektronisches Postfach - verfügen, um z. B. von der Nutzerin oder dem Nutzer hochgeladene ausgefüllte elektronische Formulare oder elektronische Nachweise der Behörde zur Bearbeitung bereitzustellen oder auch um Bescheide aus einem Fachverfahren der Behörde entgegenzunehmen.

Im Gegensatz zum Zugang nach Absatz 1 muss der Zugang über Nutzerkonten nach Absatz 2 Satz 3 durch geeignete technische und organisatorische Maßnahmen gegen den unberechtigten Zugriff Dritter geschützt sein. Die Bürgerinnen und Bürger, Unternehmen und Verbände sollen darauf vertrauen können, dass die von ihnen oder für sie eingestellten Daten nicht von Unbefugten gelesen, kopiert, gelöscht oder verändert werden können. Der Begriff der „geeigneten technischen und organisatorischen Maßnahme ist dabei der Datenschutz-Grundverordnung entnommen. Insoweit muss sich die Ausgestaltung der Maßnahmen bei der Umsetzung an den Bestimmungen der Datenschutz-Grundverordnung, insbesondere an Artikel 5 Abs. 1 lit. f, Artikel 24 Abs. 1 und 2, Artikel 25 Abs. 1 und 2 und Artikel 32, orientieren.

Der Zugang über Nutzerkonten soll auch dazu animieren, dass diese vermehrt genutzt werden, da sie sich als komfortabler Weg des Zugangs zur Verwaltung darstellen und ohnehin vom Land vorgehalten werden. Nach § 12 Abs. 1 Satz 1 Nr. 1 ist das Land verpflichtet, Nutzerkonten als Basisdienst bereitzustellen. § 12 Abs. 2 verpflichtet die Behörden des Landes, diesen Basisdienst zu nutzen.

Der Zugang über das Nutzerkonto soll der bevorzugte Weg für die vertrauliche elektronische Kommunikation werden. Unzweckmäßig ist die Kommunikation über das Nutzerkonto, wenn das betreffende Verwaltungsverfahren so gestaltet ist, dass die Kommunikation auf anderem Wege einfacher ist. Dies kann etwa der Fall sein, wenn besondere Unterlagen beigefügt werden müssen, die in digitaler Form nicht vorliegen und die Digitalisierung unverhältnismäßig wäre. Zudem kann eine Kommunikation über das Nutzerkonto unzweckmäßig sein, wenn das Gegenüber dies nicht wünscht oder die Behörde nach § 7 Abs. 1 Satz 2 in bestimmten Verfahren die Vorlage eines Originals verlangt oder wenn das Nutzerkonto als Zugang für ein bestimmtes Verfahren nicht geeignet ist. In diesen Fällen ist ein Abweichen von der grundsätzlichen Nutzung des Nutzerkontos zulässig.

Die LfD merkte in ihrer Stellungnahme an, dass auf die Normen zum technisch-organisatorischen Datenschutz der Datenschutz-Grundverordnung (insbondere Artikel 5 Abs. 1 lit. f, Artikel 24 Abs. 1 und 2 und Artikel 25 Abs. 1 und

2 und Artikel 32) verwiesen werden sollte. Da die Datenschutz-Grundverordnung unmittelbar geltendes Recht und somit bereits mitzubeachten ist, soll auf einen Verweis im Gesetzestext verzichtet werden.

Zu Absatz 3:

Absatz 3 verpflichtet die Behörden, neben dem Zugang nach den Absätzen 1 und 2 einen zusätzlichen Zugang durch einen De-Mail-Zugang zu eröffnen. Dabei soll die Bearbeitung von De-Mails für Behörden des Landes möglichst durch eine Erweiterung des E-Mail-Dienstes oder in einem E-Akte-System erfolgen. Hierfür ist ein De-Mail-Gateway erforderlich, das De-Mails an den E-Mail-Dienst oder das E-Akte-System weiterleitet und von diesem entgegennimmt. Das De-Mail-Gateway ist ein Basisdienst, der gemäß § 12 Abs. 1 Satz 1 Nr. 1 zentral zur Verfügung gestellt werden soll. Die Behörden sollen den Zugang durch De-Mail spätestens bis zum 1. Juli 2021 eröffnen. Diese Zeit erlaubt den Behörden, insbesondere organisatorische Maßnahmen zur Nutzung des De-Mail-Dienstes zu treffen.

Die Nutzung des De-Mail-Kontos ist neben den Kostenersparnissen für die Bürgerinnen, Bürger, Unternehmen und Verbände auch hinsichtlich der Sicherheit der authentischen und vertraulichen Kommunikation von Vorteil. Insbesondere ersetzt eine De-Mail mit Absenderbestätigung gemäß § 1 Abs. 1 NVwVfG in Verbindung mit § 3 a Abs. 2 Satz 4 Nr. 2 des Verwaltungsverfahrensgesetzes (VwVfG) die Schriftform. Bei den Zugängen nach den Absätzen 1 und 2 ist dies nur möglich, wenn Dokumente vor der Übersendung zusätzlich mit einer qualifizierten elektronischen Signatur versehen werden. Deutlich wird dies unter anderem an dem Prozess, den ein Diensteanbieter durchlaufen muss, um ein De-Mail-Konto anbieten zu können. Der Diensteanbieter muss durch das Bundesamt für Sicherheit in der Informationstechnik nach § 17 des De-Mail-Gesetzes akkreditiert sein. Der Diensteanbieter erhält nach erfolgreichem Ablauf des Akkreditierungsverfahrens ein Gütesiegel. De-Mail eignet sich auch als Rückkanal, also etwa für die Übermittlung von Bescheiden an antragstellende Bürgerinnen und Bürger nach § 3 a Abs. 2 Nr. 3 VwVfG.

Mit der Regelung in Absatz 3 ist allerdings nicht die Verpflichtung verbunden, ausschließlich einen gesicherten Zugang über eine De-Mail-Adresse anzubieten. Diese Form des Zugangs kommt ergänzend zum Tragen und stellt damit die Möglichkeit einer sicheren Kommunikation mit einer Behörde sicher, z. B. wenn der am Verwaltungsverfahren Beteiligte bereits ein De-Mail-Konto hat und dieses nutzen möchte, weil z. B. ein schriftformersetzendes Verfahren benötigt oder eine vertrauliche Kommunikation gewünscht wird.

Zudem stellt die Schaffung eines De-Mail-Zugangs für Kommunen keine neue Verpflichtung dar. Bereits jetzt sind die Kommunen gemäß § 110 c Abs. 1 Satz 1 des Gesetzes über Ordnungswidrigkeiten in Verbindung mit § 32 a Abs. 1, 3 und 4 der Strafprozessordnung (StPO) verpflichtet, einen De-Mail-Zugang vorzuhalten, da ihnen gemäß der Verordnung über sachliche Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten die Zuständigkeiten für mehrere Ordnungswidrigkeiten obliegt.

In der Stellungnahme der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens wird auf die geringe Akzeptanz der De-Mail hingewiesen. Aufgrund dieser Stellungnahme wurde die Norm erweitert. Hauptintention der Regelung ist es, dass alle Behörden einen schriftformersetzenden Zugang bereithalten. Da De-Mail dies leistet, wird dieses Verfahren in der Regelung konkret benannt. Die Regelung erlaubt aber auch den Einsatz eines anderen Dienstes. Sollte sich zum Beispiel in Bund und Ländern ein anderes Verfahren durchsetzen, erlaubt die Regelung somit den Wechsel zu diesem. Die Landesregierung strebt an, den Einsatz des präferierten Verfahrens zwischen den Behörden abzustimmen. Eine gesetzliche Festlegung ist hierfür nicht erforderlich.

Zu Absatz 4:

Die Vorschrift verpflichtet ausschließlich die Behörden des Landes, Identitätsfeststellungen auch durch einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes oder § 78 Abs. 5 des Aufenthaltsgesetzes zu ermöglichen und die dazu notwendige Infrastruktur bereitzustellen. Absatz 4 gilt nicht, sofern die Feststellung einer Identität unter Anwesenden erfolgt.

Trotz der Verpflichtung, eine Identifizierung mittels eID-Funktion von Personalausweis und elektronischem Aufenthaltstitel zu ermöglichen, können Behörden im Bedarfsfall eine Identitätsprüfung zum Beispiel durch Vorlage von Reisepässen und Personenstandsurkunden vornehmen.

Verwaltungsverfahren können auf diesem Wege effektiver und bürgerfreundlicher gestaltet werden, da in vielen Fällen der Weg zur Behörde erspart wird.

Die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens fordert eine Übernahme der Kosten für die Infrastruktur und den personellen Mehraufwand durch das Land und hält eine Nutzungsverpflichtung für vertrauliche und rechtsverbindliche Nachrichten für angebracht. Die zur Umsetzung der Regelung erforderlichen Dienste sind entweder bereits vorhanden (E-Mail-Dienst) oder werden zukünftig als Basisdienst vom Land, meist kostenfrei, zur Verfügung gestellt. Die Übernahme der Kosten ist daher gesetzlich geregelt. Eine allgemeine Verpflichtung von Bürgerinnen, Bürgern, Unternehmen und Verbänden, bestimmte Zugangswege zu nutzen, soll bewusst nicht erfolgen, um diese bei der Wahl ihres Zugangsweges nicht unnötig einzuschränken. Allerdings wird eine Festlegung der Zugangswege erfolgen, wenn spezialgesetzliche Regelungen dies erfordern. Setzt etwa ein Fachgesetz die Schriftform voraus, kann ein per E-Mail übersandter Antrag nicht bearbeitet werden. Insofern wird

die von der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens geforderte Nutzungsverpflichtung festgelegt. Eine Regelung darüber hinaus ist entbehrlich.

Zu § 5 (Elektronische Informationen und Verwaltungsportal):

Zu Absatz 1**:**

Die Regelung in Absatz 1 dient einem bürger- und unternehmensfreundlichen Verfahren. Dazu ist es erforderlich, Informationen hinsichtlich der Aufgaben, Erreichbarkeiten und Kontaktmöglichkeiten über das Internet zur Verfügung zu stellen. Der Hinweis auf die elektronische Erreichbarkeit umfasst das Nutzerkonto nach § 4 Abs. 4 Satz 1. Diese Verpflichtung gilt für alle Behörden, da nur so ein vollständiges Informationsangebot für Bürgerinnen, Bürger, Unternehmen und Verbände bereitgestellt werden kann. Absatz 1 enthält einen Mindestkatalog der bereitzustellenden Informationen und die Verpflichtung, diese auf dem aktuellen Stand zu halten. Gemäß § 12 Abs. 1 Satz 1 Nr. 3 steht hierfür ein Basisdienst zur Verfügung, der nach § 12 Abs. 2 und 3 von den Behörden des Landes und den Kommunen zu nutzen ist. Die Informationen sollen in einer allgemein verständlichen Sprache gefasst sein. Das bedeutet, dass Menschen ohne einschlägige fachliche Vorbildung oder besondere Begabung den Sachverhalt verstehen können müssen. Der Aufwand für die Behörden ist gering, weil der nach Absatz 1 erforderliche Datensatz nur von geringem Umfang und selten anzupassen ist.

Hinsichtlich der Begründung zum Wirkungsbereich des E-Government-Gesetzes wird auf die Begründung zu § 4 Abs. 1 verwiesen.

Zu Absatz 2:

Absatz 2 enthält einen Katalog von Informationen, die jede Behörde über sich und ihre nach außen wirkende öffentlich-rechtliche Tätigkeit im Internet über Absatz 1 hinaus veröffentlichen soll. Die nach außen wirkende öffentlich-rechtliche Tätigkeit umfasst sämtliche verwaltungsrechtlich geregelten Leistungen und Verfahren der Behörde, die sich nicht in einer reinen verwaltungsinternen Tätigkeit erschöpfen.

Zweck der Vorschrift ist, dass Bürgerinnen, Bürger, Unternehmen und Verbände über das Internet (über Webseiten oder mobile Anwendungen) und alle weiteren Zugangskanäle gleichlautende Informationen darüber erhalten können, wie ein bestimmtes Verfahren abläuft, welche Nachweise zu erbringen sind, welche Kosten voraussichtlich entstehen, wer die zuständige Ansprechstelle in der Behörde ist und wie diese erreichbar ist. Durch diese Vorschrift wird die allgemeinere Verpflichtung des § 1 OZG im Hinblick auf die Informationsbereitstellung konkretisiert.

Die Vorschrift eröffnet die Möglichkeit, sich besser auf einen Kontakt mit der Behörde vorzubereiten. Zudem gehen eine Verfahrensbeschleunigung und eine Entlastung der Verwaltung mit Absatz 2 einher, da die Antragstellerin oder der Antragsteller etwa über die für das Verfahren einzureichenden Unterlagen informiert ist. Die Bereitstellung der Informationen ist der erste Schritt bei der vollständigen elektronischen Abwicklung von Verwaltungsdienstleistungen. Die Informationen liefern die nötige Grundlage, damit Bürgerinnen, Bürger, Unternehmen und Verbände erkennen können, was sie zur Umsetzung ihrer Anliegen veranlassen müssen.

Die Informationen sollen in allgemein verständlicher Sprache verfasst werden. Ziel sind also klare und adressatengerechte Formulierungen, um den Bürgerinnen und Bürgern, Unternehmen und Verbänden Informationen an die Hand zu geben, die nicht durch fachterminologische Begrifflichkeiten verwirren.

Um diese Vorschrift umzusetzen und die damit verbundenen Lasten möglichst themengerecht zu verteilen, haben sich Bund und Länder auf den Aufbau und die Pflege eines Leistungskatalogs der öffentlichen Verwaltung (LeiKa, integriert in die Anwendung „Föderales Informationsmanagement – FIM“, eine Anwendung des IT-Planungsrats des Bundes und der Länder) verständigt, der auch im Portalverbund verwendet werden soll. Dieser Katalog soll als Teil der föderalen Infrastruktur die Anbieter von Informationen zu Verfahren auf allen föderalen Ebenen redaktionell unterstützen. Bundesbehörden stellen für den LeiKa sogenannte Stammtexte zu den Verfahren bereit, deren Ausführung den Ländern übertragen wurde. Das Land ergänzt diese Stammtexte anhand von Ausführungsvorschriften und stellt sie ebenso wie die entsprechend strukturierten Informationen zu landesgesetzlich geregelten Verfahren über das IT-Verfahren BUS den vollziehenden Behörden auf Landes- oder kommunaler Ebene zur Verfügung. Soweit die von den Bundesbehörden bereitzustellenden Stammtexte für bundesrechtlich geregelte Verfahren noch nicht vorliegen, stellen die fachlich federführenden obersten Behörden des Landes diese Texte bereit. Dies ist im BUS heute schon weitestgehend gegeben. Die obersten Behörden des Landes werden durch eine vom für zentrale IT-Steuerung zuständigen Ministerium koordinierte Portalredaktion so weit wie möglich unterstützt.

Das sogenannte „Föderale Stammtexte-Management“ über den LeiKa kann wesentlich zur Konsolidierung der Redaktionsaufwände zu Verfahrensinformationen in der öffentlichen Verwaltung beitragen. Auskünfte zu Verfahren in allgemein verständlicher Sprache müssen nicht mehr durch jede vollziehende Landes- oder Kommunalbehörde selbst erstellt und gepflegt werden. Über den LeiKa und den BUS kann auf validierte und aktuelle Verfahrensinformationen zugegriffen werden. Dadurch werden landesweit einheitliche und sachlich richtige Auskünfte zu Verwaltungsverfahren unterstützt.

Verwaltungsintern sollen die Informationen in einer maschinenlesbaren Form zur Weiterverarbeitung durch internetbasierte Endkundenanwendungen der öffentlichen Verwaltung auf allen staatlichen Ebenen zur Verfügung gestellt werden. Die Bereitstellung der Informationen soll sich in Struktur und Format nach den zwischen Bund und

Ländern festgelegten Standards richten. Die Bereitstellung der Informationen soll möglichst im Vorfeld des Inkrafttretens einer regulatorischen Änderung oder innerhalb einer kurzen Frist bei ungeplanten Ereignissen, wie z. B. ad hoc eintretenden Informationslagen, erfolgen.

Hinsichtlich der Begründung zum Wirkungsbereich des E-Government-Gesetzes wird auf die Begründung zu § 4 Abs. 1 verwiesen.

Zu Absatz 3:

Die Behörden haben die Informationen nach den Absätzen 1 und 2 sowie nach § 3 Abs. 1 und 2 EGovG aktuell zu halten.

Zu Absatz 4:

Satz 1 normiert die Verpflichtung der obersten Landesbehörden, dafür Sorge zu tragen, dass die Informationen bei Vollzug von Bundes- oder Landesrecht durch die Kommunen über das Internet verfügbar sind. Sie müssen also die über das föderale Stammtext-Management gelieferten Daten sichten und gegebenenfalls anpassen und ergänzen. Durch diese Bereitstellung an zentraler Stelle werden alle anderen Behörden entlastet, was für das Land insgesamt zu einer erheblichen Erleichterung führt.

Satz 2 stellt klar, dass die Kommunen den Informationen, die durch den Bund und das Land bereits zur Verfügung gestellt werden, weitere Informationen hinzufügen können. Sie sind also nicht verpflichtet, die Informationen unverändert zu übernehmen.

Zu Absatz 5:

Mit § 5 Abs. 5 wird § 1 OZG für Niedersachsen konkretisiert. § 1 OZG verpflichtet Bund und Länder, ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Für die Bürgerinnen, Bürger, Unternehmen und Verbände sollen hierdurch bessere und schnellere Dienstleistungen, ein weder zeitlich noch örtlich eingeschränkter, einfacherer Verkehr mit den Behörden sowie die Nachvollziehbarkeit des Verwaltungshandelns erreicht werden. Im Gesetzentwurf des Onlinezugangsgesetzes wird die Auffassung vertreten, dass diese Verpflichtung auch für die Kommunen gilt, andernfalls ließe sich das Ziel des Onlinezugangsgesetzes nicht erfüllen (vergleiche BT-Drs. 18/11135 S. 5). Darüber hinaus ist eine Einschränkung der kommunalen Selbstverwaltung an dieser Stelle auch verhältnismäßig, um die bislang heterogenen IT-Strukturen bei Verwaltungsleistungen von Bund, Ländern und Kommunen sukzessive interoperabel zu gestalten.

Um in Niedersachsen eine systematische und einheitliche Umsetzung des Onlinezugangsgesetzes zu erreichen, schreibt Satz 1 vor, dass das für zentrale IT-Steuerung zuständige Ministerium ein niedersächsisches Verwaltungsportal bereitzustellen und mit dem Portalverbund von Bund und Ländern zu verknüpfen hat. Durch das zentrale Portal werden die Bereitstellung der erforderlichen Leistungen und die Verknüpfung zum Portalverbund wesentlich vereinfacht. Damit das niedersächsische Verwaltungsportal sinnvoll genutzt werden und die Vorgaben des Onlinezugangsgesetzes erfüllen kann, muss es über verschiedene Basisdienste verfügen, insbesondere ein Informationssystem über die niedersächsischen Behörden und ihre Leistungen, über Zugriffsmöglichkeiten auf elektronische Formulare und Online-Dienste sowie über elektronische Zugangsverfahren. Die Bereitstellung dieser Basisdienste wird in § 12 geregelt.

Satz 2 verpflichtet die Behörden, ihre Verwaltungsleistungen auch über das niedersächsische Verwaltungsportal anzubieten. Hierdurch wird sichergestellt, dass das Portal ein vollständiges Leistungsangebot der niedersächsischen Behörden enthält, was wesentlich zu dessen Akzeptanz bei Bürgerinnen, Bürgern, Unternehmen und Verbänden beitragen sollte. Die Verknüpfung mit dem Portalverbund kann vollständig über das Portal erfolgen. Eine Verknüpfung zu weiteren Internetangeboten ist in Niedersachsen nicht erforderlich. Es besteht die Möglichkeit, das Portal z. B. in kommunale Portale einzubinden oder mit diesen zu synchronisieren, sodass diese ohne größeren Aufwand umfassende Leistungsangebote bereitstellen können.

Die Umsetzung der Vorschrift ist weitgehend dadurch möglich, dass die Behörden die für die Verwaltungsleistungen verwendeten Formulare in elektronischer Form über das Verwaltungsportal bereitstellen und eine Übermittlung der ausgefüllten Formulare zusammen mit gegebenenfalls erforderlichen Nachweisen ermöglichen. Dabei muss unter Umständen ein schriftformersetzendes Verfahren verwendbar sein. Ergänzend zum BUS ist für Behörden in Niedersachsen bereits heute ein zentraler Formularservice und das Niedersächsische Antragsverwaltungssystem Online (NAVO) verfügbar, mit denen eine Umsetzung der Vorschrift erreicht werden kann. Der Formularservice enthält bereits einen Großteil der gängigen Formulare in elektronischer Form und kann von den Behörden in Niedersachsen kostenfrei genutzt werden.

Für die Behörden bietet es sich an, sich nicht auf die Bereitstellung und Entgegennahme elektronischer Formulare zu beschränken. Vielmehr muss es zum einen Ziel sein, die Daten aus den elektronisch ausgefüllten Formularen über standardisierte Schnittstellen in ihre Fachverfahren zu übernehmen, um so den Erfassungsaufwand deutlich zu reduzieren. Zum anderen sollten zumindest bei Massenverfahren anstelle elektronischer Formulare Assistenzsysteme angeboten werden, mit denen Bürgerinnen, Bürger, Unternehmen und Verbände im automatisierten Dialog Anträge stellen können. Hierdurch werden die Online-Angebote attraktiver und weniger fehleranfällig, was auch

zur Arbeitserleichterung in der Verwaltung beiträgt. Auch hierfür kann das NAVO als Basissystem verwendet werden. Die vollständige Einführung der Schnittstellen zu den Fachverfahren und der Assistenzsysteme erfordert allerdings noch größere Anstrengungen und wird nur über einen längeren Zeitraum umsetzbar sein.

Zur Umsetzung dieser Regelung stehen den Behörden der BUS, der Formularservice und das NAVO mit Nutzerkonto zur Verfügung.

Mit der Regelung in Absatz 5 soll der Weg für eine prozessorientierte elektronische Verwaltungsarbeit mit einheitlichen, einfach nutzbaren und rechtskonformen elektronische Verfahren bereitet werden. Langfristig soll erreicht werden, dass die Behörden ihre Geschäftsprozesse modernisieren, Daten untereinander mithilfe optimierter Verfahren elektronisch austauschen und die Bürgerinnen, Bürger, Unternehmen und Verbände Verwaltungsverfahren mit den Behörden vollständig elektronisch - auch mobil - abwickeln können. Für alle Beteiligten sollen daraus Vereinfachungen und deutliche Kostenersparnisse resultieren.

Die Regelungen der Absätze 1 und 2 werden seitens der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens als überflüssig angesehen, da sie in großen Teilen bereits erfüllt seien. Bestehende Systeme, die weiter genutzt würden, müssten erheblich verbessert und ausgebaut werden. Zudem fordert sie ein lediglich optionales Befüllen des niedersächsischen Verwaltungsportals. Mit den hier vorgesehenen Regelungen soll ein Mindeststandard für bestehende und zukünftige elektronische Informationen gewährleistet werden. Sofern diese bereits erfüllt sind, dient die Regelung der Klarstellung. Das Land sieht ferner seine Verpflichtung und beabsichtigt einen erheblichen Ausbau und Verbesserungen vorhandener Systeme. Über das niedersächsische Verwaltungsportal soll der Protalverbund nach dem Onlinezugangsgesetz befüllt werden. Ohne diese Verpflichtung würde den Vorgaben des Onlinezugangsgesetzes nicht ausreichend Rechnung getragen.

Zu § 6 (Elektronische Bezahlmöglichkeiten und Rechnungen):

Zu Absatz 1:

Absatz 1 orientiert sich an § 4 EGovG. Die Vorschrift ist erforderlich, um einheitliche Verfahren zu gewährleisten, auch wenn von den Behörden kein Bundesrecht ausgeführt wird. Der Text ist insofern nicht wortgleich mit dem Text des Bundesgesetzes, sondern an die Erfordernisse des Niedersächsischen Verwaltungskostengesetzes angepasst. Der Text des Bundesgesetzes stellt auf „Gebühren und sonstige Forderungen“ ab. Das Niedersächsische Verwaltungskostengesetz trifft eine Unterscheidung zwischen Gebühren und Auslagen und subsumiert beide gemeinsam unter dem Begriff „Verwaltungskosten“. Aus diesem Grund wurde der Begriff „Gebühren“ durch den Begriff „Verwaltungskosten“ ersetzt. Im Übrigen kann auf die Begründung des Bundesgesetzes Bezug genommen werden, die lautet (vgl. BT-Drs. 17/11473, S. 36):

> *„Die Regelung dient der Umsetzung des Ziels A.4 der Nationalen E-Government-Strategie („Alle geeigneten Verwaltungsangelegenheiten lassen sich über das Internet abschließend elektronisch erledigen“). Sehr häufig fallen in einem Verwaltungsverfahren Gebühren oder sonstige Forderungen (öffentlich-rechtlicher, gegebenenfalls auch privatrechtlicher Natur) an. Diese sollen mittels üblicher Zahlungsverfahren wie z. B. mittels Überweisung, Lastschrift, EC- Karte, Kreditkarte oder elektronische Bezahlsysteme (über Payment-Service-Provider), die sich bereits im elektronischen Geschäftsverkehr als unbare Zahlungsmethoden bewährt haben, beglichen werden können. Beim Einsatz dieser Systeme ist den Anforderungen der Datensicherheit und des Datenschutzes hinreichend Rechnung zu tragen.*
>
> *Mit der Regelung werden die Behörden verpflichtet, mindestens eines dieser üblichen Zahlverfahren anzubieten, damit die an dem Verwaltungsverfahren Beteiligten die Gebühren oder sonstigen Forderungen öffentlich-rechtlicher, gegebenenfalls auch privatrechtlicher Art, auf einfache Weise begleichen können. (…). Der Zahlungspflichtige soll nicht etwa aus diesem Grunde doch eine Behörde persönlich aufsuchen müssen. Das Angebot ist bei Verwaltungsverfahren zu eröffnen, die ganz oder teilweise elektronisch durchgeführt werden und bei denen Bürgerinnen und Bürger für das gesamte Verfahren keine Behörde persönlich aufsuchen müssen. Zu den öffentlich-rechtlichen Forderungen zählen neben den Gebühren auch Steuern und steuerliche Nebenleistungen sowie alle sonstigen Abgaben wie Beiträge, Zinsen, Geldstrafen oder Geldbußen.“*

Zu Absatz 2**:**

Absatz 2 verpflichtet die Behörden grundsätzlich zum Einsatz eines E-Payment-Verfahren, mit dem eine Zahlung an die Behörde sofort im Rahmen eines elektronischen Verwaltungsverfahrens durchführbar sein muss und die Gutschrift der Verwaltungskosten sofort erkennbar ist. Dies bedeutet, dass unmittelbar nach Durchführung der Zahlung die Gutschrift bei der Behörde bekannt sein muss und der nächste Schritt des elektronischen Verwaltungsverfahrens beginnen kann. Im Idealfall kann die gewünschte Leistung wie z. B. der Zugriff auf kostenpflichtige Geodaten sofort erfolgen. Zumindest aber müssen z. B. Antragsdaten zusammen mit der Information, dass die Verwaltungskosten zum Antrag beglichen wurden, sofort der weiteren Bearbeitung zugeführt werden. Die simple Möglichkeit, Überweisungen per Online-Banking durchführen zu können, reicht hier nicht aus, wenn die Information über den Zahlungseingang hierbei erst zu einem späteren Zeitpunkt im Verwaltungsverfahren bekannt wird.

Eine Einschränkung erfährt der Absatz dadurch, dass diese Verpflichtung dann nicht zum Tragen kommt, wenn die Festsetzung der Verwaltungskosten eine weitere Bearbeitung durch die Behörde erfordert und die Bearbeitung erst erfolgt, wenn die Zahlung eingegangen ist.

Eine Festsetzung ist unter anderem dann erforderlich, wenn es sich um eine Rahmengebühr handelt oder eine Prüfung etwa hinsichtlich der Voraussetzungen einer Billigkeitsmaßnahme durchzuführen ist. Zudem ist der Einsatz eines E-Payment-Verfahrens besonders hilfreich in den Fällen, in denen die Bearbeitung erst nach Eingang erfolgt. Wenn eine Bezahlung erst nach Durchführung der Verwaltungsleistung vorgesehen ist, kann auf das E-Payment-Verfahren verzichtet werden.

Die Formulierung als Soll-Vorschrift zeigt, dass es sich grundsätzlich um eine Verpflichtung handelt, die aber in atypischen Fällen nicht erfüllt werden muss. Ein atypischer Fall liegt z. B. vor, wenn in einem Verfahren nur sehr selten ein Zahlungsvorgang erforderlich ist, sodass sich der Aufwand für die Anbindung des E-Payment-Verfahrens nicht lohnt.

Ein E-Payment-Verfahren ist in Niedersachsen bereits eingeführt und kann auch für weitere Verfahren genutzt werden.

Zu Absatz 3**:**

Absatz 3 setzt die Richtlinie 2014/55/EU in niedersächsisches Recht um. Die Vorschrift gilt aufgrund des erweiterten Geltungsbereiches auch für niedersächsische Auftraggeber nach § 3 Abs. 4. Dieser knüpft an den aktuellen § 98 GWB an. Anders als die Richtlinie 2014/55/EU umfasst die Regelung nicht nur Rechnungen, die infolge einer europaweiten Ausschreibung entstehen (oberschwelliger Bereich), sondern alle Rechnungen mit Auftragshöhen unterhalb der jeweils maßgeblichen EU-Schwellenwerte (unterschwelliger Bereich). Diese Ausweitung ist erforderlich, um die angestrebte Wirtschaftlichkeit und damit Akzeptanz der elektronischen Rechnungsstellung bei Unternehmen zu erreichen, zumal ein Großteil der Aufträge in die letztgenannte Kategorie fällt. Es wäre der Wirtschaft nicht vermittelbar, wenn nur Rechnungen aus europaweiten Ausschreibungen elektronisch angenommen würden und andere nicht. Insbesondere würde eine reine Erfassung lediglich des oberschwelligen Bereichs dazu führen können, dass Unternehmen ihre internen Buchhaltungssysteme umstellen müssten, wodurch ein hoher Aufwand entstehen würde.

Von dieser Regelung profitiert auch die Verwaltung, weil die Einführung der elektronischen Rechnungen nur dann wirtschaftliche Vorteile bringt, wenn ausreichend viele Rechnungssteller diese Einführung mitgehen. Das Erfassen von Rechnungen im unterschwelligen Bereich ist zudem aus Gründen der Verwaltungspraktikabilität auch günstiger als die schlichte Umsetzung der Richtlinie, da die Rechnungsempfänger nicht unterscheiden müssen, sondern sämtliche Rechnungen, die elektronisch eingehen, auch angenommen werden. Durch die sich aus dem Gesetz für Auftraggeber ergebende umfassende Verpflichtung zum Empfang und zur Verarbeitung elektronischer Rechnungen – unabhängig von einem Schwellenwert im Sinne des § 3 Abs. 4 – ergeben sich Synergieeffekte.

Eine Belastung von kleinen und mittleren Unternehmen findet nicht statt, da keine Forderungsverpflichtung für elektronische Rechnungen besteht. Vielmehr werden die Unternehmen, die bereits auf elektronische Rechnungen umgestellt haben, gestärkt, indem ein zusätzlicher, vereinfachter Weg der Rechnungsstellung eröffnet wird.

Für die Verarbeitung reichen eine Visualisierung der Rechnung und eine anschließende papierbasierte Bearbeitung zunächst aus, obgleich dies in der Sache nicht zweckdienlich wäre und eine rein elektronische Weiterverarbeitung der zu bevorzugende Weg wäre.

Der in Absatz 3 verwendete Begriff der elektronischen Rechnung wird in § 1 Nr. 5 definiert. Eine Rechnung ist demgemäß nicht bereits dann elektronisch, wenn sie im PDF-Format versendet wurde, obgleich dies nach dem allgemeinen Sprachgebrauch so verstanden werden könnte. Ein solches Vorgehen stellt jedoch keine elektronische Rechnung im Sinne dieses Gesetzes dar. Erforderlich ist vielmehr, dass es sich um ein strukturiertes elektronisches Format handelt und dieses die automatische und vollständige elektronische Verarbeitung der Rechnung ermöglicht, heute üblicherweise ein XML-Format. Insofern muss die elektronische Rechnung so ausgestaltet sein, dass eine vollständige elektronische Verarbeitung möglich ist, sofern in den Behörden die entsprechenden Strukturen und Schnittstellen vorhanden sind.

Die Verpflichtung nach Absatz 3 gilt gemäß Artikel 3 Abs. 2 Satz 2 Nr. 1 erst ab dem 18. April 2020. Damit wird der mögliche Spielraum für die Verschiebung der Verpflichtung (30 Monate nach Veröffentlichung der Europäischen Norm durch das CEN) ausgeschöpft. Hierdurch bleibt genügend Zeit zur Einführung eines geeigneten elektronischen Verfahrens. Gemäß § 12 Abs. 1 Satz 1 Nr. 6 ist ein Basisdienst zum Empfang und zur Verarbeitung von elektronischen Rechnungen den Behörden zur Verfügung zu stellen. Der Basisdienst soll unter anderem einen Service bereitstellen, damit Unternehmen elektronische Rechnungen online erstellen können, falls sie nicht über eine entsprechende Software verfügen.

Zu Absatz 4:

In Absatz 4 wird eine Verordnungsermächtigung für die Einzelheiten, also das Verfahren der Verarbeitung, die Verwendung von Standards und die Möglichkeit von Ausnahmen, normiert. Dies ist unter anderem erforderlich, weil sich der technische Standard der elektronischen Rechnung aufgrund der technischen Entwicklung verändern kann.

Die Ausgestaltung der Datenverarbeitung hat entsprechend den Vorgaben der Datenschutz-Grundverordnung zu erfolgen.

In Satz 2 wird der Umfang der Verordnungsermächtigung konkretisiert. Nach Nummer 1 kann die Art und Weise des Empfangs und der Verarbeitung elektronischer Rechnungen näher ausgestaltet werden. Hier können z. B. die bereitzustellenden Übertragungswege oder das Formatprüfungsverfahren normiert werden. Nummer 2 ermächtigt dazu, Anforderungen an die elektronischen Rechnungen zu stellen. Nur wenn diese Anforderungen vom Rechnungssteller erfüllt werden, müssen die elektronischen Rechnungen entgegengenommen werden. Wichtigster Punkt ist die Festlegung des Rechnungsdatenmodells, das aufgrund der Richtlinie 2014/55/EU in bestimmtem Rahmen vorgegeben wird. Nummer 3 ermächtigt die Landesregierung, Ausnahmen von den Verpflichtungen nach Absatz 1 im Bereich von sicherheitsspezifischen Aufträgen zuzulassen.

Die Regelungen sollten nach Ansicht der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens auf zwei Paragrafen aufgeteilt werden, da die Absätze 1 und 2 das elektronische Bezahlverfahren und die Absätze 3 und 4 die elektronische Rechnung regeln. Zudem sieht sie die Fristen für den zeitlichen Vorlauf zur Einführung der elektronischen Rechnung als zu gering. Dieser Anregung wird nicht gefolgt: Aufgrund des Sachzusammenhangs zwischen Bezahlverfahren und Rechnungsstellung sollen die Regelungen in einer Norm geregelt werden. Hinsichtlich der Fristen wurde der Entwurf in Artikel 3 angepasst, sodass nunmehr von den Möglichkeiten zur Umsetzung der Richtlinie 2014/55/EU weitergehender Gebrauch gemacht wird.

Zu § 7 (Nachweise):

Zu Absatz 1:

Die Regelung ist wortgleich mit der Regelung in § 5 Abs. 1 EGovG. Da keine landesspezifischen Besonderheiten vorliegen, wird auf die Begründung des Bundesgesetzes Bezug genommen. Die Begründung des Bundes hierzu lautet (BT.-Drs. 17/11473, S. 37):

> *Die elektronische Durchführung eines Verwaltungsverfahrens erfasst sowohl die durchgängige wie auch die lediglich teilweise elektronische Durchführung mittels elektronischer Kommunikation (vgl. § 2).*
>
> *Die Verwaltungspraxis lässt bereits derzeit häufig die Vorlage von Kopien genügen. Dies soll zur Regel werden, wenn die Vorlage eines Originals nicht durch Rechtsvorschrift angeordnet ist oder die Behörde in Ausübung ihres Verfahrensermessens (§ 26 VwVfG) für bestimmte Verfahren (z. B. Visumverfahren) oder im Einzelfall die Vorlage eines Originals verlangt, da selbst eine beglaubigte elektronische Kopie ausnahmsweise keine hinreichende Sicherheit gewährt. Letzteres kommt insbesondere bei Verfahren in Betracht, bei denen ein besonderes Täuschungsrisiko besteht. Auch für den Fall, dass Umstände zu der Annahme berechtigen, dass die eingereichte elektronische Kopie mit dem Original nicht übereinstimmt, kann die Behörde die Vorlage im Original verlangen. Solche Umstände können z. B. Bearbeitungsspuren an der Kopie oder Inkonsistenzen im Vorbringen sein, die anderweitig in dem Verfahren zutage getreten sind oder in einem späteren Stadium zutage treten. Als Originale sind sowohl papiergebundene Formate wie auch elektronische Originale zu verstehen. Die von der Behörde zu bestimmende Art der Einreichung umfasst neben der Frage der Zulassung einer Kopie oder der Forderung des Originals auch die bewusst technikoffen gestaltete und an § 3a VwVfG angelehnte Frage, in welchem Format ein elektronisches Dokument einzureichen ist.*

Fachaufsichtsbehörden, insbesondere die Ministerien, sind durch diese Regelung nicht gehindert, den nachgeordneten Behörden im Rahmen der ihnen zukommenden Fachaufsicht, die auch die Zweckmäßigkeit der Aufgabenwahrnehmung umfasst, allgemein oder im Einzelfall vorgeben zu können, in welchen Fällen und Verfahren Nachweise gegebenenfalls nicht elektronisch eingereicht werden können.

Zu Absatz 2:

Die Regelung orientiert sich an der Regelung in § 5 Abs. 2 EGovG. Aufgrund der Vorgaben der Datenschutz-Grundverordnung wurden die Begrifflichkeiten in Satz 2 auf den Oberbegriff der „Verarbeitung“ reduziert. Da keine landesspezifischen Besonderheiten vorliegen, wird im Übrigen auf die Begründung des Bundesgesetzes Bezug genommen. Die Begründung des Bundes hierzu lautet (BT.-Drs. 17/11473, S. 37):

> *Der Grundsatz, dass personenbezogene Daten regelmäßig beim Betroffenen zu erheben sind, führt häufig dazu, dass dieser die Daten auch dann noch einmal erneut bei einer Behörde angeben muss, wenn die Daten bereits in einem anderen Verwaltungsverfahren bei einer anderen Behörde angegeben wurden. Dies ist nicht nur eine unnötige Erschwernis für Bürgerinnen und Bürger sowie Unternehmen, sondern auch für die elektronische Abwicklung von Verwaltungsverfahren. Denn wenn in einem Verwaltungsverfahren als Nachweise z. B. Bescheide oder Bescheinigungen einer anderen Behörde benötigt werden, könnte die Behörde auf die Vorlage der Originale durch Bürgerinnen und Bürger oder das Unternehmen verzichten und stattdessen diese Nachweise elektronisch bei der ausstellenden Behörde einholen. Auch andere öffentliche Stellen im Sinne des Bundesdatenschutzgesetzes (BDSG) wie z. B. Organe der Rechtspflege, Handwerkskammern stellen häufig Bescheinigungen aus, die in Verwaltungsverfahren benötigt werden. Sie sollten daher diesbezüglich gleichgestellt werden. Elektronische Bescheinigungen der Handwerkskammern entsprechen bereits der Praxis im Rahmen der Anwendung der Dienstleistungsrichtlinie.*

Dieser Weg ist insbesondere dann von Interesse, wenn wegen eines besonderen Bedürfnisses nach Verlässlichkeit der Nachweise die Vorlage einfacher elektronischer Kopien durch den Antragsteller nicht ausreicht. Im Interesse der Bürgerfreundlichkeit sollte die Devise „die Daten sollen laufen, nicht die Bürgerin/der Bürger" den Verwaltungsverfahren zugrunde gelegt werden. Der Antragsteller hat die Möglichkeit der Entscheidung, ob er der Behörde die Daten selbst übermittelt, z. B. durch Vorlage der Originalbescheide, oder ob er die Behörde ermächtigt, die Daten bei der Stelle abzurufen, bei der sie vorliegen. Dabei darf die Mitwirkungspflicht, die sich auch auf das Beibringen von Unterlagen erstreckt, nicht auf die Behörde abgewälzt werden. Es bedarf weiterhin einer aktiven Beteiligung des Antragstellers. § 26 VwVfG bleibt als Grundsatz von der Regelung des § 5 EGovG unberührt.

Als bereichsspezifische Ausnahme zum in § 4 Absatz 2 Satz 1 BDSG normierten Grundsatz der Direkterhebung regelt Absatz 2 daher als weitere Verfahrenserleichterung, dass eine für ein Verwaltungsverfahren zuständige Behörde erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, direkt bei der ausstellenden Behörde elektronisch einholen kann. Die Erforderlichkeit der Datenübermittlung ergibt sich auch aus dem datenschutzrechtlichen Rahmen, der für die anfordernde und die abgebende Behörde gilt.

Dabei muss die Einwilligung des betroffenen Verfahrensbeteiligten vorliegen. Gegebenenfalls notwendige Schwärzungen personenbezogener oder schutzwürdiger Daten Dritter, auf die sich die Einwilligung naturgemäß nicht beziehen kann, sind dabei auch in elektronischen Dokumenten vorzunehmen. Die Einwilligung des Verfahrensbeteiligten ist entbehrlich, sofern Rechtsvorschriften die Erhebung bei der ausstellenden Behörde bzw. die Übermittlung zwischen den beteiligten Stellen erlauben. Der Grundsatz der Direkterhebung gilt dann nicht, sofern es spezialgesetzliche Sondervorschriften gibt.

Die aktuelle Formulierung des Absatzes 2 Satz 2 bezieht auch die Begründung eines Antrags mit ein, da diese zur Ermittlung des Sachverhalts benötigt wird. Wenn eine Behörde den Nachweis bei einer anderen Behörde einholt, muss sie dieser mitteilen, dass die Einwilligung des Betroffenen vorliegt, soweit die abgebende Behörde über diese Information nicht bereits nachweislich verfügt. Die Mitteilung muss daher so erfolgen, dass die abgebende Behörde später glaubhaft machen kann, dass eine Einwilligung vorgelegen hat.

Hinsichtlich der Einwilligung als solche muss sie den direkt anwendbaren Voraussetzungen der Artikel 7 und 8 DSGVO entsprechen.

Hervorzuheben ist hierbei, dass Artikel 7 DSGVO grundsätzlich keine Schriftform für die Einwilligung vorschreibt. Dennoch ist aufgrund der Nachweispflicht und der im Gerichtsverfahren damit verbundenen Beweispflicht generell auf ein freiwilliges Schriftformerfordernis zurückzugreifen. Hinsichtlich des Inhalts der Einwilligung gilt Artikel 7 Abs. 2 DSGVO unmittelbar. Auch ist die Erklärung nach Artikel 7 Abs. 3 DSGVO jederzeit für die betroffene Person widerrufbar auszugestalten.

Sofern die Einwilligung im Rahmen eines Dienstes der Informationsgesellschaft erteilt werden können soll, also insbesondere auf Webseiten, und Einwilligungen von Minderjährigen nicht ausgeschlossen sind, sind die weiteren Vorgaben gemäß Artikel 8 DSGVO zu beachten.

Zu § 8 (Elektronische Formulare):

§ 8 entspricht dem Wortlaut des § 13 EGovG. Da keine landesrechtliche Besonderheiten vorliegen, kann die Regelung sowie ihre tragenden Gründe in Anlehnung an das E-Goverment-Gesetz übernommen werden. Die Begründung des Bundes lautet (BT.-Drs. 17/11473, S. 44 f.):

„§ 126 Absatz 1 des Bürgerlichen Gesetzbuches (BGB) bestimmt, dass eine Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden muss, wenn durch Gesetz schriftliche Form vorgeschrieben ist.

Der Umkehrschluss, dass immer dann, wenn eine Unterschrift vorgeschrieben ist, damit eine gesetzliche Schriftform angeordnet ist, kann weder aus dem Wortlaut noch aus dem Zweck der Norm hergeleitet werden. Unterschriften werden im täglichen Leben vielmehr auch außerhalb gesetzlicher Schriftformerfordernisse zu verschiedensten Zwecken geleistet und sind insbesondere als Feld für die Unterschrift des Erklärenden üblicher Bestandteil jeglicher Art von Formularen.

Dennoch gibt es eine verbreitete Rechtspraxis, die im Fall von durch Rechtsnorm vorgeschriebenen Formularen aus dem Unterschriftsfeld des Formulars ein gesetzliches Schriftformerfordernis herleitet. In der Fachliteratur und Rechtsprechung spiegelt sich diese Praxis nicht wieder. Was im Fall der händischen Unterschrift unter ein Papierformular jedenfalls in der Praxis keine Probleme verursacht, wird bei der elektronischen Abbildung des Formulars zu einer erheblichen Hürde im Rechtsverkehr: Damit kann das Formular nur dann elektronisch verschickt werden, wenn es qualifiziert elektronisch signiert wird. Dies führt angesichts der mangelnden Verbreitung der [qualifizierten elektronischen Signatur (qeS)] in der Praxis dazu, dass die von zahlreichen Verwaltungen im Internet schon jetzt zum Download angebotenen Formulare ausgedruckt und in Papierform versandt werden müssen, statt eine Versendung per einfacher E-Mail zu ermöglichen, wenn nicht explizit Schriftform angeordnet ist.

Mit Satz 1 wird klargestellt, dass kein Schriftformerfordernis vorliegt, wenn dieses nicht explizit in der Norm angeordnet wird.

Sofern die dem Formular zugrundeliegende Rechtsnorm für die Erklärung explizit Schriftform anordnet, kann hier in der elektronischen Welt auch künftig nur eine Unterzeichnung über die qeS sowie durch die mit diesem Gesetz neu eingeführten schriftformersetzenden Technologien abgebildet werden.

Für alle anderen durch Rechtsvorschrift angeordneten Formulare ist klargestellt, dass auch eine Übermittlung des elektronischen Formulars an die Behörde beispielsweise als ausgefülltes pdf-Dokument ohne Unterschrift möglich ist. Das Ausdrucken eines online ausgefüllten Formulars, das Unterschreiben sowie das frühere Übersenden mittels Post durch die Bürger bzw. Unternehmen entfallen. Das Interesse der Verwaltung an der durch das Formular strukturierten Abfrage von Informationen ist dadurch gleichermaßen gewahrt.

Satz 2 stellt klar, dass bei in Papierform ausgegebenen Formularen weiterhin das in der Rechtsnorm abgedruckte Format samt Unterschriftsfeld beizubehalten ist und das Unterschriftsfeld bei an die Behörde gerichteten Formularen lediglich bei der elektronischen Fassung entfällt. Dies gilt auch in den Fällen, in denen ein Schriftformerfordernis besteht, da die Schriftform gemäß § 3a VwVfG (neu), § 36a SGB I (neu), § 87a AO (neu) nicht durch eine handschriftliche Unterschrift in einem Feld, sondern durch deren elektronischen Substitute abgebildet wird.

Da das Unterschriftserfordernis häufig die Funktion hat, die moralische Hemmschwelle gegenüber Falschangaben zu erhöhen, bleibt es der Behörde unbenommen, diese Hemmschwelle auf andere Weise zu erhalten.

Hierzu kann sie z. B. das Unterschriftsfeld bei einer für die elektronische Versendung bestimmten Fassung des Formulars durch eine vorformulierte Erklärung ersetzen, mit deren Bestätigung versichert wird, dass die Person, die die Erklärung in den Rechtsverkehr gibt, mit der im Formular bezeichneten Person identisch ist, oder andere geeignete Maßnahmen ergreifen, sodass bei einem Missbrauch der Urheberschaft eine strafrechtliche Verfolgung nach § 269 des Strafgesetzbuches (StGB) erfolgen kann.

Die Regelung des § 13 findet unabhängig von der Bezeichnung als Formular, Vordruck, Formblatt oder ähnlichen Begriffen Anwendung."

Zu § 9 (Georeferenzierung):

Zu Absatz 1:

Viele Sachdaten der öffentlichen Verwaltung (Angaben) haben einen sogenannten Raumbezug, z. B. zu einer Adresse oder zu einem Landschaftsschutzgebiet. Dennoch ist es aufgrund der Vorhaltung und Verwaltung dieser Register nicht möglich, die Informationen räumlich in Beziehung zu setzen, z. B. um Nachbarschaften oder Entfernungen, Häufigkeit von Einrichtungen festzustellen. Anwendungsbeispiele sind unter anderem: Wo liegen die Schulen im Stadtgebiet? In welcher Entfernung liegen Schulen zu Kindergärten? Eine Verbindung kann derzeit nur aufwändig hergestellt werden, z. B. indem für die Adresse oder eine geografische Angabe (Schloss Marienburg, Wurmberg, Solling) die Lage über Hilfsmittel ermittelt wird. Dieser Aufwand entsteht somit bei jeder Analyse oder Abfrage erneut. Dies kann verbessert werden, wenn sämtliche Daten, die einen Bezug zu einem Grundstück haben, mit der Koordinate des Flurstücks bzw. des Gebäudes verknüpft werden. Flurstücke sind nach dem Liegenschaftskataster definierte Eigentumsflächen. Gebiete sind z. B. Baugebiete oder Naturschutzgebiete, die wiederum häufig aus mehreren Flurstücken bestehen. Zur einheitlichen Umsetzung sind technische Regelungen zu treffen. Das Liegenschaftskataster führt bereits zu Gebäuden eine sogenannte Hauskoordinate und zu Flurstücken eine sogenannte Flurstückskoordinate. Es liegt nahe, diese Informationen zu nutzen, um Daten mit einer bundesweit einheitlich festgelegten direkten Georeferenzierung (Koordinate) zu ergänzen. Das Niedersächsische Gesetz über das amtliche Vermessungswesen verpflichtet Behörden und andere Stellen des Landes schon heute, Angaben des amtlichen Vermessungswesens (Geobasisdaten) für ihre raumbezogenen Informationen zu nutzen. Die Speicherung der Koordinate ergänzt die Adressangabe innerhalb des Registers. Es wird keine neue Information erfasst. Zusätzlich kann zur Koordinate, die in jedem Fall innerhalb des betroffenen Gebäudes bzw. Flurstücks oder Gebietes liegen sollte, auch ein Flächenumring im Register gespeichert werden. Eine darüber hinausgehende, von Grundstücken und Gebäuden losgelöste Beschreibung raumbezogener Objekte durch thematisch und geometrisch adäquate Koordinaten im Landesbezugssystem einschließlich der Metadaten für jedes Objekt ist unbenommen. Durch die Speicherung der Koordinaten ist dann eine direkte räumliche und vor allem technisch einfache Zuordnung und Verknüpfung verschiedener Informationen möglich. Damit können auch Auswertungen deutlich vereinfacht werden. Die Registerangaben können z. B. mithilfe von Geobasisdaten leicht auf einer elektronischen Karte dargestellt werden.

Die Angaben sind für alle niedersächsischen Grundstückbezüge zu ergänzen. Dies stellt klar, dass bei Bezügen zu Grundstücken außerhalb Niedersachsens die Koordinaten nicht aufgenommen werden müssen. Von der Regelung sind alle Register ausgeschlossen, die ausschließlich Bezüge zu Grundstücken außerhalb Niedersachsens haben.

Die einheitliche Festlegung für die Georeferenzierung in Registern fördert die Nutzungs- und Auswertungsmöglichkeiten aller Daten der öffentlichen Verwaltung. Einheitliche Vorgaben für die Georeferenzierung, also die Möglichkeit zur „Übersetzung" von Raumbezugsinformationen wie Adressen in ein Koordinatenpaar, sind die grundlegende

Voraussetzung für die Interoperabilität der Geodaten, auch im Sinne einer Geodateninfrastruktur Deutschland. Daher wurde die Festlegung für einen Geokodierungsdienst gemeinsam in Bund-Länder-Gremien erarbeitet und im IT-Planungsrat des Bundes und der Länder beschlossen.

Von der Regelung sind nur Register betroffen, die entweder neu aufgebaut oder überarbeitet werden, z. B. durch Umsetzung eines analogen Registers in ein digitales oder durch wesentliche Neustrukturierung und grundlegender Überarbeitung eines digitalen Registers. Die Ergänzung der Georeferenzierung sollte nicht den Hauptgrund und Hauptaufwand der Überarbeitung durch die niedersächsischen Behörden darstellen. Nicht betroffen von der Regelung ist auch das Grundbuch, das ebenfalls durch Bundesgesetz geregelt ist. Das Grundbuch dient zudem der Dokumentation von Eigentums- und anderen Sachenrechten an Grundstücken und grundstücksgleichen Rechten und damit in erster Linie dem Grundstücksverkehr. Die Grundstücke werden im Grundbuch nach den in den Ländern eingerichteten amtlichen Verzeichnissen benannt (Liegenschaftskataster). Das Liegenschaftskataster weist die tatsächlichen Verhältnisse am Grund und Boden nach (Flurstücke) und wird auf Basis des § 2 Abs. 2 der Grundbuchordnung geführt. Eine Erstreckung des Anwendungsbereichs der Regelung auf das Grundbuch ist damit nicht erforderlich, weil eine Verbindung zum Liegenschaftskataster – und damit zu den Flurstückskoordinaten – bereits besteht.

Die Regelung legt nicht fest, ob, durch wen und wie die in den jeweiligen elektronischen Registern gespeicherten Daten genutzt werden können; dies ergibt sich aus den jeweiligen spezialgesetzlichen Vorschriften. Datenschutzrechtliche Aspekte (Abstrahierung, Löschungsfristen etc.) ergeben sich aus den jeweiligen Rechtsvorschriften für das einzelne Register. Klarstellend wird darauf hingewiesen, dass bei der Verknüpfung personenbezogener Geoinformationen die datenschutzrechtlichen Vorschriften zu beachten sind.

Der an § 14 EGovG angelehnte § 9 setzt einen Mindeststandard für Georeferenzierung, der mit wenig Aufwand bei Verwendung des Geokodierungsdienstes des Bundesamtes für Kartografie und Geodäsie in sehr vielen Anwendungsfällen ausreicht und für niedersächsische Landesbehörden und Kommunen keine zusätzlichen Kosten verursacht.

Zu Absatz 2:

Absatz 2 legt fest, dass in diesem Gesetz nur Register aufgrund von Rechtsvorschriften des Landes geregelt werden. Für Register aufgrund von Bundesvorschriften ist § 14 EGovG einschlägig. So sind z. B. Melderegister, Personalausweisregister, Passregister und Personenstandsregister bundesrechtlich geregelt und daher von der Vorschrift nicht betroffen. Das Gleiche gilt für Register aufgrund bundesrechtlich geregelter amtlicher Statistiken.

Die Umsetzbarkeit der Georeferenzierung und der Mehrwert werden seitens der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens bezweifelt. Zudem äußerte sie in ihrer Stellungnahme datenschutzrechtliche Bedenken hiergegen. Die vorgetragenen Zweifel werden nicht geteilt. Da die Regelung nur bei neuen oder überarbeiteten Registern zum Tragen kommt, sind die Daten nicht nachzupflegen, sondern bei der Planung der Register mit zu berücksichtigen. Der Aufwand erscheint insoweit übersichtlich. Auch besteht ein hoher Mehrwert, so werden bereits heute Leistungen der Verwaltungen vermehrt auf Karten auf den Webseiten von Behörden dargestellt. Hierdurch wird das Auffinden von Leistungen für die Nutzerinnen und Nutzer erheblich erleichtert. Zukünftig wird dies durch die Georeferenzierung noch einfacher zu integrieren sein. Zudem stellt das Land einen Basisdienst für die Georeferenzierung zur Verfügung. Datenschutzrechtliche Bedenken wurden seitens der LfD nicht erhoben.

Zu § 10 (Elektronische Aktenführung):

Eine elektronische Akte ist eine logische Zusammenfassung sachlich zusammengehöriger oder verfahrensgleicher Vorgänge und Dokumente, die alle bearbeitungs- und aktenrelevanten Informationen (unter anderem E-Mails, sonstige elektronisch erstellte Unterlagen sowie gescannte Papierdokumente) umfasst und so eine vollständige Information über die Geschäftsvorfälle eines Sachverhalts ermöglicht. Sie kann in Einzelfällen durch Aktenteile in Papierform ergänzt werden, wenn dies z. B. zur besseren Nachweisbarkeit geboten ist (Hybridakten), etwa um Originalurkunden für einen Schriftvergleich, der elektronisch nicht möglich wäre, vorzuhalten. Die elektronische Akte ersetzt auf diese Weise die Aktenführung auf Papierbasis oder in anderer körperlicher Form. Die Aktenführung beinhaltet im Sinne dieses Gesetzes alle Arbeitsschritte im Umgang mit Akten, also sowohl die Erstellung und Umschreibung von Akten, das Ablegen und Aufrufen von aktenrelevanten Dokumenten in Akten (Aktenablage), die Bearbeitung von Dokumenten und Vorgängen innerhalb der Verwaltung inklusive der Zeichnungsverfahren (Vorgangsbearbeitung), die Aufbewahrung der Akten, das Schließen von Akten und das Aussondern oder Vernichten von Akten. Auch das Scannen oder sonstige Aufbereiten von Unterlagen für die Ablage in Akten ist Teil der Aktenführung. Die Vorteile der elektronischen Akte liegen vor allem im schnelleren Auffinden bearbeitungsrelevanter Informationen, im ortsunabhängigen, kontinuierlichen Zugriff auf Informationen, im Wegfall von Medienbrüchen und in der Verbesserung von Transparenz. Gemäß § 12 Abs. 1 Satz 1 Nr. 7 wird für die elektronische Aktenführung ein Basisdienst bereitgestellt, den die Behörden des Landes gemäß § 12 Abs. 2 Satz 1 zu nutzen haben, soweit nicht andere IT-Systeme für konkrete Aufgaben zur Aktenführung eingesetzt werden müssen.

Im Rahmen der Verbandsbeteiligung fordert der Deutsche Gewerkschaftsbund Bezirk Niedersachsen – Bremen – Sachsen-Anhalt, dass die Planung der Infrastruktur der elektronischen Akte immer im Einklang mit der Finanzierung

der notwendigen IT-Sicherheit geplant werden muss. Mit der zunehmenden Digitalisierung nehmen auch die Anforderungen an die IT-Sicherheit zu. Bei der Planung zukünftiger IT-Vorhaben wird daher der Aspekt der IT-Sicherheit stets zu berücksichtigen sein. Im Rahmen der elektronischen Akte gilt dies umso mehr, da die Vorgaben ordnungsgemäßer Aktenführung nach § 10 Abs. 3 zu berücksichtigen sind.

Zu Absatz 1:

Für alle Behörden besteht nach Absatz 1 die Möglichkeit zur Einführung der elektronischen Aktenführung. Absatz 1 stellt keine Verpflichtung dar. Damit wird insbesondere ein Eingriff in die Organisationshoheit der Kommunen vermieden. In der Sache gilt natürlich auch für diese Behörden, dass eine digitale Verwaltung nur mit der Einführung der elektronischen Aktenführung zu erreichen ist. Tatsächlich haben bereits viele Kommunen damit begonnen, Akten elektronisch zu führen. Die Regelung unterstützt diese insoweit bei der Einführung und Ausgestaltung der E-Akte. Grundsätzlich ist die elektronische Aktenführung auch ohne diese Regelung zulässig. Es gibt aber in vielen Behörden Unsicherheiten, ob dies für alle Bereiche zutrifft. Absatz 1 dient daher zur Klarstellung. Nur wenn spezialgesetzliche Regelungen die elektronische Aktenführung explizit verbieten, ist sie unzulässig.

Zu Absatz 2:

Satz 1 verpflichtet alle Behörden des Landes, neu anzulegende Akten ab dem1. Januar 2026 ausschließlich elektronisch zu führen. Mit dieser Vorgabe wird die Grundlage geschaffen, um die internen Prozesse in der Verwaltung vollständig elektronisch zu unterstützen. Ohne eine elektronische Aktenführung ist eine digitale Verwaltung nicht möglich. Die Verpflichtung ist als Soll-Vorschrift formuliert, da in begründeten Fällen Ausnahmen von der Verpflichtung möglich sein müssen.

Durch Satz 2 soll eine Minimalversorgung mit Arbeitsplätzen, die eine elektronische Akte führen, sichergestellt werden. Die Verpflichtungen aus dem Onlinezugangsgesetz sehen vor, dass Anträge und Leistungen auch elektronisch angeboten und entgegengenommen werden müssen. Hierfür ist es notwendig, auch die Dokumente rechtssicher zu verwahren, um deren Beweiskraft zu erhalten. Beispielhaft lassen sich Dokumente mit einer elektronischen Signatur oder De-Mail-Eingänge nennen. Dies lässt sich effizient nur dadurch realisieren, dass mindestens die Arbeitsplätze mit einem E-Akte-System ausgestattet werden, auf denen Verwaltungsleistungen im Sinne des Onlinezugangsgesetzes erbracht werden.

Sofern besondere Gründe vorliegen, kann für die Umsetzung im nachgeordneten Bereich, im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung, ein späterer Termin bestimmt werden. Ein besonderer Grund kann auch dann vorliegen, wenn die erforderlichen Haushaltsmittel für die Einführung der elektronischen Aktenführung nicht bereitgestellt werden können.

Weiter bleibt festzuhalten, dass sich Satz 3 sowohl auf Satz 1 als auch auf Satz 2 bezieht. Beide Termine können im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung individuell verschoben werden.

Satz 4 konkretisiert die Voraussetzungen, unter denen die oder der IT-Bevollmächtigte ihr oder sein Einvernehmen verweigern kann. Oberstes Ziel ist es, die umfängliche Einführung der elektronischen Akte in Niedersachsen im vorgegebenen Umfang zu den Stichtagen einzuführen. Hierzu bedarf es einer Gesamtübersicht zwischen aller Ressorts, die durch die IT-Bevollmächtigte oder den IT-Bevollmächtigten als Schlüsselstelle gewährt werden soll. Sofern es sich lediglich um eine geringfügige, organisatorische Verzögerung handelt, soll das Einvernehmen nicht verweigert werden. Ebenso muss es Ausnahmemöglichkeiten geben, sofern berechtigte Umsetzungsprobleme bestehen. Dies kann auch nur im Interesse der jeweiligen Ressorts liegen, da sie ansonsten die unmittelbare Rechtsverpflichtung des Satzes 1 treffen würde.

Die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens erbat in ihrer Stellungnahme die Klarstellung, dass auch im übertragenen Wirkungskreis keine Verpflichtung zur elektronischen Aktenführung besteht. Dies ist grundsätzlich korrekt, aber nur in Bezug auf dieses Gesetz. Eine Verpflichtung über entsprechende spezialgesetzliche Regelungen hingegen wird nicht ausgeschlossen. Auch wenn der Nutzen der Digitalisierung sich erst bei einer medienbruchfreien Verarbeitung der Daten vollends einstellt, greift die Verpflichtung nur für Behörden des Landes.

Zu Absatz 3:

Satz 1 stellt klar, dass die Behörden auch bei der elektronischen Aktenführung die Grundsätze der ordnungsgemäßen Aktenführung einzuhalten haben. Diese folgen aus dem Rechtsstaatsprinzip, da nur eine geordnete Aktenführung einen rechtsstaatlichen Verwaltungsvollzug mit der Möglichkeit einer Rechtskontrolle durch Gerichte und Aufsichtsbehörden ermöglicht. Hieraus ergibt sich die Verpflichtung der öffentlichen Verwaltung, Akten zu führen (Gebot der Aktenmäßigkeit), alle wesentlichen Verfahrenshandlungen vollständig und nachvollziehbar abzubilden (Gebot der Vollständigkeit und Nachvollziehbarkeit) und diese wahrheitsgemäß aktenkundig zu machen (Gebot wahrheitsgetreuer Aktenführung). Umgekehrt folgen aus dieser Pflicht das grundsätzliche Verbot der nachträglichen Entfernung und Verfälschung von rechtmäßig erlangten Erkenntnissen und Unterlagen aus den Akten (Sicherung von Authentizität und Integrität) sowie das Gebot, den Aktenbestand langfristig zu sichern. Die ordnungsgemäße

Aktenführung muss durch geeignete technisch organisatorische Maßnahmen gemäß dem Stand der Technik sichergestellt werden. Die Klarstellung durch Satz 1 erleichtert die Gestaltung, den Einsatz und die Nutzung von E-Akte-Systemen. Eine umfassende Regelung der Aktenführung insgesamt wird hierdurch nicht vorgenommen.

Bei der elektronischen Aktenführung verdienen mehrere Grundsätze besondere Aufmerksamkeit. Die dauerhafte Lesbarkeit sichert die Archivierungsfähigkeit der Akten. Durch die Integritäts- und Authentizitätsverpflichtung sind Vorkehrungen dafür zu treffen, dass die elektronischen Akten manipulationssicher sowohl im Hinblick auf ihren Gesamtbestand als auch den Inhalt einzelner Dokumente gestaltet werden. Aufgrund der begrenzten Haltbarkeit der Trägermedien, der entsprechenden Lesegeräte oder Datenformate müssen die gespeicherten Informationen regelmäßig auf aktuelle Datenträger und aktuell gebräuchliche Datenformate übertragen werden, wobei sicherzustellen ist, dass die oben genannten Grundsätze stets eingehalten werden. Bei der Einführung der elektronischen Aktenführung muss darauf geachtet werden, alle Dokumente so zu speichern, dass die aktenrelevanten Informationen bei späteren Formatkonvertierungen erhalten bleiben. Gegebenenfalls muss der Import von Dokumenten in bestimmten Formaten verboten oder technisch unterbunden werden, wenn diese die oben genannten Anforderungen nicht erfüllen können. In Ausnahmefällen muss es auch möglich sein, Akten oder Aktenteile weiterhin in Papierform zu führen. Diese Ausnahmen werden in Satz 2 geregelt. Hierunter sind vor allem solche Bereiche zu subsumieren, in denen aufgrund des Beweiswertes eine Papierakte geführt werden muss, insbesondere, wenn es sich z. B. um Urkunden handelt, deren Beweiswert in elektronischer Form deutlich abnimmt. Ein unverhältnismäßiger Aufwand ist hingegen nicht bereits dann anzunehmen, wenn überhaupt eine umfangreiche Digitalisierung erfolgen soll. Vielmehr sind solche Fälle umfasst, in denen aufgrund besonderer Formate (Größe, Form, etc.) eine Digitalisierung nur mithilfe von speziellen Geräten erfolgen kann.

Zu Absatz 4:

Satz 1 beschreibt die Pflicht der Behörden, auch untereinander Akten grundsätzlich elektronisch zu übermitteln. Hierdurch sollen vor allem die Kommunikation der Behörden untereinander beschleunigt und Medienbrüche vermieden werden. Die Norm ist zwar als Soll-Vorschrift konzipiert, da es gegebenenfalls nicht immer möglich ist, den Austausch elektronisch abzuwickeln, sie ist aber grundsätzlich als Verpflichtung zu verstehen. Die Vorgabe gilt sowohl behördenintern als auch zwischen Behörden.

Satz 2 enthält eine Ermächtigung, technische Verfahren und Standards durch Verordnung zu regeln. Dies können zum einen Standards sein, die die automatisierte Verarbeitung der ausgetauschten Daten erleichtert, etwa XÖV-Standards wie XDOMEA oder zukünftige Weiterentwicklungen dieses Standards. Zum anderen können so auch Transportstandards festgelegt werden, die besondere Anforderungen an die Authentizität oder die Vertraulichkeit erfüllen. Die Justizverwaltung hat z. B. EGVP oder das besondere Behördenpostfach (beBPo) entwickelt, das den OSCI-Standard berücksichtigt und für den authentischen Datenaustausch zwischen Behörden und der Justizverwaltung geeignet ist. EGVP oder beBPo könnten per Verordnung als Austauschstandard zwischen den niedersächsischen Behörden insgesamt festgelegt werden.

Diese Verordnungsermächtigung soll nach Ansicht der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens auf den Austausch zwischen Behörden beschränkt werden. Dem wurde nachgekommen, da der Austausch innerhalb der Behörden diesen selbst überlassen bleiben kann.

Zudem nimmt der IT-Planungsrat gemäß Artikel 91 c Abs. 2 des Grundgesetzes in Verbindung mit § 1 Abs. 3 des Gesetzes über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91 c Absatz 4 des Grundgesetzes – bundesweite Koordinierungs- und Standardisierungsaufgaben wahr. Sofern hier Beschlüsse zu Austauschverfahren ergehen, sind diese in der Verordnung zu berücksichtigen.

Wie von der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens erbeten, ist der zügige Erlass der Verordnung beabsichtigt.

Zu Absatz 5:

Absatz 5 regelt das Verfahren der Akteneinsicht hinsichtlich elektronischer Akten. Die Anpassung an das Landesrecht ist marginal, sodass auf die Begründung des Bundesgesetzes abgestellt werden kann. Diese lautet wie folgt (BT-Drs. 17/11473, S. 39 f):

> *„Die Vorschrift regelt Art und Weise der Akteneinsicht und schafft kein eigenes Akteneinsichtsrecht.*
>
> *Das Recht auf Akteneinsicht ist Bestandteil des rechtsstaatlichen fairen Verwaltungsverfahrens und ergibt sich aus dem grundrechtlich verbürgten Anspruch auf rechtliches Gehör. Der Umfang des Akteneinsichtsrechts darf nicht vom Medium abhängig gemacht werden, dessen sich die Behörde zur Führung der Akte bedient. Soweit die allgemeinen Voraussetzungen an die Gewährung der Akteneinsicht gegeben sind bzw. eine solche überhaupt vorgesehen ist, muss also die Einsicht in die elektronische Akte im gleichen Umfang ermöglicht werden wie bei der Papierakte. Es gelten aber auch die gleichen Grenzen (z. B. sind geheimhaltungsbedürftige Informationen auszuklammern).*
>
> *Über die Art und Weise der Erteilung der Akteneinsicht hat die Behörde nach pflichtgemäßem Ermessen zu entscheiden.*

Dabei muss die Behörde darauf achten, auch weniger technikaffine Bevölkerungsgruppen nicht auszuschließen. In diesem Fall können z. B. Papierausdrucke gefertigt werden. Auch kann die Behörde dem Begehrenden einen elektronischen Zugriff auf dem Bildschirm in den Behördenräumen ermöglichen. Hierbei sind im pflichtgemäßen Ermessen der Behörde liegende Vorkehrungen zu treffen, die sicherstellen, dass der Begehrende nur von den für ihn bestimmten Informationen Kenntnis erlangen kann und Manipulationen ausgeschlossen sind. Erforderlichenfalls sind die ihn betreffenden Teile zu extrahieren. Daneben ist auch die Zurverfügungstellung des Inhalts der elektronischen Akte mittels Datenträger oder über E-Mail-Versand zulässig.

Bei der elektronischen Übermittlung ist den Erfordernissen des § 9 BDSG Rechnung zu tragen, insbesondere ist zu gewährleisten, dass die Integrität und Authentizität der Daten sichergestellt und deren Inhalte nicht unbefugt zur Kenntnis genommen und nicht missbräuchlich verwendet werden können.

Der elektronische Zugriff auf den Akteninhalt stellt eine zukunftsträchtige, wenngleich technisch derzeit aufwändige Form der Aktenübermittlung dar. Sie ist in der Rechtsordnung bereits in § 299 Absatz 3 ZPO sowie § 100 Absatz 2 VwGO eröffnet und soll auch außerhalb gerichtlicher (Verwaltungs-)Verfahren genutzt werden können."

Abweichend von der Begründung des E-Government-Gesetzes ist der Artikel 32 DSGVO maßgeblich.

Die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens schlägt vor, den Aktenausdruck als mögliche Einsichtnahme nicht mit aufzuführen. Das Akteneinsichtsrecht stellt ein hohes Gut dar. Der Zugang hierzu muss niedrigschwellig möglich sein. Der Forderung kann daher nicht nachgekommen werden. Solange nicht sichergestellt ist, dass durch eine hohe Interoperabilität die Einsichtnahme stets möglich ist, muss auch die Möglichkeit des Einblicks in einen Ausdruck erhalten bleiben.

Zu § 11 (Übertragen und Vernichten von Dokumenten in Papierform):

Zu Absatz 1:

Diese Norm gilt für alle Behörden des Landes, sofern sie ihre Akten elektronisch führen und nicht spezielle Gesetze vorgehen. Die Landesbehörden sollen nach Satz 1 anstelle von Dokumenten in Papierform oder in anderer körperlicher Form (wie z. B. Röntgenaufnahmen, Filmaufnahmen oder Ähnliches) diese als elektronische Wiedergabe in der elektronischen Akte speichern. Da die sonstigen Behörden durch dieses Gesetz nicht zur Führung einer elektronischen Akte verpflichtet werden, werden zur Übertragung von Dokumenten durch dieses Gesetz - anders als von der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens erbeten - keine Vorgaben gemacht. Die Regelungen zur Übertragung obliegen den sonstigen Behörden im Rahmen ihrer Organisationshoheit.

Dies soll die Anwendbarkeit der elektronischen Akte fördern, da andernfalls ein Nebeneinander von Papierakte und elektronischer Akte zu befürchten wäre. Die Möglichkeit einer Hybridakte für Dokumente, die aus besonderen Gründen nicht in die elektronische Form überführt werden können, bleibt davon unberührt und wird auch durch die Regelung in § 10 Abs. 3 Satz 2 erkennbar.

Behörden der Kommunen sowie der sonstigen Selbstverwaltung steht es im Rahmen ihrer Selbstverwaltung frei, wie mit Dokumenten und Akten nach der Digitalisierung verfahren werden soll. Im Rahmen der Förderung der elektronischen Akte wäre jedoch ein einheitliches Vorgehen wünschenswert.

Dem in § 11 geregelten „ersetzenden Scannen" wird auf dem Weg zur digitalen Verwaltung zunächst eine hohe, später aber eine deutlich geringere Bedeutung zukommen, weil in der digitalen Verwaltung der Empfang und Versand von Dokumenten oder Daten fast ausschließlich elektronisch erfolgen wird. Insofern sind die durch das Scannen entstehenden Aufwände zeitlich begrenzt.

Satz 2 legt die Anforderungen an die Übertragung von Papierdokumenten oder Dokumenten in anderer körperlicher Form in die elektronische Form fest. Zugleich werden damit auch Anforderungen an das Scanergebnis festgelegt, da das Scannen von Papierdokumenten Voraussetzung für ein medienbruchfreies Verwaltungsverfahren ist und künftig den Regelfall darstellen wird, was durch die „Soll"-Regelung in Satz 1 zum Ausdruck gebracht wird. Zur Sicherstellung der Übereinstimmung mit dem Papieroriginal ist eine vollständige Sichtprüfung aller digitalisierten Papierdokumente (Digitalisate) nicht erforderlich und praktisch auch nicht möglich. Die Behörde kann allerdings konkretisierende organisatorische Regelungen in einer internen Organisationsverfügung (etwa einer Scan-Anweisung) treffen.

Als Beispiel für den Stand der Technik kann die Technische Richtlinie „Rechtssicheres ersetzendes Scannen" (TR-RESISCAN) des Bundesamtes für Sicherheit in der Informationstechnik herangezogen werden. In dieser werden Anforderungen technisch-organisatorischer Art an Scanprozesse entwickelt, deren Einhaltung das Erstellen und die Anwendung möglichst rechtssicherer Scanlösungen ermöglicht. Die Begriffe „bildliche Übereinstimmung" und „inhaltliche" Übereinstimmung sind dort definiert. Diese Definition liegt auch der Verwendung der Begriffe in Satz 2 zugrunde. Gegenstand der Richtlinie sind Papieroriginale, die in einem sicheren Scanprozess so eingescannt werden können, dass trotz Vernichtung des Originals die damit einhergehende Minderung des Beweiswertes so gering wie möglich ist. Die TR-RESISCAN ist eine Richtlinie, die bei der praktischen Umsetzung in den Behörden verwendet werden kann. Das Niedersächsische Ministerium für Inneres und Sport plant darüber hinaus, eine Handreichung zu erstellen, in der aktuelle Hinweise zum ersetzenden Scannen gegeben werden. Hierdurch erhalten die Behörden

Anhaltspunkte, welche Verfahren dem geforderten „Stand der Technik" entsprechen. Die Handreichung soll dem niedersächsischen IT-Planungsrat mit dem Ziel vorgelegt werden, diese zu empfehlen.

Satz 3 regelt Ausnahmen vom Scannen. Soweit der Aufwand technisch unvertretbar hoch ist oder einen unverhältnismäßig großen Zeit-, Kosten- oder Personalaufwand erfordert, kann die Behörde von dem Grundsatz des Satzes 1 abweichen. Dies kann z. B. bei großen Formaten oder Röntgenbildern der Fall sein, die mit herkömmlichen Scan-Geräten nur unter erhöhtem Aufwand eingelesen werden oder an gängigen Bildschirmen nicht mehr sinnvoll bearbeitet werden können. Diese Regelung muss allerdings restriktiv angewendet werden, um den Zielen der digitalen Verwaltung dennoch Genüge zu tun.

Die Bestimmungen des § 11 beziehen sich nicht auf „Altbestände" von Papierakten. Alle Akten, die vor der Einführung der elektronischen Aktenführung nach § 10 Abs. 2 angelegt wurden, sind somit nicht nachzuerfassen. Sofern eine Nacherfassung aus anderen Gründen sinnvoll erscheint, ist diese aber durch die Regelung auch nicht ausgeschlossen. Ob eine Umwandlung von bereits vorhandenen Papierunterlagen in die E-Akte erfolgt, ist unter Berücksichtigung des Wirtschaftlichkeitsgebots und des weiteren Nutzens in das Ermessen der jeweiligen Behörde gestellt.

Die Anmerkungen der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens zur Begrenzung der Übertragung auf erforderliche Dokumente wurden aufgenommen.

Zu Absatz 2:

Absatz 2 beinhaltet die Ermächtigungsgrundlage für die Vernichtung der eingescannten Papierunterlagen nach ihrer Digitalisierung, sodass das Scanprodukt zur Grundlage der weiteren Bearbeitung gemacht werden kann. Dabei soll das ersetzende Scannen zum Regelfall des Umgangs mit Dokumenten werden.

Eine vorübergehende Aufbewahrung (in der Praxis dürften bis zu sechs Monate ausreichend sein) der Originaldokumente nach dem Scanvorgang in einer Zwischenablage der Behörde kann zum Zweck der „Qualitätssicherung" des Digitalisats zweckmäßig sein. Hierdurch können nachträgliche Korrekturen vorgenommen werden, falls trotz der technischen und organisatorischen Vorkehrungen für den Scanvorgang ein Dokument fehlerhaft, unvollständig oder unleserlich eingescannt worden sein sollte. Auch können Dokumente erhalten werden, wenn sich erst im Verlauf der Sachbearbeitung herausstellt, dass es auf die Originaleigenschaft ankommen könnte, etwa aus Beweisgründen. Die Dauer der Aufbewahrung von eingescannten Dokumenten sollten von der Behörde in einer Organisationsverfügung (etwa einer Scan-Anweisung) klargestellt werden, um für die betroffenen Bediensteten Klarheit und Rechtssicherheit zu schaffen.

Eine ausnahmslose Vernichtung des Papieroriginals ist aufgrund des Rechts auf effektiven Rechtsschutz nach Artikel 19 Abs. 4 des Grundgesetzes sowie aufgrund des im Rechtsstaatsprinzip verbürgten Justizgewährungsanspruchs nicht möglich. Hierzu zählt das Recht auf ein faires Verfahren, zu dem auch eine faire Handhabung des Beweisrechts gehört. Mit der ausnahmslosen Vernichtung der Originalurkunden würde in einzelnen Fällen dem Betroffenen die Möglichkeit genommen, den Urkundsbeweis ordnungsgemäß führen zu können. Durch den Scanvorgang entsteht nur ein zweidimensionales Abbild des Originals. Die forensischen Prüfungsmöglichkeiten, etwa im Hinblick auf die Echtheit einer handschriftlichen Unterschrift, sind gegenüber einem Originaldokument stark eingeschränkt. Zudem sind Privaturkunden grundsätzlich im Original vorzulegen, wenn der Urkundsbeweis greifen soll.

Ausnahmen von der grundsätzlichen Vernichtung des Papierdokuments greifen daher, wenn es für das Verfahren auf die Originaleigenschaft des Dokuments ankommt oder eine Vernichtung aus anderen Gründen ausgeschlossen ist.

Als solche Ausnahmetatbestände können in Betracht kommen:

- Ausschluss der Vernichtung durch eine (spezialgesetzliche) Vorschrift,
- eine nur für die Dauer der Bearbeitung vorübergehende Überlassung der Dokumente, die dann nicht in das Eigentum der Behörde übergehen und dem Absender entweder nach expliziter Erklärung oder aus den Umständen des Falles erkennbar zurückzugeben sind (z. B. bei Ausweispapieren, Originalverträgen),
- Urkunden, an denen die Verfahrensbeteiligten ein Beweisführungsrecht haben und bei denen es im Verfahren auf die Gewährung der Möglichkeit des Urkundsbeweises ankommen kann.

Eine Abweichung von der Soll-Vorschrift ist unter anderem auch gerechtfertigt

- bei kulturhistorisch wertvollen archivwürdigen Papierunterlagen oder
- wenn die Abgabe des Verfahrens an eine Behörde notwendig ist, die ihre Akten nicht elektronisch führt.

Einzelheiten sollten von der Behörde ebenfalls in einer Organisationsverfügung (etwa einer Scan-Anweisung) klargestellt werden.

Die Anbietungspflicht gegenüber dem Landesarchiv wird durch die spätere Anbietung der elektronischen Dokumente erfüllt. Insoweit handelt es sich lediglich um einen Wechsel des Mediums.

Die Ärztekammer erbittet in ihrer Stellungnahme ein früheres Inkrafttreten der Regelungen des § 11 Abs. 2. Mit dem Inkrafttreten dieser Regelung am Tag nach der Verkündung (Artikel 3 Abs. 2 Satz 1) wurde jedoch bereits der frühestmögliche Zeitpunkt gewählt.

Zu Absatz 3:

Entsprechend der Stellungnahme der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens wurde mit dem neuen Absatz 3 eine Ermächtigungsgrundlage für die Vernichtung oder Rückgabe der eingescannten Papierunterlagen nach ihrer Digitalisierung für Kommunen und sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts geschaffen. Sofern diese im Rahmen ihrer Organisationshoheit die Übertragung und Speicherung von Dokumenten in einer elektronischen Akte veranlassen, steht ihnen ebenfalls die Möglichkeit des ersetzenden Scannens offen. Allerdings ist eine ausnahmslose Vernichtung des Originals ebenfalls nicht möglich. Insoweit wird insbesondere auf die Ausführungen in Absatz 2 zum Recht auf effektiven Rechtsschutz nach Artikel 19 Abs. 4 des Grundgesetzes sowie auf den im Rechtsstaatsprinzip verbürgten Justizgewährungsanspruch verwiesen. Auch die Ausführungen zu weiteren möglichen Ausnahmetatbeständen gelten entsprechend.

Zu § 12 (Basisdienste):

Zu Absatz 1:

Das Land stellt durch das für die zentrale IT-Steuerung zuständige Ministerium den Behörden des Landes Basisdienste zur Verfügung. Durch Verortung im für zentrale IT-Koordinierung zuständigen Ministerium wird am besten sichergestellt, dass die Basisdienste aufeinander abgestimmt sind und etwaigen IT-Architekturvorgaben entsprechen. Dabei wird davon ausgegangen, dass in der Landesregierung jederzeit ein Ministerium bestimmt ist, das für die zentrale Koordination der Informationstechnik in der niedersächsischen Verwaltung zuständig ist. Zurzeit ist dies das Ministerium für Inneres und Sport.

Die Bereitstellung der Basisdienste durch das für zentrale IT-Steuerung zuständige Ministerium gilt darüber hinaus auch für die Kommunen und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Diese können mit Ausnahme der nach Absatz 3 verpflichtend zu nutzenden Basisdienste selbst entscheiden, ob sie die vom Land bereitgestellten Basisdienste nutzen möchten.

Der Begriff des Basisdienstes wird in den Begriffsbestimmungen (§ 1 Nr. 2) definiert.

Die Regelung führt dazu, dass die von diesem Gesetz geforderten Zugänge und digitalen Angebote über vom Land bereitgestellte Anwendungen angeboten werden, sodass aufeinander abgestimmte, kompatible Dienste entstehen können und der Aufwand für die Behörden des Landes so gering wie möglich ist. Im Einzelnen sind nach Satz 1 folgende Basisdienste bereitzustellen:

- ein einfacher elektronischen Zugang (z. B. E-Mail-Service),
- ein gesicherter Zugang über Nutzerkonten mit Postfachfunktion,
- ein De-Mail-Zugangssystem über einen De-Mail-Gateway,
- ein Service mit Identifizierungsfunktion (eID-Funktion) mithilfe des neuen Personalausweises (nPA),
- ein Behördeninformationssystem (z. B. BUS)
- ein Antragsverwaltungssystem und ein Formularservice,
- ein elektronisches Bezahlverfahren,
- ein E-Akte-System mit Vorgangsbearbeitungs- und Scansystem und
- ein IT-Verfahren zum Empfang und zur Verarbeitung von elektronischen Rechnungen.

Die ersten sieben aufgelisteten Basisdienste bilden die Grundlage für das niedersächsische Verwaltungsportal. Das für zentrale IT-Steuerung zuständige Ministerium hat für die Bereitstellung dieser Dienste zu sorgen, dies muss aber nicht kostenfrei geschehen, soweit dies nicht ausdrücklich geregelt ist. Insbesondere der Betrieb der Basisdienste kann durch Entgelte gegenfinanziert werden. Dabei muss das für zentrale IT-Steuerung zuständige Ministerium für wirtschaftliche Lösungen sorgen. Die folgenden Tabellen geben einen Überblick über die Verpflichtungen im Zusammenhang mit den normierten Basisdiensten.

Nach Satz 2 wird zudem ein Basisdienst für die Georeferenzierung durch das für Geoinformation zuständige Ministerium bereitgestellt. Durch die Georeferenzierung auf der Grundlage der Angaben des amtlichen Vermessungswesens (Geobasisdaten) kann einem Ort, einer Straße, einem Grundstück oder einer raumbezogenen Fachinformation eine Koordinate zugeordnet werden. Damit wird gewährleistet, dass raumbezogene Sachverhalte in Beziehung zueinander gesetzt, analysiert und visualisiert werden können. Einheitliche Vorgaben für die Georeferenzierung sind die grundlegende Voraussetzung für die Interoperabilität der Geodaten, auch im Sinne einer Geodateninfrastruktur Deutschland (GDI-DE). Die Nutzung des Geokodierungsdienstes ist für die Behörden des Landes, der Kommunen und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen kostenfrei.

Verpflichtungen aus den §§ 4, 5, 6, 9, 10 und 12 für Behörden des Landes			
IT-Verfahren	**Verpflichtung**	**Bereitstellung Basisdienst**	**Verpflichtung Nutzung Basisdienst**
einfacher Zugang, z. B. E-Mail (ggf. qeS)	Zugangseröffnung, § 4 Abs. 1, Satz 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1	verpflichtend, § 12 Abs. 2 Satz 1
Nutzerkonto	Zugangseröffnung, § 4 Abs. 2, Satz 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1	verpflichtend, § 12 Abs. 2 Satz 1
De-Mail	Zugangseröffnung, § 4 Abs. 3;	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1	verpflichtend, § 12 Abs. 2 Satz 1
Identifizierung mit nPA	Identifizierung, § 4 Abs. 4	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 2	verpflichtend, § 12 Abs. 2 Satz 1
BUS (Allgemein)	Info-Bereitstellung, § 5 Abs. 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 3	verpflichtend, § 12 Abs. 2 Satz 1
BUS (Leistungsbeschreibung) mit Formularserver	Info-Bereitstellung, § 5 Abs. 2	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 3	verpflichtend, § 12 Abs. 2 Satz 1
Antragsverwaltungssystem	Verfahren bereitstellen, § 5 Abs. 5	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 3, 4	verpflichtend, § 12 Abs. 2 Satz 1
Elektronisches Bezahlverfahren	Bereitstellung, § 6 Abs. 1 und 2	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 5	verpflichtend, § 12 Abs. 2 Satz 1
E-Rechnung	Empfang und Verarbeitung ab 18. April 2020, § 6 Abs. 3	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 6	verpflichtend, § 12 Abs. 2 Satz 1
Georeferenzierung	Angabe von Koordinaten nach § 9	Durch das für Geobasisdaten zuständige Ministerium, § 12 Abs. 1 Satz 2	verpflichtend, § 12 Abs. 2 Satz 1
Elektronische Aktenführung	Stufenweise bis flächendeckende Einführung ab 1. Januar 2026, § 10 Abs. 2	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 7	verpflichtend, § 12 Abs. 2 Satz 1

Verpflichtungen aus den §§ 4, 5, 6, 9, 10 und 12 für Kommunen und sonstigen Aufsicht des Landes unterstehenden juristischen Personen			
IT-Verfahren	**Verpflichtung**	**Bereitstellung Basisdienst**	**Verpflichtung Nutzung Basisdienst**
einfacher Zugang, z. B. E-Mail (ggf. qeS)	Zugangseröffnung, § 4 Abs. 1 Satz 1		
Nutzerkonto	Zugangseröffnung, § 4 Abs. 2 Satz 1	durch IT-Ministerium, kostenfrei § 12 Abs. 3 Satz 2	verpflichtend, § 12 Abs. 3 Satz 1
De-Mail	Zugangseröffnung, § 4 Abs. 3		
Identifizierung mit nPA			
BUS (Allgemein)	Info-Bereitstellung, § 5 Abs. 1	durch IT-Ministerium, kostenfrei § 12 Abs. 3 Satz 2	verpflichtend, § 12 Abs. 3 Satz 1
BUS (Leistungsbeschreibung) mit Formularserver	Informationsbereitstellung, § 5 Abs. 2	durch IT-Ministerium, kostenfrei § 12 Abs. 3 Satz 2	verpflichtend, § 12 Abs. 3 Satz 1

Verpflichtungen aus den §§ 4, 5, 6, 9, 10 und 12 für Kommunen und sonstigen Aufsicht des Landes unterstehenden juristischen Personen			
IT-Verfahren	**Verpflichtung**	**Bereitstellung Basisdienst**	**Verpflichtung Nutzung Basisdienst**
Antragsverwaltungssystem	Verfahren bereitstellen, § 5 Abs. 5	durch IT-Ministerium, kostenfrei § 12 Abs. 3 Satz 2	
Elektronisches Bezahlverfahren	Bereitstellung, § 6 Abs. 1 und 2	durch IT-Ministerium, § 12 Abs. 3 Satz 3	
E-Rechnung	Empfang und Verarbeitung ab 18.04.2020, § 6 Abs. 3		
Georeferenzierung	Angabe von Koordinaten nach § 9	Durch das für Geobasisdaten zuständige Ministerium, § 12 Abs. 1 Satz 2	verpflichtend, § 12 Abs. 3 Satz 1
Elektronische Aktenführung			

Gemäß Satz 3 ist auch die Nutzung anderer Basisdienste für Funktionen nach Absatz 1 Sätze 1 und 2 möglich, wenn die oder der IT-Bevollmächtigte des Landes ihr oder sein Einvernehmen erteilt hat. Grund für die Notwendigkeit der Erteilung des Einvernehmens ist die Herstellung einer einheitlichen Landschaft an Basisdiensten. Zudem muss sichergestellt sein, dass ein Lagebild über die vorhandenen Basisdienste im Land an zentraler Stelle vorliegt. Das Einvernehmen ist vor allem erforderlich, um auszuschließen, dass ein unwirtschaftliches Nebeneinander von inhaltsgleichen Basisdiensten besteht und um einen Überblick über die vom Land aufgesetzten Basisdienste zu erhalten und fortzuschreiben. Sinnvolle fachbezogene Basisdienste sind möglicherweise derzeit z. B. das elektronische Gerichts- und Verwaltungspostfach (EGVP) oder beA und beBPo der Justizverwaltung oder das Identifizierungsverfahren der Steuerverwaltung im Rahmen von ELSTER. Beide Verfahren sind im jeweiligen Fachbereich bundesweit etabliert und daher dort sinnvollerweise weiter zu nutzen. Ebenso stellen die durch die Verordnung (EU) Nr. 907/2014 definierten besonderen Anforderungen an die EU-Zahlstelle bei der Durchführung von Fördermaßnahmen mit europäischer Finanzbeteiligung oder der Zahlungen im Rahmen der Gemeinsamen Agrarpolitik (GAP) ein solches fachbezogenes Verfahren dar. Auch dieses kann im Einvernehmen mit der oder dem IT-Bevollmächtigten weiterbetrieben werden und von der verpflichtenden Nutzung der Basisdienste ausgenommen werden.

Es wird angestrebt, alle Basisdienste in eine Gesamtstrategie mit dem Ziel einzubinden, diese nach Möglichkeit interoperabel zu gestalten oder zu vereinheitlichen.

Satz 4 konkretisiert sodann, unter welchen Voraussetzungen die oder der IT-Bevollmächtigte ihr oder sein Einvernehmen verweigern kann. Dies korrespondiert mit ihrem oder seinem Einvernehmen nach Absatz 2 Satz 3.

Satz 5 macht deutlich, dass die Bereitstellung von Basisdiensten nicht durch das zuständige Ministerium selbst geschehen muss. Es besteht vielmehr die Möglichkeit, dass hiermit z. B. der IT-Dienstleister des Landes beauftragt wird. Im Rahmen der Zusammenarbeit mit den Kommunen oder dem Bund und anderen Ländern kann es auch sein, dass das zuständige Ministerium einen Basisdienst z. B. durch eine kommunale Datenzentrale oder das Rechenzentrum eines anderen Landes bereitstellen lässt. Weiterhin ist es möglich, dass das zuständige Ministerium für diese Aufgabe einen Auftragsverarbeiter einbindet (Artikel 28 DSGVO). Das zuständige Ministerium hat für die jeweilige Entscheidung vor allem wirtschaftliche, vergaberechtliche und IT-strategische Gründe zu berücksichtigen.

Zu Absatz 2:

Absatz 2 sieht für die Verpflichtungen, die sich aus § 4, § 5 Abs. 1 und 2, § 6, § 9 sowie § 10 Abs. 2 ergeben, die verpflichtende Nutzung der Basisdienste des Landes für die Behörden des Landes vor. Dies bedeutet, dass diese grundsätzlich zu nutzen sind.

Für die Verpflichtungen, die sich aus § 4 ergeben, sind also die Basisdienste „einfacher elektronischer Zugang (z. B. E-Mail-Server)“, „gesicherter Zugang über Nutzerkonten mit Postfachfunktion“, „De-Mail-Zugangssystem über eine De-Mail-Gateway“ und „Service mit Identifizierungsfunktion (eID-Funktion) mithilfe des neuen Personalausweises“ zu nutzen.

In Niedersachsen wurde als zentrale Plattform das Serviceportal Niedersachsen geschaffen, integriert ist dort der BUS. Dieser stellt einen Basisdienst für die Verpflichtungen dar, die sich aus § 5 Abs. 1 und 2 ergeben. Beim BUS handelt es sich um ein zentrales IT-Verfahren, in der Leistungsbeschreibungen, Informationen zu zahlreichen niedersächsischen Kommunen sowie notwendige Unterlagen und Anträge in elektronischer Form hinterlegt sind.

Diese Struktur soll genutzt und manifestiert werden, Doppelstrukturen sollen allein schon aus Kostengründen vermieden werden. Auch der Aufwand für die Pflege und die Aktualisierung ist weniger aufwändig, wenn diese nur an einer Stelle durchgeführt werden müssen. Zudem sind die obersten Landesbehörden in die Bearbeitung eingebunden, sodass eine einheitliche, koordinierte und stetige Aktualisierung stattfindet. Die einheitliche Struktur, die durch die verbindliche Nutzung manifestiert wird, sorgt in einem besonders hohen Maße für ein bürgerfreundliches Auftreten.

Aus Absatz 3 ergibt sich für die Behörden des Landes unter anderem auch die Verpflichtung zur Nutzung des Basisdienstes „elektronisches Bezahlverfahren“. Für erste elektronische Verfahren ist bereits eine produktive Lösung im Einsatz, die auch für den einfachen und kostensparenden Einsatz in weiteren Verfahren geeignet ist.

Ebenso ergibt sich aus Absatz 2 Satz 1 die Verpflichtung, den Basisdienst für den Empfang und die Verarbeitung von elektronischen Rechnungen zu nutzen. Dieser Dienst muss noch realisiert werden. Idealerweise unterstützt der Dienst die vollständige Rechnungsbearbeitung bis zur Übergabe an das Haushaltswirtschaftssystem. Zwingend erforderlich ist dies aber nicht. Auch von dieser Nutzungsverpflichtung können Ausnahmen zugelassen werden.

Schließlich sieht Absatz 2 die Verpflichtung vor, einen zentral bereitgestellten E-Akte-Basisdienst einzusetzen. Bereitstellung, Support und Fortentwicklung von E-Akte-Systemen sind mit hohen Aufwänden verbunden. Diese lassen sich durch ein zentral bereitgestelltes System erheblich reduzieren. Auf diese Weise verringert sich auch der Schulungsaufwand bei Personalwechsel zwischen den Behörden des Landes, der System-Anpassungsaufwand beim Austausch von Dokumenten zwischen Behörden sowie die Vorgangsbearbeitung bei behördenübergreifenden Zeichnungsprozessen. In der Landesverwaltung gibt es bereits seit Längerem ein zentrales E-Akte-Einführungsprojekt. Hieraus kann der geforderte Basisdienst hervorgehen. Nur in Ausnahmefällen können andere IT-Systeme für konkrete Aufgaben zur Aktenführung eingesetzt werden. Ein Ausnahmefall kommt in Betracht, wenn technische oder rechtliche Gründe vorliegen oder die Behörde des Landes bereits ein System zur elektronischen Akten-führung einsetzt. Im letzteren Fall müsste nachgewiesen werden, dass das neue System für die Behörde ungeeignet oder unwirtschaftlich ist. Der E-Akte-Basisdienst, der vom für zentrale IT-Steuerung zuständigen Ministerium bereitgestellt wird, sollte mit den vorhandenen Systemen kompatibel sein, sodass auch mit den anderen Systemen ein Austausch möglich ist. Der Basisdienst muss so gestaltet sein, dass er die Anforderungen an eine elektronische Aktenführung erfüllt. Er sollte nicht nur über ein geeignetes Ablagesystem verfügen, sondern z. B. auch die Vorgangsbearbeitung, die Aufbewahrung nach Schließung der Akten und die Aussonderung unterstützen. Dabei kann der Basisdienst modular aufgebaut sein.

Satz 2 sieht die Möglichkeit vor, dass die sich aus den §§ 4, 5 Abs. 1 und 2, §§ 6, 9 sowie 10 Abs. 2 ergebenden Verpflichtungen auch über andere Basisdienste oder fachbezogene informationstechnische Verfahren erfüllt werden können, sofern das Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung hergestellt worden ist. Das Einvernehmen kann verweigert werden, wenn die Zweckmäßigkeit oder die Wirtschaftlichkeit nicht erkennbar ist. Es muss also mindestens einer der beiden Kriterien erfüllt sein. Diese Möglichkeit soll dem Umstand Rechnung tragen, dass es Bereiche gibt, in denen Fachanwendungen schon fest implementiert sind und ein Zurückgreifen auf die Basisdienste, die für das gesamte Land Anwendung finden sollen, wenig zielfördernd oder für die Bürgerinnen und Bürger verwirrend wäre. Zudem können so fachspezifische Notwendigkeiten, die sich z. B. aus der Abstimmung im Länderverbund ergeben, beachtet und gegebenenfalls auch kostengünstiger implementiert werden.

Zu Absatz 3:

Die Kommunen und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts haben nach § 4 Abs. 2 einen Zugang auch über Nutzerkonten anzubieten. Entsprechend dem Wunsch der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens wird klargestellt, dass es den Kommunen unbenommen ist, weiterhin einen Zugang über andere Möglichkeiten zu eröffnen. Jedoch bedarf es zur Umsetzung des Onlinezugangsgesetzes eines einheitlichen Nutzerkontos. Außerdem sind sie nach § 5 verpflichtet, allgemeine, sie betreffende Informationen (Absatz 1) sowie weitere Informationen über öffentlich zugängliche Netze (Absatz 2) bereitzustellen. Satz 1 sieht vor, dass diese Bereitstellungen über Basisdienste des Landes zu erfolgen haben. Eine Verbindung der IT-Systeme mit dem Landesdatennetz ist hierfür nicht erforderlich. Diese Vorgabe setzt die Verpflichtungen nach § 1 Abs. 1 OZG und § 3 Abs. 2 um. Sie soll sicherstellen, dass ein interoperables Nutzerkonto sowie ein einheitlicher und bürgerfreundlicher BUS vom Land zur Verfügung gestellt werden kann, in dem die Kommunen und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts mindestens mit Basisinformationen aufgelistet sind. Die Vorgabe gegenüber den Kommunen und sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts stellt auch einen verhältnismäßigen Eingriff in die Selbstverwaltung dar. Mit der Verpflichtung zur Nutzung des Basisdienstes des Landes zur Umsetzung des § 5 Abs. 1 dient dazu eine Zersplitterung zu vermeiden. Auch greift die Verpflichtung nur gering in das Recht auf Selbstverwaltung ein, da es lediglich um die Bereitstellung von Informationen an dieser Stelle geht.

Idealerweise nutzen die Kommunen auch weitere Basisdienste des Landes. Um diese Nutzung zu unterstützen, verpflichtet Satz 2 das für zentrale IT-Steuerung zuständige Ministerium, den Kommunen und den sonstigen der

Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts bestimmte Basisdienste kostenfrei zur Verfügung zu stellen. Die Behörden können diese nutzen, müssen es aber nicht. Mit Rücksicht auf die Organisationshoheit der Kommunen wird hier auf eine Verpflichtung verzichtet.

Auch zur Erfüllung der Verpflichtungen nach § 4 Abs. 2 und § 5 Abs. 2 Satz 1 sowie Abs. 5 werden durch das Land Basisdienste zur Verfügung gestellt. Diese Basisdienste werden kostenfrei angeboten, um die Kommunen von Aufwänden zu entlasten. Die Kommunen haben somit einen Anspruch, diese Basisdienste kostenfrei zu nutzen. Die Basisdienste müssen dafür geeignet sein, die hiermit verbundenen Verpflichtungen zu erfüllen. Die konkrete Ausgestaltung der Basisdienste ist allerdings nicht gesetzlich geregelt und kann vom für zentrale IT-Steuerung zuständigen Ministerium festgelegt werden. Zum Beispiel muss der Formularservice die Bereitstellung aller elektronischen Formulare ermöglichen, die die Kommunen anbieten möchten. Das für zentrale IT-Steuerung zuständige Ministerium muss diese aber nicht auf eigene Kosten erstellen lassen, was insbesondere bei individuellen Formularen einzelner Kommunen mit einem erheblichen Finanzierungsaufwand verbunden wäre. Zudem kann das für zentrale IT-Steuerung zuständige Ministerium festlegen, in welchem Format die Formulare eingestellt werden sollen. Auch die Schnittstellen zu eigenen Verfahren der Kommunen müssen von diesen selbst finanziert werden.

Die Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens merkt in ihrer Stellungnahme an, dass die Regelungen zu den notwendigen Formularen nicht ausreichend gefasst seien. Es wird nunmehr klargestellt, dass keine Verpflichtung zur Nutzung der Formulare, die durch das Land bereitgestellt werden, besteht. Zudem wird klargestellt, dass der einzurichtende Basisdienst für Formulare nunmehr ebenfalls von den Kommunen kostenfrei genutzt werden kann. Sofern andere Dienste genutzt werden, müssen diese zur Erfüllung der Vorgaben des Onlinezugangsgesetzes mit dem Verbundportal kompatibel ausgestaltet und nutzbar sein.

Die übrigen Basisdienste können, wie oben bereits ausgeführt, von den Kommunen und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts ebenfalls gemäß § 12 Abs. 1 genutzt werden. Ob sie dieses Angebot nutzen möchten, obliegt ihnen im Rahmen ihrer Organisationshoheit.

Die Kritik der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens zur Regelung von marktüblichen Qualitätsstandards sowie Service- und Nutzungsregelungen bei der Nutzung von Basisdiensten ist bekannt und wird sehr ernst genommen. Im Rahmen der Neugestaltung der Dienste müssen diese Anforderungen berücksichtigt und die Vorgehens- und Umsetzungsweise optimiert werden.

Zu Absatz 4:

Absatz 4 enthält eine Verordnungsermächtigung für die Landesregierung. Nach Nummer 1 kann die Landesregierung per Verordnung bestimmen, dass weitere Basisdienste mit einer Nutzungsverpflichtung belegt werden können und Verpflichtungen zur Bereitstellung zur Nutzung geregelt werden können, um flexibel die vorhandenen Basisdienste weiterzuentwickeln und die Nutzung weiterer Basisdienste verpflichtend auszugestalten oder eine Nutzung selbiger zuzulassen. Es ist derzeit nicht absehbar, welche technischen Neuheiten es geben wird und wo Bedarf für weitere Basisdienste bestehen wird, sodass eine flexible Handhabung erforderlich ist.

Nummer 2 ermöglicht die weitere Ausgestaltung der Basisdienste im Wege einer Verordnung. Insofern können nach Buchstabe a Standards hinsichtlich der Interoperabilität und der Informationssicherheit festgelegt werden. Dies muss im Wege einer Verordnung geschehen, um auf die unter Umständen sehr kurzfristigen Anforderungen reagieren zu können.

Nach Buchstabe b sollen Regelungen zu Anforderungen an die Qualitätssicherung getroffen werden können. Hierdurch wird die Verlässlichkeit der Dienste erhöht, sodass die nutzenden Behörden ein hohes Maß an Sicherheit haben, ihre Aufgaben mithilfe der Basisdienste zuverlässig zu erfüllen.

Die Buchstaben c und d schaffen die Basis für eine konkretere und präzisere Beschreibung der Funktionen der Basisdienste sowie für Regeln zur damit verbundenen Verarbeitung personenbezogener Daten. Zudem kann die Nutzung der Basisdienste geregelt werden. Damit können einerseits Bedingungen für deren Nutzung normiert werden. Andererseits kann es notwendig werden, die Modalitäten der Weiterentwicklung auch im Zusammenwirken mit den Kommunen verbindlich zu regeln.

Bei Erlass der Verordnung sind die Beschlüsse des IT-Planungsrates jeweils zu berücksichtigen.

Zum Dritten Teil (IT-Sicherheit):

Die Nutzung von IT-Systemen, insbesondere die Kommunikation über das Internet, durchdringen die Gesellschaft zwischenzeitlich fast vollständig. Auch staatliches Handeln, insbesondere die Funktionsfähigkeit der Exekutive, ist heute ohne eine funktionierende Informationstechnologie erheblich beeinträchtigt. Die Verwaltung kommuniziert überwiegend per E-Mail, nutzt vermehrt Voice-Over-IP-Technologien und verarbeitet die zur Aufgabenerledigung erforderlichen Daten von Bürgerinnen und Bürgern auf ihren IT-Systemen.

Die starke Fokussierung auch der Verwaltung auf die IT-unterstützte Aufgabenerledigung birgt allerdings auch Gefahren. Angriffe auf Informations- und Kommunikationsinfrastrukturen sind in den letzten Jahren immer zahlreicher und komplexer geworden; gleichzeitig ist eine zunehmende Professionalisierung der Angreifer zu verzeichnen. So hat sich sogenannte „Ransomware“, das heißt Software, welche die Daten der betroffenen Computer durch eine

Verschlüsselung von Dateien angreift, die nur durch Zahlung eines Lösegeldes entschlüsselt werden können und damit zum Gegenstand einer Erpressung gemacht werden, stark verbreitet. Eine Weiterentwicklung ist das Kapern fremder Rechner, um Internetwährungen zu schürfen, ohne dabei die dafür erforderlichen hohen Rechenkapazitäten und Energiemengen bereitstellen zu müssen. Der angestrebte monetäre Ertrag ergibt sich nun unmittelbar, ohne erforderliche Mitwirkung des Opfers bei der Erpressung. Die Beispiele belegen, dass die Angriffe immer ausgefeilter werden und sich Cyberkriminelle längst von wirtschaftlichen Interessen leiten lassen.

Daneben werden wiederholt sogenannte „Advanced Persistent Threats“ (APT) registriert: komplexe, zielgerichtete und mit großem Wissen und Aufwand durchgeführte, möglichst unbemerkte Angriffe, um über einen längeren Zeitraum sensible Informationen auszuspähen oder anderweitig Schaden anzurichten. Bekannte Beispiele sind der Angriff auf die IT des Deutschen Bundestages 2015 sowie auf den Informationsverbund der Bundesregierung, der zum Jahreswechsel 2017/2018 bekannt wurde.

Wegen des globalisierten Datenaustausches haben nationalstaatliche Grenzen für Angriffe aus dem Cyberraum keine Bedeutung, sodass sich auch die Verwaltungen der Länder auf weltweite Angriffe einzustellen haben. Dabei bieten die Offenheit und Ausdehnung des Cyber-Raums den Angreifern mannigfaltige Möglichkeiten, ihre Identität durch besondere Techniken (z. B. die Nutzung von Tor-Netzwerken oder Bot-Netzwerken) zu verschleiern. Gegenüber den von technisch sehr versierten Experten entwickelten Schadprogrammen sind die Abwehr- und Rückverfolgungsmöglichkeiten sehr begrenzt, sodass bei Angriffen häufig weder auf die Identität noch auf die Hintergründe des Angreifers geschlossen werden kann.

Insoweit besteht eine Gefahr. Der Zweck des Dritten Teils zielt auf die Abwehr dieser Gefahr ab und dient neben der Gewährleistung der Funktionsfähigkeit der Verwaltung auch dem Schutz der von den Bürgerinnen und Bürgern auf den IT-Systemen des Landes gespeicherten Daten und der Gewährleistung der Vertraulichkeit der Kommunikation zwischen Bürgerinnen, Bürgern und Staat und damit der Gewährleistung des Grundrechtsschutzes der Bürgerinnen und Bürger.

Zum Erkennen und zur Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme oder Angriffe ist der Einsatz von den Systemen: „Intrusion Detection System“ (IDS) und „Security Incident and Event Management“ (SIEM)-Systems erforderlich.

Bei IDS handelt es sich um IT-Systeme, die den Einbruch in andere IT-Systeme erkennen sollen. Ein Einbruch in ein IT-System liegt vor, wenn sich eine Person unberechtigt Zugriff zu einem IT-System verschafft. IDS sollen bestehende Sicherheitsmaßnahmen zur Verhinderung von Einbrüchen (sogenannte Intrusion Prevention) flankieren (und keinesfalls ersetzen), da allgemein davon ausgegangen wird, dass es keine zu 100 % sicheren Systeme gibt, mithin also immer damit gerechnet werden muss, dass ein Angreifer auch in geschützte Systeme eindringen kann. Es werden zwei Arten von IDS unterschieden: anomaliebasierte Systeme, die auf Basis eines festgelegten (oder festgestellten) tatsächlichen Verhaltens (sogenannte „baseline“) der Subjekte eines IT-Systems (z. B. Nutzer, Computersysteme, Netzwerkkomponenten) Auffälligkeiten als signifikant für das Vorliegen eines Einbruchs heranziehen, und Systeme, die auf der Erkennung von bekanntem, missbräuchlichem Verhalten (sogenannte „pattern“) basieren. Beiden Ansätzen ist immanent, dass sie zur Erkennung auf Daten der bestehenden IT-Systeme Zugriff haben müssen. Ein IDS, dessen Betriebszweck die Erzeugung sicherheitsrelevanter Ereignisse ist, kann insoweit eine Datenquelle für ein SIEM-System darstellen.

Bei SIEM-Systemen handelt es sich um Systeme, die einerseits eine Echtzeitanalyse von sicherheitsrelevanten Ereignissen ermöglichen, die beim Betrieb von IT-Systemen und den darauf betriebenen Computerprogrammen einschließlich des Betriebssystems und seiner Dienste – in der Regel in Protokolldateien (sogenannte „log files“) – anfallen und gespeichert werden und andererseits durch die Speicherung der Ereignisse über einen längeren Zeitraum die Möglichkeit für eine Analyse eröffnen (z. B. von sich verändernden Angriffsverhalten und der Ermittlung neuer Angriffsvektoren), welche typischerweise Gegenstand eines regelmäßigen Berichtswesens an die für die Informationssicherheit einer Organisation verantwortlichen Führungskräfte ist.

Der Deutsche Gewerkschaftsbund Bezirk Niedersachsen – Bremen – Sachsen-Anhalt sieht ebenfalls die Notwendigkeit der Analyse verschlüsselter Daten (§ 20), warnt jedoch vor der Missbrauchsgefahr durch die Speicherung von IP-Adresse und Zugriffszeitpunkt. Insoweit wird die starke Zweckbindung des § 18 Abs. 3 begrüßt.

Die Deutsche Rentenversicherung Braunschweig-Hannover erbittet in ihrer Stellungnahme die Ausnahme vom Anwendungsbereich des Dritten Teils. Da der Dritte Teil lediglich eine Befugnis darstellt, jedoch keine konkrete Verpflichtung für die Deutsche Rentenversicherung Braunschweig-Hannover auslöst, erscheint dies nicht erforderlich.

In der Stellungnahme der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens wird vor allem das Fehlen von verbindlichen Vorgaben zur Gewährleistung der Informationssicherheit im faktischen Sicherheitsverbund der an das Landesdatennetz angeschlossenen Behörden sowie das Fehlen eines einheitlichen Sicherheitskonzept angesprochen. Eine gesetzliche Verpflichtung der Kommunen soll bewusst nicht vorgesehen werden, um die Kommunen nicht in ihrer Organisationshoheit zu beschränken. Aufgrund der heterogenen Struktur der Behörden bedarf es hier einer genauen Abstimmung mit den vorgehaltenen Systemen.

Zum Ersten Abschnitt (Gewährleistung der Informationssicherheit):

Zu § 13 (Förderung der Sicherheit in der Informationstechnik):

Zu Absatz 1:

Die mit dem Betrieb des Landesdatennetzes beauftragte Behörde hat die Verantwortung für die Verfügbarkeit, Vertraulichkeit und Integrität der über das Landesdatennetz übertragenen Daten. Aufgrund der Komplexität des Netzes sowie dessen Übergänge in andere Verwaltungsnetze und das Internet kann dies – wie zuvor dargelegt – nur durch den Einsatz von Sicherheitstechnologien nach dem Stand der Technik sichergestellt werden. Der Betrieb des Landesdatennetzes und dessen Sicherheitsüberwachung stellen somit in der Praxis eine untrennbare Aufgabe dar, die in einer Verantwortung liegen muss. Der Betrieb der Sicherheitstechnologie mit der dafür notwendigen Expertise soll in einem „Security Operation Center“ bei der mit dem Betrieb des Landesdatennetzes beauftragten Behörde erfolgen.

Zu Absatz 2:

Absatz 2 beschreibt mit den Nummern 1 bis 4 die Aufgaben

- Abwehr von Gefahren für die IT-Sicherheit,
- Untersuchung der detektierten Sicherheitsvorfälle,
- Zurverfügungstellung der gewonnenen Erkenntnisse,
- Planung von Sicherheitsvorkehrungen und
- Unterstützung der Zentralstelle für IT-Sicherheit nach deren Vorgaben.

Zu Absatz 3:

Nach Absatz 3 besteht die Aufgabe, die sicherheitstechnischen Anforderungen zu entwickeln und fortzuschreiben (Nummer 1), IT-Sicherheitsprodukte bereitzustellen (Nummer 2), die Verantwortlichen in Abstimmung mit der Zentralstelle für IT-Sicherheit (§ 16 Abs. 1) zu unterstützen (Nummer 3) sowie bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen zu unterstützen (Nummer 4). Diese Leistungen können zentral finanziert oder über eine Entgeltberechnung vergütet werden.

Die Zentralstelle für IT-Sicherheit des für die zentrale IT-Steuerung zuständigen Ministeriums (§ 16 Abs. 1) benötigt neben vielfältigen externen Erkenntnisquellen auch insbesondere eine exakte Sicherheitslage des Landesdatennetzes. Hierzu ist ihr auf Basis der Auswertungen aus den Sicherheitssystemen zuzuarbeiten.

Bei herausgehobenen Fällen soll das Security Operation Center im Rahmen seiner Fähigkeiten die betroffenen Behörden unterstützen.

Zu Absatz 4:

Absatz 4 verpflichtet die das Landesdatennetz betreibende Behörde und die vom Justizministerium bestimmte Stelle zur Wahrnehmung ihrer Aufgaben nach den Absätzen 2 und 3, dem jeweiligen Stand der Technik entsprechende informationstechnische Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme und Angriffe zu betreiben.

Die verfassungsrechtliche Sonderstellung der Niedersächsischen Justiz bleibt von den Regelungen des § 13 unberührt. Es handelt sich um eine klarstellende Aufgabenzuweisung für den Bereich des Landesdatennetzes in Zusammenhang mit der Verpflichtung von der das Landesdatennetz betreibenden Behörde. Um der verfassungsrechtlichen Sonderstellung der Niedersächsischen Justiz nachzukommen, sind die Aufgaben nach Absatz 2 für den Bereich der Justiz einer von dem Niedersächsischen Justizministerium zu bestimmenden Stelle zugewiesen worden. Durch diese Regelung und die bestehenden technischen Vorkehrungen ist sichergestellt, dass die Justiz Herrin über ihre Daten bleibt. Somit gibt es keine netzübergreifenden technischen Erhebungen über betriebliche sicherheitsrelevante Ereignisse in den beiden Netzen. Ein Informationsaustausch darüber muss zwischen dem Niedersächsischen Justizministerium und dem Niedersächsischen Ministerium für Inneres und Sport vereinbart werden. Die Aufgaben nach Absatz 3 berühren nicht die Sonderstellung der Justiz und sollten aus Effizienzgründen einer zentralen Stelle zugewiesen werden. Sie sind deshalb der das Landesdatennetz betreibenden Behörde, auch für das Netz des Geschäftsbereichs des Justizministeriums, zugewiesen worden.

Zu § 14 (Unaufschiebbare Maßnahmen zur Gewährleistung der IT-Sicherheit):

Der oder dem IT-Bevollmächtigten des Landes wird gesetzlich das Recht eingeräumt, bei einer gegenwärtigen Gefahr für die IT-Sicherheit, die zu einer Gefahr für die IT-Sicherheit bei anderen Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden sind, führen kann, vorübergehende und unaufschiebbare Maßnahmen gegenüber Behörden und Gerichten des Landes anzuordnen, die zur Gewährleistung der IT-Sicherheit erforderlich sind. Dies gilt nur im Sicherheitsverbund des Landesdatennetzes und gegenüber Behörden des Landes. Auch dürfen die Maßnahmen nur vorübergehend angeordnet werden, da es sich quasi um Notstandsmaßnahmen handelt. Das Ressortprinzip wird zwar grundsätzlich durch diese Anordnungsbefugnis eingeschränkt, jedoch würde andernfalls ein anderes Ressort oder eine andere Behörde beeinträchtigt werden, sodass diese Einschränkung aufgrund kollidierender Rechte gerechtfertigt ist.

Wenn Angriffe auf die elektronische Verwaltungsinfrastruktur des Landes Niedersachsen drohen oder bekannt werden oder sonstige Sicherheitsrisiken auftreten, muss die Verfügbarkeit der Informationstechnik, insbesondere des Landesdatennetzes, entsprechend der Bedrohungslage und dem Schadensrisiko vorübergehend eingeschränkt werden können. Im Interesse der Funktionsfähigkeit der gesamten Landesverwaltung und der Vertraulichkeit der Datenbestände kann der Schutz vor erheblichen Schäden vorrangig gegenüber der Funktionsfähigkeit einzelner Bereiche oder einzelner Dienste sein. Vertretbare Einschränkungen in Bedienung und Komfort sind in diesem Fall hinzunehmen. Dies gilt in besonderem Maße für die Übergänge zu anderen Netzwerken, vor allem zum Internet, und wenn eine gegenwärtige Gefahr besteht. Für die Definition der „gegenwärtigen Gefahr“ kann die Legaldefinition in § 2 Nr. 1 Buchst. b des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) herangezogen und modifiziert werden. Eine gegenwärtige Gefahr ist eine Gefahr, bei der im einzelnen Fall die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht.

Diese Maßnahme darf nur angewendet werden, wenn eine Gefahr für die IT-Sicherheit oder ein gravierender Sicherheitsvorfall vorliegt oder unmittelbar bevorsteht und die Maßnahme daher vorübergehend und unaufschiebbar ist. Ansonsten sollen solche Maßnahmen von den Behörden selbst getroffen werden, die für das jeweilige Verfahren zuständig sind – in Abstimmung mit den ansonsten betroffenen Behörden.

Zu beachten ist auch, dass die Anordnungsbefugnis nur gegenüber den Behörden des Landes greift. Allerdings kann eine Anordnung auch gegenüber dem zentralen IT-Dienstleister erfolgen. Inhalt könnte die Anordnung zum Abschalten einzelner Netzsegmente oder Basisdienste sein. Hiervon können auch die Kommunen betroffen sein, da diese das Landesdatennetz und bestimmte Basisdienste mit nutzen. Entsprechende Regelungen sind in die Anschlussbedingungen nach § 15 Abs. 3 aufzunehmen. Da es sich um ein Ultima-Ratio-Mittel handelt, wird dies nur im absoluten Ausnahmefall nach einer gründlichen Abwägung erfolgen.

Zu § 15 (Sicherheitsverbund, Verpflichtung zu Sicherheitsmaßnahmen):

Um der Bedeutung der gemeinschaftlichen Aufgabe eines einheitlichen Sicherheitsniveaus gerecht zu werden, gelten die Grundsätze der Informationssicherheit sowie die Grundzüge der Sicherheitsorganisation und des Information Security Management System (ISMS) für alle mit dem Landesdatennetz verbundenen Behörden gleichermaßen. Alle mit dem Landesdatennetz verbundenen Behörden und Organisationen bilden letztlich einen Sicherheitsverbund, dessen Niveau nur so hoch ist, wie das des schwächsten Gliedes. Das Ziel muss daher darin bestehen, das Sicherheitsniveau im gesamten Verbund angemessen einheitlich zu realisieren. Ein einheitliches Sicherheitsniveau kann nur dann gewährleistet werden, wenn für alle Teilnehmerinnen und Teilnehmer dieselben Maßgaben gelten. Deshalb gelten die Vorschriften des § 15 auch für die Gerichte und die Bereiche der Hochschulen und Forschungseinrichtungen, die an das Landesdatennetz angeschlossen sind. Letztere haben sicherzustellen, dass zwischen dem Landesdatennetz und den Forschungsnetzen keine Netzübergänge bestehen. Das Sicherheitsniveau wird gemäß dem Stand der Technik und unter wirtschaftlichen Aspekten definiert. Dazu ist eine Risikoanalyse hinsichtlich der Schutzziele der Verfügbarkeit, Vertraulichkeit und Integrität für die übertragenen Informationen durchzuführen. Die für den Betrieb des Netzes verantwortliche Stelle hat unter Berücksichtigung von Wirtschaftlichkeitsaspekten das Restrisiko für die Informationssicherheit des Netzes zu verantworten.

Zu Absatz 1:

Die digitale Verwaltung ist nur möglich, wenn die ihr anvertrauten Informationen auch in den verwendeten IT-Systemen in Hinblick auf die Vertraulichkeit, Verfügbarkeit und Integrität hinreichend geschützt verarbeitet werden. § 15 legt Regelungen fest, die zur Erreichung dieser Schutzziele erforderlich sind. Dabei dürfen die IT-Systeme nicht isoliert betrachtet werden, weil ein Sicherheitsvorfall in einem System auch eine Gefahr für andere Systeme zur Folge hat. In Absatz 1 wird deshalb festgelegt, dass die Behörden des Landes ihre IT-Systeme in einem Sicherheitsverbund betreiben. Insbesondere das Landesdatennetz muss als Einheit betrachtet werden, an das die unterschiedlichen Beteiligten mit ihren Systemen angeschlossen sind. Jede Behörde ist daher verantwortlich, dass das Landesdatennetz nicht durch die eigenen Systeme korrumpiert wird, indem z. B. Schadsoftware in das Landesdatennetz gelangt. Aber auch für den Fall, das Landesbehörden nicht an das Landesdatennetz angeschlossen sind, sind sie im Fall des Datenaustausches und bei der Nutzung gemeinsamer Verfahren gegenüber den korrespondierenden Behörden verantwortlich. Sie müssen daher nach Satz 2 Sorge dafür tragen, dass die Informationssicherheit in angemessenem Maße gewährleistet wird. Dafür sind Risikoanalysen durchzuführen, die eine Einschätzung der Bedrohungslage in Relation zu dem Schutzbedarf der verarbeiteten Daten beinhalten. Dabei wird der Schutzbedarf in die drei Kategorien „normal“, „hoch“ und „sehr hoch“ unterteilt.

Die sich aus der Datenschutz-Grundverordnung ergebenden Anforderungen an die Verarbeitung personenbezogener Daten bleiben hiervon unberührt.

In Satz 3 wird klarstellend die Verantwortlichkeit der Behördenleitung dargestellt. Nur sie hat es in der Hand, entsprechende Standards und Vorkehrungen zu treffen, und muss dieses Handeln auch gegenüber den anderen Mitgliedern des Sicherheitsverbunds verantworten. Diese Verantwortungsübernahme ist auch zwingend erforderlich: die Behördenleitung kann zwar die Aufgaben delegieren oder Dritte mit der Aufgabenerfüllung beauftragen, sie kann sich aber nicht von ihrer Verantwortung befreien. Es liegt daher an ihr, die Beauftragten zu kontrollieren und

sich durch diese Kontrolle zu exkulpieren. Die Verantwortungsübernahme für Informationssicherheit durch die Organisations- oder Behördenleitung entspricht der zentralen Vorgabe der in der Verwaltung gebräuchlichen Standards des Bundesamtes für Sicherheit in der Informationstechnik, der ISO 27000-Reihe sowie daraus abgeleiteter Standards, etwa dem bayrischen ISIS 12.

Es handelt sich insgesamt auch um einen Grundpfeiler des Informationssicherheitssystems in Niedersachsen.

Die Verantwortung der Behördenleitung ist ein Grundsatz, der allgemein gilt. Nur die Behördenleitung hat es in der Hand, die entsprechenden Prozesse und Verfahren zu initiieren und zu begleiten, um die Informationssicherheit innerhalb der Behörde sicherzustellen. Sie kann sich dazu Dritter bedienen und die Aufgaben entsprechend verteilen, sie kann aber nicht die Verantwortung selbst an Dritte abgeben. Die Behördenleitung kann sich aber insofern exkulpieren, wenn sie nachweisen kann, dass sie ihrerseits alles Erforderliche veranlasst hat und sich auch in angemessenen Abständen vergewissert hat, dass ihre Vorgaben beachtet worden sind. Sie muss sich z. B. unterrichten lassen, ob die IT-Sicherheitskonzepte umgesetzt wurden. Gegebenenfalls hat die Behördenleitung Verfahren einzustellen, wenn die Informationssicherheit nicht ausreichend gewährleistet ist. Falls die Behördenleitung Weisungen von der übergeordneten Behörde erhält, deren Beachtung zu einer Beeinträchtigung der Informationssicherheit führen würde, muss sie die übergeordnete Behörde hierauf hinweisen. Die Verantwortung der Behördenleitung kann allerdings nur so weit reichen wie ihre Einflussnahme. Hat sie nicht die Möglichkeit, auf die Verfahren oder Prozesse einzuwirken, etwa weil eine übergeordnete Behörde diese in Auftrag gegeben hat und ein Mitsprachrecht nicht besteht, so muss die übergeordnete Behörde die Verantwortung dafür tragen. Hierzu wird in Satz 4 explizit geregelt, dass die oberste Landesbehörde oder bei anderen als Behörden des Landes die oberste Dienstbehörde abweichende Verantwortlichkeiten festlegen kann.

Zu Absatz 2:

Absatz 2 besagt, dass Risikoanalysen durchzuführen sind. Das bedeutet, dass die Behörden des Landes für ihren Verantwortungsbereich Bedrohungen und Schwachstellen erkennen müssen, die bei deren Zusammentreffen entstehenden Gefahren als Risiken für Informationen einschätzen und bewerten müssen. Die Analysen oder die daraus gewonnenen Erkenntnisse sind Grundlage für das weitere Handeln und Basis für weitere Maßnahmen. Satz 2 sieht daher vor, dass die für die Behandlung des Risikos erforderlichen Schritte unverzüglich, also ohne schuldhaftes Zögern zu treffen sind. Zudem sind die Maßnahmen regelmäßig zu überprüfen („check“) und anzupassen („act“). Risikobehandlung bedeutet in diesem Zusammenhang, dass die identifizierten Risiken durch entsprechende Sicherheitsmaßnahmen vermindert oder akzeptiert werden müssen. Dies muss fortlaufend geschehen, um neuen Risiken zeitnah zu begegnen und um jederzeit ein gleichbleibendes Niveau an Informationssicherheit herstellen zu können. Die erforderlichen einheitlichen Mindestanforderungen an das risikoorientierte Vorgehen werden in einer Informationssicherheitsrichtlinie festgelegt.

Zu Absatz 3:

Bei den von Absatz 3 erfassten angeschlossenen Mitgliedern handelt es sich nicht nur um Behörden, sondern häufig um Einrichtungen des Privatrechts oder um Kommunale Datenverarbeitungszentren, die eigene Rechtspersonen darstellen und von den Kommunen getragen werden. Eine Verpflichtung auf vertraglicher Grundlage ist daher die einzig sinnvolle Option. Eine Verpflichtung zu Anschlussbedingungen, die technische und organisatorische Vorgaben enthalten können, ist erforderlich, um einen gemeinsamen Sicherheitsverbund im Landesdatennetz zu gestalten, der den Ansprüchen des im ISMS festgeschriebenen Landesstandards genügt. Sie sind weiterhin erforderlich, da das Land einen Übergang vom Landesdatennetz zum Verbindungsnetz des Bundes betreibt und gegenüber dem Bund zu Anschlussbedingungen an das Verbindungsnetz des Bundes verpflichtet ist.

Zu § 16 (Zentralstelle für Informationssicherheit):

Den Aufbau und Betrieb des ressortübergreifenden Informationssicherheitsmanagementsystems (ISMS) in der niedersächsischen Landesverwaltung beschreibt die Leitlinie zur Gewährleistung der Informationssicherheit in dem Gemeinsamen Runderlass vom 9. November 2016 (Nds. MBl. S. 1193). Die Leitlinie zur Gewährleistung der Informationssicherheit dient der langfristigen Gewährleistung der Informationssicherheit für die unmittelbare Landesverwaltung.

Zu Absatz 1:

In Absatz 1 wird gesetzlich festgehalten, dass das für zentrale IT-Steuerung zuständige Ministerium eine Zentralstelle betreibt, die die Behörden im Hinblick auf die Sicherheit in der Informationstechnik berät und bei informationstechnischen Sicherheitsvorfällen Hilfestellung gibt. Diese Leistungen werden von der Zentralstelle für die Behörden des Landes grundsätzlich kostenfrei erbracht, gegenüber anderen Behörden kann dies jedoch auch in Rechnung gestellt werden, sofern ein zusätzlicher Aufwand damit verbunden ist und sich die Tätigkeit nicht im Weiterleiten von Informationen erschöpft, die schon den Behörden des Landes zur Verfügung gestellt wurden.

Zu Absatz 2:

Absatz 2 verpflichtet die Behörden und Gerichte des Landes, der Zentralstelle Sicherheitsvorfälle unverzüglich mitzuteilen, wenn diese geeignet sind, auch die Informationssicherheit anderer Sicherheitsdomänen zu beeinträchtigen.

Zum Zweiten Abschnitt (Einsatz von Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit):

Zu § 17 (Geltungsbereich, Wahrnehmung der Befugnisse nach diesem Abschnitt):

Zu Absatz 1:

Die Befugnis, Maßnahmen nach dem Zweiten Abschnitt zu treffen, erhalten Behörden, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind. Eine Beschränkung der Befugnisse, wie dies von der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens gesehen wird, ist grundsätzlich nicht beabsichtigt. Eine Wahrnehmung der Befugnisse im Netz der Kommunen bleibt diesen im Rahmen ihrer Organisationshoheit überlassen. Im Hinblick auf die Schwere des Grundrechtseingriffs sowie die Geeignetheit der Vorschrift im Hinblick auf die betrieblichen Aufwände entsprechender Sicherheitssysteme soll die Anwendung der Befugnis auf den abgrenzbaren Raum des Landesdatennetzes beschränkt werden.

Hier wäre auch zu erwägen gewesen, ob nur eine zentrale Behörde, etwa eine oberste Landesbehörde, diese Befugnis erhalten soll. Dies würde jedoch der IT-Struktur des Landes nicht gerecht werden und würde die deutliche Mehrheit der Behörden von der zentralen Behörde abhängig machen und gegebenenfalls zu einem erheblichen Eingriff in verfassungsmäßig statuierte Rechte führen. Da es sich allerdings durchweg um Behörden handelt, deren IT-Systeme mit dem Landesdatennetz verbunden sind, ist es notwendig, dass alle die Befugnis ausüben dürfen. Andernfalls würde die Gefahr drohen, dass einige Behörden nicht die Möglichkeit hätten, ihre Systeme hinsichtlich Sicherheitslücken, Schadprogrammen oder Angriffen auszuwerten. Dadurch könnten z. B. Schadprogramme in den Sicherheitsverbund des Landesdatennetzes eindringen und die Sicherheit weiterer Behörden beeinträchtigen. Der von der LfD im Rahmen der Verbandsbeteiligung vorgebrachten Kritik zur Streubreite der Eingriffsbefugnisse ist entgegenzuhalten, dass auch die Stellungnahme der Arbeitsgemeinschaft der Kommunalen Spitzenverbände Niedersachsens hinsichtlich der Anwendbarkeit der Regelungen auf mittlere und kleinere Kommunen deutlich macht, dass aufgrund des Bedarfs an Fachpersonal und Technik keine ausufernde Verbreitung derartiger Systeme zu erwarten ist. Aufgrund der hohen Anforderungen der Eingriffsregelungen ist faktisch nicht zu erwarten, dass jede Stelle von den Ermächtigungsgrundlagen Gebrauch machen kann. Es ist eher davon auszugehen, dass dies durch einen zentralen Dienstleister bei den Kommunen oder durch den IT.Niedersachsen vorgenommen wird.

Ein IT-System gilt im Sinne dieses Gesetzes mit dem Landesdatennetz verbunden, wenn es direkt oder über ein untergeordnetes behördeneigenes Netz (z. B. lokale Netze oder Datennetze der Kommunen) technisch angeschlossen ist. Nicht verbunden mit dem Landesdatennetz sind IT-Systeme, die nur über das Internet erreichbar sind. Netze von Verwaltungen außerhalb Niedersachsens einschließlich des Verbindungsnetzes zwischen den Landesdatennetzen sind im Sinne dieses Gesetzes nicht mit dem Landesdatennetz verbunden.

Der Behördenbegriff wird in § 1 definiert und ist identisch mit § 1 Abs. 4 NVwVfG. Satz 2 stellt sicher, dass der Abschnitt ausnahmslos für das Justizministerium und seinen Geschäftsbereich Anwendung findet.

Zu Absatz 2:

Absatz 2 Satz 1 weist der das Landesdatennetz bereitstellenden Behörde die Befugnis zu, in eigener Zuständigkeit im Rahmen der Aufgabenzuweisung nach § 13 im Landesdatennetz mit Ausnahme des Justizbereichs Anomalieerkennungssysteme anzuwenden. Diese Behörde betreibt bislang als Querschnittsaufgabe für die an das Landesdatennetz angeschlossenen Behörden die bereits etablierte Sicherheitstechnologie. Damit leistet diese Behörde mit besonderer Expertise an einer Stelle einen wesentlichen Beitrag für die IT-Sicherheit der angeschlossenen Behörden. Dieses Vorgehen hat sich aus wirtschaftlicher Sicht und im Ergebnis nachhaltig bewährt. Ergänzend betreiben nur wenige, zumeist große Fachverwaltungen zusätzliche Sicherheitstechnologien, zumeist aus rechtlichen Gründen. Der mit den Befugnissen im Zweiten Abschnitt des Dritten Teils ermöglichte Einsatz von Anomalieerkennungssystemen erfordert deutlich höhere Aufwände und weitergehende Expertise als die bislang im Einsatz befindliche Technologie. Damit die an das Landesdatennetz angeschlossenen Behörden an dieser Sicherheitstechnologie teilhaben können, soll das bisherige Organisationsmodell des zentralen Betriebs in Form einer internen Dienstleistung auch für die neuen Technologien angewandt werden. Viele Behörden sind faktisch nicht in der Lage, geeignetes Personal und die notwendige Infrastruktur bereitzustellen, um derartige Systeme zu betreiben. Ihnen soll in Form einer Dienstleistung die Nutzung der neuen Sicherheitstechnologie ermöglicht werden. Ein Zugang zu diesen Leistungen für Kommunen kann in der Anfangsphase des Einsatzes von Anomalieerkennungssystemen noch nicht angeboten werden, da zunächst Erfahrungen mit dem System gewonnen werden müssen.

Der Zustimmungsvorbehalt gemäß Satz 2 ist mit der besonderen Verfassungsstellung und damit einhergehenden Unabhängigkeit nach der Niedersächsischen Verfassung zu begründen.

Die Regelung in Satz 3 betrifft die Wahrnehmung der Befugnisse im Netz des Justizministeriums und seines Geschäftsbereichs.

Zu Absatz 3:

Absatz 3 wurde nach Maßgabe des Ministeriums für Wissenschaft und Kultur zur Wahrung der Unabhängigkeit der Hochschulen aufgenommen und nimmt die Hochschulen und Einrichtungen des Landes, die mit Forschungsaufgaben betraut sind, aus dem Geltungsbereich aus.

Zu § 18 (Allgemeine Bestimmungen):

Zu Absatz 1:

Absatz 1 dient einer allgemeinen Klarstellung, dass die in diesem Gesetz vorgesehenen Beschränkungen nur für solche Daten gelten, die dem Fernmeldegeheimnis des Artikels 10 des Grundgesetzes unterliegen oder sofern bei diesen ein Personenbezug gegeben ist. Andernfalls greifen die in diesem Gesetz vorgesehenen Beschränkungen nicht. Das Fernmeldegeheimnis schützt die Vertraulichkeit der unkörperlichen Übermittlung von Informationen an individuelle Empfänger unter Zuhilfenahme des Telekommunikationsverkehrs (Maunz/Dürig, GG, Artikel 10 Rn. 81). Eine öffentliche Kommunikation ist hingegen nicht vom Schutzbereich erfasst.

Zu Absatz 2:

Absatz 2 dient ebenfalls der Klarstellung. Sofern durch die Auswertungen nach den §§ 19 bis 22 ein Schadprogramm erkannt wird, kann dieses jederzeit gelöscht werden. Eine Strafbarkeit, etwa nach § 303 a des Strafgesetzbuchs, ist dann ausgeschlossen. Der von der LfD im Rahmen der Verbandsbeteiligung geforderten Aufnahme eines angemessenen Verfügbarkeitsschutzes wird nicht nachgekommen. Die Beseitigung von Schadprogrammen erfolgt erst nach Vorliegen der Voraussetzungen der §§ 19 bis 22 und damit erst nach sorgfältiger Prüfung des Stufenmodells. Das verbleibende minimale Risiko für die Verfügbarkeit ist ungleich geringer als der Schaden, der durch die Maßnahme abgewehrt wird. Entgegen der Kritik der LfD wird in Absatz 2 und den folgenden Regelungen an dem Begriff der Auswertung festgehalten. Bei der automatisierten Auswertung handelt es sich um einen technischen Begriff, der nicht nur im Zusammenhang mit dem Anomalieerkennungssystemen fachlich üblich ist, sondern auch in anderen Fachgesetzen verwendet wird. Die Begriffsbestimmungen des datenschutzrechtlichen Verarbeitungsbegriffs können in diesem Zusammenhang nicht zutreffend verwendet werden. Von einer Legaldefinition des Begriffs wurde abgesehen, um den technikneutralen Ausdruck nicht zu gefährden.

Zu Absatz 3:

Absatz 3 zeigt die strenge Zweckbindung auf. Dieser Absatz macht insbesondere auch deutlich, dass die Daten nicht für Leistungskontrollen oder Ähnliches verwendet werden dürfen.

Zu § 19 (Auswertung von gespeicherten Daten):

Zu Absatz 1:

Bei § 19 handelt es sich um eine Zweckänderungsnorm, die es zulässt, bereits gespeicherte Datenbestände aus enumerativ aufgezählten Systemen auszuwerten. Nicht enthalten ist darin allerdings eine Ermächtigung zum Erheben dieser Daten, da eine derartige Ermächtigungsgrundlage gemäß § 3 NDSG und im Übrigen gemäß Artikel 6 Abs. 1 DSGVO bereits besteht. Aufgrund der strengen Zweckbindung dürfen die erhobenen Daten bisher nicht für den Zweck der IT-Sicherheit im Sinne dieses § 19 verwendet werden. Die Zweckänderung in diesem Absatz lässt die Auswertung zu diesem Zweck nunmehr zu. Die Behörden dürfen die Daten, mit Ausnahme der Inhaltsdaten, nach den Anforderungen des § 22 dieses Gesetzes auszuwerten, um Sicherheitslücken, Schadprogramme oder Angriffe zu erkennen und damit Gefahren für die IT-Sicherheit, nämlich die Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten, abzuwehren. Satz 1 enthält daher selbst eine strenge Zweckbindung für die Verwendung der bereits auf anderer rechtlicher Grundlage erhobenen Daten.

Die Systeme, deren automatisierte Ereignisdokumentationen automatisiert untersucht werden dürfen, sind in Absatz 1 Satz 2 enumerativ aufgezählt. Automatisierte Ereignisdokumentationen sind die Protokolldaten, die in Protokolldateien, auch „log files“ genannt, abgelegt werden.

Nummer 1 betrifft die Protokolldateien von Firewall-Systemen sowie von Systemen zum Netzbetrieb. Eine Firewall schützt als Sicherungssystem das Netzwerk eines Rechnernetzes oder einzelner Computer vor unerwünschten Zugriffen. Protokolldaten der Firewall-Systeme, die ausgewertet werden dürfen, sind insbesondere IP-Adresse und Port, vollständiger Domänenname von ein- und ausgehenden Verbindungen, der Erhebungszeitpunkt und die durch die Firewall durchgeführte Aktion. Systeme zum Netzbetrieb sind z. B. Router und Switches.

Nummer 2 betrifft die sogenannten Antivirenprogramme. Diese versuchen, Schadprogramme auf IT-Systemen zu erkennen, deren Ausführung zu verhindern und sie nach Möglichkeit zu beseitigen. Basis für das Erkennen von Schadprogrammen sind Signaturen von bereits bekannten Schadprogrammen und Heuristiken. Ausgewertet werden dürfen auch die IP-Adresse, der vollständige Domänenname des betroffenen Systems, die ausgegebene Meldung, der Erhebungszeitpunkt sowie Informationen über die Schadsoftware und die als Schadprogramm erkannten Daten.

Nach Nummer 3 können die Protokolldaten der sogenannten Spam-Filter ausgewertet werden. Spam-Filter arbeiten in der Regel mit sogenannten Blacklist-Methoden. Die entstandenen Protokolldaten enthalten Informationen über mögliche Angriffe, vor allem wenn die Schadsoftware via E-Mail versendet wurde. Zu den Daten, die bei den Spam-Filtern ausgewertet werden dürfen, gehören unter anderem die IP-Adresse und der vollständige Domänenname von ein- und ausgehenden Verbindungen, die E-Mailadresse des Absenders und des Empfängers einer

Nachricht, deren Größe und eindeutige Identifikationsnummer sowie Fehler und sonstige Statusmeldungen, der Erhebungszeitpunkt und die als Schadprogramm erkannten Daten.

Nummer 4 erfasst die Daten der Datenbankserver. Ausgewertet werden dürfen unter anderem der Erhebungszeitpunkt, der Anmeldename, die IP-Adresse und der vollständige Domänenname von Verbindungen, die Identifikationsnummer der ausgegebenen Meldung sowie deren Klartext. Weiterhin sind auch die Server von Verzeichnisdiensten, wie z. B. das Active Directory-Systeme oder LDAP, erfasst und die Anwendungsserver, die Anwendungsprogramme ausführen, wie z. B. die Steuerung von Vorgangsbearbeitungssystemen oder Web-und Proxy-Server.

Die Betriebssoftware nach Nummer 5 liefert ebenfalls Verdachtsmomente für Angriffe oder Schadsoftware, da sie in Protokolldateien erfolgreiche und erfolglose Aktionen und Aufrufe von Programmen speichert. Daher sind die dort gewonnenen Daten weiter zu verwenden. Dies gilt auch für den Erhebungszeitpunkt, die IP-Adresse, den vollständigen Domänennamen des betroffenen Computersystems, den Namen des Programms oder Systemdienstes sowie dessen Typ, die Identifikationsnummer der ausgegebenen Meldung und deren Klartext.

Die Ermächtigung dieses Absatzes dient der Gefahrenermittlung für die IT-Sicherheit der mit dem Landesdatennetz verbundenen Systeme. Nur wenn dabei gemäß Absatz 2 zureichende tatsächliche Anhaltspunkte für eine Gefahr festgestellt werden, können unter den dort aufgeführten Maßgaben weitere Auswertungen vorgenommen werden.

Zu Absatz 2:

Satz 1 trägt dem Grundsatz der Datenminimierung Rechnung und führt zu einer Senkung der Eingriffsintensität, indem eine sofortige Löschung der Auswertungsergebnisse und der gefertigten Kopien der Ereignisdokumentationen nach Absatz 1 Satz 2 vorgesehen ist, sofern nicht zureichende tatsächliche Anhaltspunkte für eine Gefahr für die IT-Sicherheit vorliegen. Zureichende tatsächliche Anhaltspunkte liegen vor, wenn ein Anfangsverdacht für eine Gefahr für die IT-Sicherheit vorliegt. Dies ist der Fall, wenn diese Gefahr zumindest möglich erscheint. Satz 2 stellt klar, dass im Rahmen dieses Paragrafen nur die Kopien der Daten zu löschen sind, da die Ursprungsdaten selbst in Protokolldateien für andere Zwecke erhoben wurden. Sie unterliegen in der Regel eigenen Löschfristen, weil sie für die anderen Zwecke, für die sie ursprünglich erhoben wurden, noch benötigt werden und aus diesem Grund nicht in der Urform gelöscht werden können. Sofern keine Kopien vorliegen, kann außer den Auswertungsergebnissen nichts weiter gelöscht werden. Liegen allerdings aufgrund der Auswertungen zureichende tatsächliche Anhaltspunkte dafür vor, dass eine Gefahr im Sinne des Absatzes 1 Satz 1 vorliegt, so darf weiter ausgewertet werden nach § 22.

Satz 3 stellt klar, dass sich die Auswertung von Inhaltsdaten nicht nach den §§ 20 und 21 richtet, sondern ausschließlich nach § 22. Grund dafür ist die besondere Sensibilität von Inhaltsdaten, sodass für deren Auswertung strengere und weitere Anforderungen zu erfüllen sind.

Satz 4 wurde zur Klarstellung aufgrund der Forderung der LfD im Rahmen der Verbandsbeteiligung aufgenommen. Bereits § 18 Abs. 3 regelt, dass personenbezogene Daten, die zum Zweck der Gewährleistung der IT-Sicherheit nach diesem Gesetz verarbeitet werden dürfen, nicht für andere Zwecke verarbeitet werden dürfen.

Zu § 20 (Erhebung und Auswertung des Datenverkehrs):

Zu Absatz 1:

Während § 19 die automatisierte Auswertung bestimmter bereits erhobener und gespeicherter Daten regelt, dient § 20 dazu, die Rechtsgrundlage zu schaffen, um den Datenverkehr im Landesdatennetz nach Auffälligkeiten zu durchsuchen. Der Absatz stellt klar, dass es lediglich um die Daten geht, welche innerhalb der Informations- und Kommunikationsinfrastruktur des Landes verarbeitet und gespeichert werden und damit dem Verfügungsbereich des Landes unterliegen.

In Satz 1 wird die strenge Zweckbindung normiert. Die Auswertung des Datenverkehrs hinsichtlich vorhandener Sicherheitslücken, Schadprogrammen oder Angriffen darf nur zur Abwehr von Gefahren für die IT-Sicherheit der Behörden erfolgen, gemäß § 1 Nr. 8 zur Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten. Dazu sollen Schadprogramme, Sicherheitslücken oder Angriffe gefunden werden können. Angriffe sollen erkannt und deren Folgen beseitigt werden können, zudem soll Angriffen vorgebeugt werden. Die Suche nach Auffälligkeiten erfolgt an den Übergabe- und Knotenpunkten der Behördennetze, die von der Behörde oder in deren Auftrag betrieben werden. Übergabe- und Knotenpunkte sind IT-Systeme, die den Datenverkehr mit einem anderen Netz sicherstellen oder ihn innerhalb des eigenen Netzes verteilen. Die Übergabe- und Knotenpunkte müssen gemäß § 1 Abs. 2 mit dem Landesdatennetz verbunden sein.

Die Auffälligkeiten im Datenverkehr ergeben sich aus einem Abweichen von dem festgelegten Normalzustand des Datenverkehrs und des Systemverhaltens sowie der Entdeckung von Schadsoftware.

Satz 2 stellt die eigentliche Erhebungsnorm dar. Um Gefahren für die IT-Sicherheit abzuwehren, darf der an den Übergabe- und Knotenpunkten anfallende Datenverkehr erhoben werden.

Übergabe- und Knotenpunkte sind im Sinne dieses Gesetzes alle aktiven Netzwerkgeräte zur Steuerung des Netzwerkverkehrs auf der Sicherungsschicht (OSI Layer 2), insbesondere Kopplungselemente wie z. B. Switche, sowie

Netzwerkrouter und höhere Switches, welche auf Basis der Vermittlungsschicht (OSI Layer 3) die Weiterleitungsentscheidung für Netzwerkpakete treffen.

Es handelt sich um eine automatisierte Erhebung. Ein bereits überwiegender, weiter zunehmender Anteil des hier anfallenden Datenverkehrs wird aus Sicherheitsgründen verschlüsselt abgewickelt. Da ohne eine Entschlüsselung ein Großteil des Datenstroms einer Auswertung durch zentrale Sicherungssysteme im Sinne des Zweiten Abschnitts gar nicht zugänglich wäre, bliebe als letzte Schutzmaßnahme hierfür nur die Schadsoftwareerkennungslösung auf den Endgeräten. Diese Erkennungssysteme, nämlich vorrangig Virenscanner, werden gegenüber hochentwickelten Angriffen zunehmend wirkungslos, da diese die musterbasierte Erkennung von Schadsoftware durch die ständigen Veränderungen des Programmcodes unterlaufen. Die daher in modernen IT-Schutzsystemen erforderliche Mehrstufigkeit von zentralen und lokalen Sicherungssystemen könnte dann nicht realisiert werden. Der Zweck der Vorschrift, Schadprogramme und Angriffe zu verhindern oder sie zumindest zu erkennen und deren Folgen zu beseitigen, kann ohne die erforderliche Entschlüsselung des Datenverkehrs nicht erreicht werden. Mit der Klarstellung in der Norm, Datenverkehr zu entschlüsseln, soll zudem den Anforderungen an die Bestimmbarkeit des Grundrechtseingriffs entsprochen werden.

Bei der weit überwiegenden Menge des verschlüsselten Datenverkehrs kommt eine Verschlüsselung mit dem Verfahren „Transport Layer Security“ (TLS) zum Einsatz. Insbesondere handelt es sich beim Zugriff auf Web-Seiten per „Hypertext Transfer Protocol Secure“ (HTTPS, englisch für „sicheres Hypertext-Übertragungsprotokoll“) um eine mit TLS verschlüsselte HTTP-Verbindung („Hypertext Transfer Protocol“ (HTTP), englisch für „Hypertext-Übertragungsprotokoll“). Eine Entschlüsselung ist bei TLS nur möglich, wenn bereits ab dem Verbindungsaufbau an einem Übergabepunkt der gesamte Datenverkehr unverschlüsselt erhoben wird. Ein nachträgliches Entschlüsseln des verschlüsselt erhobenen Datenverkehrs – so nach der Feststellung, dass zureichende tatsächliche Anhaltspunkte für eine Gefahr nach Absatz 1 Satz 1 bestehen – könnte nur erfolgen, wenn die Kommunikationspartner die jeweils ausgehandelten Sitzungsschlüssel, also das Geheimnis der Verschlüsselung, überlassen würden. Dieses Verfahren widerspricht den gängigen Sicherheitsstandards im Internet. Zudem würden Angreifer gerade dies nicht tun. Somit ist eine nachträgliche Entschlüsselung technisch nicht möglich. Die sofortige Entschlüsselung des Datenverkehrs bei der Erhebung ist daher erforderlich, um Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme oder Angriffe abwehren zu können. Dies gilt sowohl für die Gefahrenermittlung nach Absatz 1 Satz 3 sowie für die weitere Auswertung nach den §§ 21 und § 22 bei Vorliegen der dort geregelten Voraussetzungen.

Satz 3 regelt detailliert, in welchem Umfang Daten zur Ermittlung von Gefahren für die IT-Sicherheit im Rahmen der Zweckbindung nach Satz 1 automatisiert ausgewertet werden dürfen. Weitergehende Befugnisse bestehen zu diesem Zeitpunkt und nach diesem Absatz nicht, insbesondere ist keine Auswertung durch eine natürliche Person denkbar.

Welche Daten ausgewertet werden dürfen, ist in Satz 3 geregelt:

In Nummer 1 sind der Erhebungszeitpunkt, die IP-Adresse mit Subnetzmaske, die Präfixlänge, die Portnummern und die MAC-Adresse, der vollständige Domänenname sowie die Kopf- und Statusdaten von Netzwerkpaketen für ein- und ausgehende Verbindungen aufgeführt. Betroffen von der Auswertung sind insofern die im IP-Datenstrom benötigten Informationen für die Steuerung der einzelnen Datenpakete.

Bei der IP-Adresse handelt es sich quasi um die „Telefonnummer eines IT-Systems“; sie ist für das Funktionieren eines Netzwerksystems erforderlich, weil sie den Anfangs- und Endpunkt der Kommunikationsverbindung definiert und so die konkrete Adressierbarkeit von Datenpaketen an bestimmte IT-Systeme und die Durchleitung über verschiedene Netzwerke (sogenanntes „Routing“) ermöglicht. Um maliziösen Datenverkehr in einem Netzwerk erkennen und auf seinen Ursprung zurückverfolgen zu können, ist die IP-Adresse daher unerlässlich, weil nur über diese Adresse eine eindeutige Identifikation des angreifenden oder angegriffenen IT-Systems möglich ist. Ohne die Erhebung der IP-Adresse könnte das angestrebte Ziel einer Einbruchsentdeckung nicht vollständig erreicht werden, weil sich nicht identifizieren ließe, in welches System konkret eingedrungen wurde oder auf welches System sich ein gegenwärtiger oder erfolgloser Angriff bezieht oder bezog. Würde man die IP-Adresse aus dem IDS/SIEM-System hinwegdenken, würde dies den Zweck der Maßnahme unmöglich und damit das Gesetz insgesamt unverhältnismäßig werden lassen.

Aus diesen Verkehrsdaten können weitere Anhaltspunkte für eine Gefahr für die IT-Sicherheit gewonnen werden, etwa die Verbindungsaufnahme zu bekannten gefährlichen oder illegalen IP-Adressen sowie unübliche oder nicht vorgesehene Verbindungsarten. Zudem erlaubt die Erhebung und Auswertung des IPv4-Headers und IPv6-Headers, Angriffe auf Netzwerkebene zu detektieren, in denen korrumpierte Paketheader eingesetzt werden und die ohne die Erhebung dieser Daten unerkannt blieben.

Der IPv4/IPv6-Header eines Netzwerkdatenpaketes enthält alle notwendigen Steuerinformationen, um das Datenpaket über das Netzwerk an einen Empfänger zu übermitteln. Ein Rückschluss auf den Inhalt des Datenpakets ist nur über die Paketgröße auf sehr genereller Ebene möglich. Es kann lediglich ermittelt werden, welche Datenlänge die Inhaltsdaten des Pakets aufweisen. Weitere Rückschlüsse auf den Inhalt sind nicht möglich.

Die im IPv4-Header angegebene Quell-IP-Adresse (Source-IP-Address) sowie Ziel-IP-Adresse (Destination-IP-Address) respektive bei IPv6 die Quell-IP-Adresse (Source Address) und Ziel-IP-Adresse (Destination Address) stellen personenbeziehbare Daten dar. Sie sind nach Maßgaben der folgenden Paragrafen zu pseudonymisieren.

Die MAC-Adresse ist nach ihrer Definition eine weltweit eindeutige Nummer für Netzwerkgeräte. Sie identifiziert ein IT-System innerhalb seines lokalen Netzwerksegments. Die MAC-Adresse kann in den Geräten oder auf Basis von Softwarelösungen leicht verändert werden (sog. „MAC-Spoofing“), um damit z. B. den Zugriffsschutz von Netzwerken zu überwinden. Die MAC-Adresse ist auch bei sog. ARP-Spoofing-Angriffen von zentraler Bedeutung, bei denen der Datenverkehr eines angegriffenen IT-Systems über den Rechner des Angreifers umgelenkt wird, indem dem angegriffenen Rechner vorgetäuscht wird, das für die Weiterleitung seines Datenverkehrs notwendige IT-System (sogenannter „Gateway“) sei der Rechner des Angreifers. Insoweit ist auch die Erhebung und Verarbeitung der MAC-Adresse zur Zweckerreichung erforderlich, da ansonsten diese häufig genutzte Angriffsmethode nicht erkannt werden und dadurch die Zweckerreichung erheblich beeinträchtigt werden würde. Der vollständige Domänenname erleichtert gerade in komplexen Netzwerken die Zuordnung einzelner IT-Systeme zu bestimmten organisatorischen Einheiten (z. B. Rechner einer bestimmten Fachverwaltung) oder bestimmten Zwecken (z. B. Webserver des Landes). Er ist zur Zweckerreichung zwar nicht zwingend erforderlich, dürfte allerdings die Bearbeitungsgeschwindigkeit bei der Auswertung von Angriffen und Angriffsversuchen erhöhen und ist damit der Zweckerreichung dienlich, ohne den Grundrechtseingriff gegenüber der bereits vorgesehenen IP-Adresse signifikant zu vergrößern.

In Nummer 2 werden für Verbindungen auf der Basis des Hypertext-Übertragungsprotokolls zusätzlich zu den bereits in Nummer 1 genannten Daten der vollständige einheitliche Ressourcenzeiger und die Kopfdaten (englisch: Header) erfasst. Dadurch sind alle weiteren Elemente des Seitenaufrufs erfasst, wobei der Cookie nicht ausgewertet werden darf. Da ein überwiegender, weiter ansteigender Teil des Datenverkehrs verschlüsselt übertragen wird, ist es erforderlich, den zuvor entschlüsselten Header von HTTPS-Verbindungen im gleichen Umfang auszuwerten. Im Fall von HTTPS-Verbindungen erfolgt zum Anfang der Kommunikationsbeziehung zwischen Client und Server eine Aushandlung der zu verwendenden Verschlüsselung. Nachdem diese Aushandlung erfolgreich abgeschlossen ist, wird die restliche Kommunikation in der Anwendungsschicht des Netzwerkpaketes in verschlüsselte Daten gekapselt. Diese Kapselung bedeutet, dass bei HTTPS-Verbindungen weiter das HTTP-Protokoll genutzt wird, diese Kommunikation wird jedoch auf der Anwendungsebene über das TLS Application Data Protocol verschlüsselt zwischen Client und Server transportiert. HTTPS ist unter Betrachtung des Protokollaufbaus daher mit dem des HTTP-Protokolls syntaktisch gleichzustellen.

Die unverzügliche automatisierte Erhebung und Auswertung des vollständigen einheitlichen Ressourcenanzeiger (Uniform Resource Locator, URL) und der Kopfdaten (http-Header Daten) exklusive des Cookies ist erforderlich, um den Ursprung und das Ziel der stattgefundenen Kommunikation eindeutig zu identifizieren. Über die Auswertung der IPv4/IPv6-Headerdaten kann lediglich die IPv4/IPv6 Adresse des Zielservers ermittelt werden. Auf eine eindeutige IP-Adresse können jedoch beliebig viele Domains registriert werden, die Auflösung und Auslieferung des korrekten Inhalts erfolgt jeweils serverintern. Hierfür beinhaltet der http-Request-Header ab Version http/1.1 den lesbaren Hostname des aufzurufenden Ziels, durch den ein Rückschluss auf den konkret aufgerufenen Inhalt erst möglich wird.

Die Verarbeitung des einheitlichen Ressourcenzeigers ist weiterhin erforderlich, weil über Zugriffe der Nutzerinnen und Nutzer mittels des Webbrowsers auf das World Wide Web ein in seiner Bedeutung zunehmender Infektionsweg für Schadprogramme liegt (sogenannte „drive by downloads“). Über die Auswertung der Zugriffe können zudem Hinweise auf Infektionen mit Schadprogrammen gewonnen werden sowie durch Blockierung bekannter Infektionswege die (weitere) Verbreitung von Schadprogrammen verhindert werden. Überdies ist die Verarbeitung der URL erforderlich, weil Schadsoftware selbst über Zugriffe mittels des http-Protokolls weiteren Schadcode oder Instruktionen aus dem Internet nachlädt oder auf diesem Weg Daten des infizierten IT-Systems exfiltriert und damit die Vertraulichkeit der auf dem IT-System gespeicherten Daten beeinträchtigt. Dazu ist es notwendig, dass sie eine Verbindung zu einem Zielsystem aufnehmen, auf dem diese Daten schließlich gespeichert werden können. Ein Großteil der Schadprogramme nutzt dafür das http-Protokoll, weil es in den allermeisten Netzwerken für die Nutzung des World Wide Web freigegeben ist. Dabei versucht das Schadprogramm, seinen Datenverkehr möglichst unverdächtig und wie die legitime Kommunikation eines Nutzers wirken zu lassen, der mittels seines Webbrowsers im World Wide Web Seitenaufrufe tätigt. Tatsächlich bieten die Kopfdaten eines http-Aufrufs eine Reihe von heuristischen Hinweisen, wenn der Seitenaufruf von einem Schadprogramm verursacht wurde (z. B. Tippfehler, verschleierte URLs). Über die Verarbeitung der aufgerufenen Seiten und die Analyse der mit dem Aufruf übermittelten Kopfdaten können daher Hinweise auf die Kommunikation von Schadprogrammen ermittelt werden. Die Auswertung der Kopfdaten ist vor diesem Hintergrund auch erforderlich.

In Nummer 3 ist geregelt, in welchem Umfang Daten des Domain-Name-Service-Protokolls (DNS) ausgewertet werden dürfen. Dies sind die Inhalte der DNS-Anfragen und DNS-Antworten. DNS stellt einen verteilten hierarchischen Verzeichnisdienst über das Internet dar. Vergleichbar mit dem Nachschlagen eines Namens in einem Telefonbuch wird mittels DNS einem Fully-Qualified-Domain-Name (FQDN) (z. B. https://www.niedersachsen.de/startseite/) eine IP-Adresse (z. B. 195.37.199.23) zugeordnet. Die IP-Adresse ist erforderlich, um die Kommunikation mit dem Endsystem herzustellen. Die Daten des DNS-Protokolls sind nicht in dem in den Nummern 1 und 2 geregelten Datenumfang enthalten.

Die Analyse des DNS-Datenverkehrs innerhalb des Netzwerkes ist zur Abwehr von Gefahren für die IT-Sicherheit des Landes durch Schadprogramme oder Angriffe erforderlich. Aktuelle Schadsoftware versucht in der Regel, eine Kommunikationsbeziehung zu Kontrollstrukturen aufzubauen. Diese Kommunikationsbeziehung dient zur Ausleitung von Daten, dem Informationsaustausch und dem Erhalt weiterer Ausführungsanweisungen. Um etablierte Sicherheitstechnologien an Übergabepunkten zu unterlaufen, z. B. Sperrlisten, werden bei der Entwicklung der Schadsoftware anstelle von statischen IP-Adressen oder Fully-Qualified-Domain-Name (FQDN) letztere zur Laufzeit der Schadsoftware dynamisch generiert. Über die DNS-Abfragen auf DNS-Servern im Internet werden dann die dynamisch generierten FQDN in dort hinterlegte, sich oft laufend ändernde IP-Adressen umgewandelt, womit eine Erkennung weiter erschwert wird.

Die Algorithmen zur Erstellung des aufzurufenden FQDN sind häufig über bereits analysierte Schadsoftware bekannt und damit auch die Muster der generierten FQDN. Über eine Auswertung des Datenverkehrs nach Maßgabe der Nummer 3 können sie erkannt werden, ebenso wie bekannte statische FQDN.

Ohne die Auswertung des DNS Netzwerkverkehrs gäbe es nur die Möglichkeit, entsprechende Kommunikationsstrukturen über HTTP-Verbindungen zu erkennen. Dies setzte voraus, dass die Schadsoftware eine HTTP-Anfrage an ein definiertes Ziel sendet, womit der FQDN über die Auswertung von HTTP-Paketen erkannt würde. Nutzt die Schadsoftware allerdings reine DNS-Anfragen, um z. B. einen aktuellen Ausführungsstatus zu erhalten, kann die Infektion des IT-Systems im Verbund des Landesnetzes ohne Auswertung des DNS Netzwerkverkehr nicht nachgewiesen werden. Damit wäre eine unerkannte, erfolgreiche DNS-Anfrage eines Schadprogramms das Start-Signal zur Aufnahme der schädlichen Funktion. Dieses Start-Signal bliebe ohne die automatisierte Analyse des DNS Netzwerkverkehrs unerkannt. Weiter kann nur durch die automatisierte Auswertung des DNS-Datenverkehrs erkannt werden, wenn eine Schadsoftware eigene DNS-Abfragen über das Netzwerk adressiert, bei denen das Netzwerkpaket derart manipuliert wird, dass notwendige Systemeinstellungen und Netzwerkeinschränkungen an Übergabepunkten umgangen werden können. Die Auswertung des DNS-Verkehrs ist somit erforderlich, um den Zweck der Vorschrift nach Absatz 1 Satz 1 zu erreichen.

Eine Auswertung weiterer Protokollheader wie zur Übertragung von Dateien (FTP, File Transfer Protocol, oder FTP/S, FTP over TLS) ist nicht erforderlich, da eine Gefahrenermittlung anhand Satz 3 Nr. 1 erfolgen kann.

Satz 4 wurde nach Maßgabe des Justizministeriums aufgenommen, um eine Rechtsgrundlage für den Betrieb eines sogenannten Advanced Threat Analytics–System (ATA) zu schaffen. Er gilt ergänzend zu den Sätzen 1 bis 3. Neben den in Satz 3 Nr. 1 aufgeführten Datenarten werden in dem System zusätzlich Metadaten aus dem Verzeichnisdienst erhoben und ausgewertet. Abweichend von Absatz 1 Satz 2 werden diese nicht an Knoten- und Übergabepunkten, sondern im Verzeichnisdienst selbst erhoben. Als auffälliger Datenverkehr im Sinne dieser Vorschrift gelten z. B. ungewöhnlich häufige, direkt aufeinanderfolgende Anmeldeversuche, die nur von einer Kennung ausgehen, ungewöhnliche Bewegungsmuster durch Konten von Systemdiensten, gleichzeitige Anmeldeversuche einer Kennung aus unterschiedlichen Subnetzen, Modifizierung von sensiblen Benutzergruppen oder die Nutzung von identischen (geklonten) Kerberos-Tickets. Die Analyse des erhobenen Datenverkehrs und der Abgleich gegen den Normalzustand erfolgen vollständig automatisch. Wird eine Abweichung vom Normalzustand identifiziert, erfolgt die Auflösung der Meldung manuell. Ziel ist es, verdächtige Aktivitäten innerhalb des Netzwerks, und hier besonders im Verzeichnisdienst, zu identifizieren. Satz 4 unterliegt nicht den Verarbeitungsvorbehalten der §§ 21 und 22. Vielmehr soll er eine neue Rechtsgrundlage für die Erkennung und Analyse abnormalen Verhaltens des Datenverkehrs schaffen.

Zu Absatz 2:

Absatz 2 Satz 1 legt verbindlich fest, dass die neu erhobenen Daten ohne schuldhaftes Zögern zu löschen sind, wenn im Rahmen der Auswertung zureichende tatsächliche Anhaltspunkte für eine Gefahr nicht zutage getreten sind. Gelöscht werden müssen neben den Daten selbst auch die Auswertungsergebnisse, um im Sinne der Datenminimierung zu agieren. An dieser Stelle sind – anders als im Rahmen des § 19 – auch die Daten selbst zu löschen, da diese nur für den Zweck in Absatz 1 Satz 1 erhoben wurden und eine weitere Verwendung der Daten aufgrund dieses Gesetzes nicht mehr stattfinden wird.

Satz 2 dient wiederum der Klarstellung, dass Inhaltsdaten nur unter den höheren Voraussetzungen des § 22 ausgewertet werden dürfen.

Die im Rahmen der Verbandsanhörung formulierte Kritik der LfD, dass in § 20 eine Regelung für eine technische und organisatorische Datenschutzmaßnahme fehle, wird nicht geteilt. In § 23 sind umfassende Datensicherungsmaßnahmen für die nach den §§ 19 bis 22 erhobenen oder gespeicherten Daten aufgeführt.

Zu § 21 (Auswertung ohne Inhaltsdaten):

§ 21 trifft Regelungen zur Auswertung aller Daten, die nicht Inhaltsdaten sind. Die Auswertung von Inhaltsdaten erfolgt nur unter den Voraussetzungen und nach den Vorgaben des § 22.

Zu Absatz 1:

Satz 1 lässt eine weitere einzelfallbezogene Auswertung zu, sofern „zureichende tatsächliche Anhaltspunkte“ für eine Gefahr im Sinne des § 19 Abs. 1 Satz 1 oder des § 20 Abs. 1 Satz 1 vorliegen. Der Begriff „zureichende tatsächliche Anhaltspunkte“ stammt aus dem strafprozessualen Bereich (§ 152 StPO). Es muss daher ein Anfangsverdacht für eine Gefahr für die IT-Sicherheit der Behörden durch Sicherheitslücken, Schadprogramme oder Angriffe vorliegen. Dies ist der Fall, wenn die Gefahr zumindest möglich erscheint.

In Satz 2 wird eine Speicherfrist von sieben Tagen vorgesehen. Die Speicherung auffälliger Daten ist bei Vorliegen der „zureichenden tatsächlichen Anhaltspunkte“ erforderlich. Denn Schadprogramme werden häufig nicht sofort, sondern mit einem zeitlichen Verzug erkannt. Die Speicherung für sieben Tage hat der Bundesgerichtshof zum Erkennen, Eingrenzen oder Beseitigen der Störung einer Telekommunikationsanlage durch den Anbieter nach sachverständiger Beratung als für „auf das zur Erreichung der legitimen Zwecke notwendige Maß begrenzt“ angesehen. Diese Erwägungen des Bundesgerichtshofs in seinem Urteil zur Speicherung von IP-Adressen aus dem Jahr 2014 (BGH NJW 2014, 2500, 2503) untermauern seine bereits im Jahr 2011 vertretene Ansicht zur Verhältnismäßigkeit einer siebentägigen Speicherung (BGH MMR 2011, 341, Rn. 28). Sollte bereits vor Ablauf dieser sieben Tage klar sein, dass sich der Anfangsverdacht nicht erhärten lässt, so sind die Daten unverzüglich zu löschen.

Satz 2 erfordert zudem eine automatisierte Pseudonymisierung, sofern die Daten nicht pseudonym sind, dies aber technisch möglich ist. In den meisten Fällen werden die Daten allerdings bereits pseudonym sein. Durch Satz 2 werden dem Grundsatz der Datenminimierung entsprochen und ein Eingriff in Grundrechte möglichst gering gehalten.

Die Daten dürfen im Rahmen des Satzes 2 weiter ausgewertet werden, jedoch nur automatisiert. Eine Kenntnisnahme durch natürliche Personen ist zu diesem Zeitpunkt daher ausgeschlossen.

Zu Absatz 2:

Absatz 2 sieht eine weitere Auswertung der Daten auch manuell durch eine natürliche Person vor sowie eine direkt personenbezogene Verarbeitung, sofern nunmehr hinreichende tatsächliche Anhaltspunkte vorliegen, die den Verdacht begründen, dass die Daten durch einen Angriff oder ein Schadprogramm verursacht wurden, sich aus ihnen Hinweise darauf ergeben und soweit die Datenverarbeitung erforderlich ist. Aufgrund der Anhaltspunkte muss es wahrscheinlicher sein, dass der Verdacht begründet ist, als dass er unbegründet ist.

Absatz 2 bedeutet daher eine Verlängerung der Speicherfrist und die Möglichkeit, eine direkte manuelle Verarbeitung der gegebenenfalls nicht pseudonymen Daten vorzunehmen. Voraussetzung sind allerdings hinreichende tatsächliche Anhaltspunkte im Sinne des § 170 StPO. Dies bedeutet, dass es wahrscheinlicher sein muss, dass die Daten durch einen Angriff oder ein Schadprogramm verursacht wurden oder dass sich entsprechende Hinweise aus diesen Daten generieren lassen, als dass die Daten nicht durch einen Angriff oder ein Schadprogramm verursacht wurden oder entsprechende Hinweise erkennbar werden. Eingeschränkt wird diese Möglichkeit der Datenverarbeitung allerdings dadurch, dass die weitere Verarbeitung stets erforderlich sein muss. Das bedeutet insgesamt, dass ein Abbruch erfolgen muss, wenn das Schadprogramm, der Angriff oder davon ausgehende Gefahren beseitigt sind oder andere Schadprogramme oder Angriffe nicht erkannt oder abgewehrt werden können. Dies betrifft auch die zeitliche Komponente, sodass die Speicherung der Daten dann nicht mehr zulässig ist, wenn sie für die bereits genannten Erfordernisse nicht mehr benötigt werden.

Satz 3 sieht vor, dass die Datenverarbeitung nach Satz 1, dies betrifft die nicht automatisierte, also manuelle Verarbeitung sowie die direkte Verarbeitung der personenbezogenen Daten, von der Behördenleitung und einer oder einem weiteren Beschäftigten mit der Befähigung zum Richteramt gesondert angeordnet werden muss. Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung nach Satz 3 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. Damit wird sichergestellt, dass auch kleinere Behörden und Kommunen, die keine Person mit der Befähigung zum Richteramt beschäftigen, die Möglichkeit der Anordnung offensteht. Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen. Da nach diesem Abschnitt keine heimliche, inhaltliche Überwachung verbunden ist, sondern nur die Suche nach Schadprogrammen erfolgen soll, ist kein Richtervorbehalt erforderlich.

Da es sich bei dem Betrieb eines IDS/SIEM-Systems um eine sogenannte „flächendeckende Maßnahme“ handelt, die grundsätzlich in die Rechte einer Vielzahl von Betroffenen eingreift, ist nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) der Anlass, Verwendungszweck und Umfang des Eingriffs bereichsspezifisch, normklar und präzise zu bestimmen und damit eine tatbestandliche Eingrenzung erkennen zu lassen. Die verschiedenen Eingriffe werden deshalb – nach Form und Intensität gestuft –mit ihren tatbestandlichen Bedingungen in den §§ 21 und § 22 ausgeformt und damit gegenüber den Betroffenen transparent gemacht. Diesem Gebot des BVerfG wird durch den vorliegenden Gesetzentwurf Rechnung getragen, indem eine nicht automatisierte Verarbeitung an das Vorliegen eines hinreichenden Verdachts gebunden wird und über die Notwendigkeit der Anordnung mit einer besonderen organisatorischen Hürde versehen wurde.

Die Anordnung oder Genehmigung als besondere organisatorische Hürde ist ein wesentliches Element des Eskalationsmodells in § 21 Abs. 2 Satz 3, § 22 Abs. 2 Satz 4 und Abs. 3 Satz 3 sowie § 25 Satz 3, um einen weitreichenden Eingriff in die Grundrechte nach Artikel 10 des Grundgesetzes kontrollierbar und nach den Anforderungen des BVerfG zu gestalten. Hierfür müssen die Anordnenden eine entsprechende Qualifikation besitzen, die durch die Befähigung zum Richteramt definiert wird. Diese Gründe rechtfertigen zudem einen Eingriff in die kommunale Personalhoheit. Die Regelung entspricht der des § 5 BSIG.

Da es sich um eine Abwägung von rechtlichen Aspekten und technischen Details handelt, ist stets eine enge Zusammenarbeit zwischen dem technischen und dem juristischen Personal dringend erforderlich, weil nur auf diese Weise sachgerechte Entscheidungen zu erwarten sind. Der im Rahmen der Verbandsbeteiligung vorgebrachten Forderung der LfD nach einem Richtervorbehalt ist entgegenzuhalten, dass die Zielrichtung und Eingriffsintensität der Maßnahme nicht zwingend einen Richtervorbehalt erfordert. Besonders das komplexe Stufenmodell, die strenge Zweckbindung, die grundsätzlich automatisierte Datenverarbeitung, der verfolgte Grundsatz der Datenminimierung und die Kontrollmaßnahmen führen zu einer grundrechtsschonenden Umsetzung und letztlich zur Angemessenheit und Verhältnismäßigkeit des Gesetzes. Hinzu kommt, dass Angriffe aus dem Cyberraum eine schnelle Reaktion erfordern, sehr hohe Fallzahlen erwartet werden und eine juristische Spezialisierung auf das Themengebiet erforderlich erscheint. Vergleichbare Eingriffsregelungen in § 5 BSIG und § 16 BayEGovG sehen ebenfalls keinen Richtervorbehalt vor.

Zu Absatz 3:

Absatz 3 regelt die Löschfrist für die für die Zwecke der Auswertung vorhandenen Daten und die Auswertungsergebnisse. Diese sind zu löschen, wenn sie nicht mehr erforderlich sind. Die Daten, die für die Zwecke der Auswertung vorhanden sind, sind die Kopien von bereits vorhandenen Daten nach § 20, die für die Auswertung nach diesem Gesetz gefertigt wurden, oder die im Rahmen des § 21 selbst für die Zwecke dieses Gesetzes erhobenen Daten. Absatz 3 dient der Verhältnismäßigkeit der Maßnahme, insbesondere dem Grundsatz der Datenminimierung.

Zu § 22 (Auswertung von Inhaltsdaten):

Zu Absatz 1:

Absatz 1 lässt die automatisierte Auswertung von Inhaltsdaten zu. Ausgewertet werden dürfen die Inhaltsdaten allerdings nur, um Hinweise auf Sicherheitslücken, Schadprogramme oder Angriffe zu erhalten. Diese lassen sich in erster Linie anhand der Inhaltsdaten erkennen. Auch in § 22 ist die strenge Zweckbindung zum Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Daten in der Informationstechnik des Landes, kurz: zum Schutz der IT-Sicherheit, aufgeführt. Die Daten müssen unverzüglich und damit ohne schuldhaftes Zögern ausgewertet werden. Satz 2 stellt insofern klar, dass die Daten, also entweder die Kopien der bereits zu anderen Zwecken vorhandenen Daten oder die für die Zwecke dieses Gesetzes neu erhobenen Daten sowie die Auswertungsergebnisse unverzüglich zu löschen sind, wenn in den folgenden Absätzen keine weitere Verwendung der Daten zugelassen ist.

Zu Absatz 2:

Absatz 2 Satz 1 regelt die Speicherfrist, wenn zureichende tatsächliche Anhaltspunkte vorliegen. Es muss insofern ein Anfangsverdacht im Sinne des § 152 StPO für eine Gefahr für die IT-Sicherheit der Behörden durch Schadprogramme oder Angriffe vorhanden sein. Die Daten dürfen vom Moment der Speicherung an sieben Tage gespeichert werden, wobei Satz 4, aufgrund der besonderen Sensibilität von Inhaltsdaten, eine gesonderte Genehmigung fordert. Es wird in diesem Zusammenhang auf die Begründung zu § 21 Abs. 2 verwiesen. Dort kann im Rahmen der siebentägigen Speicherfrist nach § 21 Abs. 1 Satz 2 über eine individuelle Darlegung des Sachverhalts eine Anordnung zur weiteren einzelfallbezogenen Verarbeitung nach § 21 Abs. 2 Satz 1 eingeholt werden. Im Fall des Satzes 1 dieses Absatzes ist bei Erkennen zureichender tatsächlicher Anhaltspunkte die Aufzeichnung aus der Auswertung nach Absatz 1 jedoch sofort mit dem laufenden Paket zu beginnen, da Angriffe oft nur Sekundenbruchteile andauern. Eine Anordnung wäre aufgrund der Zeitdauer nicht zweckmäßig. Vielmehr werden in den Überwachungssystemen Regeln hinterlegt werden müssen, die Szenarien zureichender tatsächlicher Anhaltspunkte nach Satz 1 darstellen. Diese werden zuvor mit den mit der Genehmigung nach Satz 4 betrauten Personen abgestimmt und der jeweilige Sachverhalt nach dem Auslösen des Überwachungssystems ihnen unverzüglich zur Genehmigung vorgelegt.

Satz 2 sieht eine automatisierte Pseudonymisierung der Daten vor, wenn die Daten nicht bereits mit einem Pseudonym versehen sind. Auch die weitere Auswertung der Inhaltsdaten darf nach Satz 3 nur automatisiert erfolgen. Grund für die Sätze 3 und 4 ist die besondere Sensibilität dieser Daten. Inhaltsdaten sind auch die Inhalte einer Kommunikation, sodass dort in hohem Maße Grundrechte betroffen sein können. Um die Grundrechtseingriffe bei diesem Verdachtsgrad so gering wie möglich zu halten, soll daher eine Erkennbarkeit der einzelnen Personen ausgeschlossen sein, ebenso eine manuelle Verarbeitung der Daten. Durch diese Erfordernisse wird eine natürliche Person nach diesem Absatz keine Kenntnis der Daten erhalten können. Zudem werden natürliche Personen, z. B. als Kommunikationsteilnehmende, durch die Pseudonymisierung nicht bekannt werden.

Zu Absatz 3:

Eine weitere Auswertung unter Personenbezug und mit einer Einsichtnahme oder manuellen Verarbeitung durch eine natürliche Person ist nur dann zulässig, wenn hinreichende tatsächliche Anhaltspunkte im Sinne des § 170 StPO den Verdacht begründen, dass diese durch ein Schadprogramm oder einen Angriff verursacht wurden oder entsprechende Hinweise darauf vorhanden sind. Insofern muss es aufgrund von Tatsachen wahrscheinlicher sein, dass die Daten durch ein Schadprogramm oder einen Angriff verursacht wurden oder dass sich entsprechende Hinweise aus diesen Daten generieren lassen, als dass die Daten nicht durch ein Schadprogramm verursacht wurden oder entsprechende Hinweise erkennbar werden. Diese Abwägung muss durch die Behördenleitung und eine weitere Beschäftigte oder einen weiteren Beschäftigten mit der Befähigung zum Richteramt erfolgen. Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen.

Zu Absatz 4:

Absatz 4 gibt die Löschfrist für die Kopien der Daten, die Daten selbst und die Auswertungsergebnisse vor. Auf die Ausführungen zu § 21 Abs. 3 wird verwiesen.

Zu Absatz 5:

Absatz 5 schützt den Kernbereich der privaten Lebensgestaltung. Der Kernbereich kann die Kommunikation mit engen persönlichen Vertrauten wie unter anderem Ehe- und Lebenspartnern und anderen engen Vertrauten oder Freunden sowie die Kommunikation mit Berufsgeheimnisträgern sein (LT-Drs. 15/3810, 30, siehe auch Möstl/Weiner in Roggenkamp/Albrecht Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, § 33 a Rn. 24). Entscheidend ist diesbezüglich allerdings nicht in erster Linie der Kommunikationspartner, sondern vielmehr der Inhalt der Kommunikation, der dem höchstpersönlichen Bereich zugeordnet sein muss (LT-Drs. 15/3810, 30 siehe auch Möstl/Weiner in Roggenkamp/Albrecht Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, § 33 a Rn. 24). Erfasst sind daher in erster Linie höchstpersönliche Kommunikationsinhalte. Diese dürfen nach Satz 1 grundsätzlich nicht erhoben werden. Sollten dennoch auf der Grundlage der vorstehenden Absätze dieses Paragrafen Auswertungsergebnisse aus diesen geschützten Bereichen erlangt werden, so unterliegen diese einem Verwendungsverbot nach Satz 2. Konsequenterweise sind diese daher auch nach Satz 3 ohne schuldhaftes Zögern zu löschen. Auch wenn nicht in Gänze klar ist, ob die Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind diese bei Zweifeln zu löschen, da die Gefahr besteht, dass andernfalls in den durch Artikel 1 Abs. 1 des Grundgesetzes absolut geschützten Bereich eingegriffen wird. Der Ausschluss der Verwendung in Satz 1 wurde auf Forderung der LfD im Rahmen der Verbandsanhörung auf solche Daten ausgedehnt, welche die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung beeinträchtigen können. Insbesondere die Kommunikation von Beschäftigten mit dem Personalrat oder der oder dem Suchtbeauftragten sollte hierunter fallen.

Satz 5 stellt klar, dass sowohl die Tatsache, dass Daten aus dem Kernbereich der privaten Lebensgestaltung erlangt wurden, als auch deren Löschung ordnungsgemäß dokumentiert werden müssen. Diese Dokumentation dient nach Satz 6 ausschließlich einer späteren möglicherweise in Betracht kommenden Überprüfung der Rechtmäßigkeit der Verarbeitung. Satz 7 sieht daher auch die Löschung vor, wenn dieser Zweck erfüllt wurde. Sollte dies nicht der Fall sein, hat die Löschung spätestens am 31. Dezember des auf die Dokumentation folgenden Jahres zu erfolgen.

Zu § 23 (Gewährleistung der Datensicherheit):

In § 23 werden Vorgaben getroffen, die die Gewährleistung der Datensicherheit zum Ziel hat. Diese Vorgaben sind von allen Behörden zu erfüllen, die Gebrauch von den Ermächtigungen machen wollen. Die Vorgaben resultieren insbesondere aus der Rechtsprechung.

Zu Absatz 1:

Absatz 1 sieht den weiteren Schutz der nach den §§ 19 bis 22 verarbeiteten Daten dergestalt vor, dass die notwendigen technischen und organisatorischen Maßnahmen zu ergreifen sind, um eine Kenntnisnahme unbefugter Dritter, eine Veränderung oder eine andere Verwendung als zu den in diesem Gesetz genannten Zwecken auszuschließen. Die Maßnahmen müssen allesamt dem Stand der Technik entsprechen, wodurch Sicherheitslücken aufgrund veralteter Technik ausgeschlossen werden. Da nach den §§ 19 bis 22 alle Datenkategorien ausgewertet werden können, muss als Maßstab ein besonders zu sicherndes IT-System herangezogen werden und die Maßnahmen müssen an diesem Maßstab ausgerichtet werden.

Satz 2 stellt insofern klar, dass die Umsetzung dieser Maßnahmen ein besonders hohes Maß an Datensicherheit erfordert. Die Maßnahmen, die sonst bei sensiblen Daten getroffen werden, reichen somit nicht aus. Dies ergibt sich auch aus den in Absatz 2 aufgeführten Maßnahmen.

Zu Absatz 2:

Absatz 2 nennt die zu treffenden Maßnahmen, die jeweils dem Stand der Technik entsprechen müssen. Es handelt sich um eine Aufzählung, die nicht abschließend ist.

Die „jeweilige Behördenleitung“ in Nummer 6 ist die Behördenleitung, um deren Datenverarbeitungsanlagen es sich handelt. Nur diese kann bestimmen, wer zu den Datenverarbeitungsanlagen Zutritt haben und darauf zugreifen soll. Nummer 7 wurde auf Forderung der LfD im Rahmen der Verbandsanhörung dahingehend ergänzt, dass der gemeinsame Zugriff durch zwei besonders ermächtigte Personen technisch (und organisatorisch) sichergestellt wird. So könnten stets zwei Schlüssel für den Zugriff auf den Datenbestand erforderlich sein. Um eine Weitergabe von Schlüsseln weitgehend auszuschließen, sollten die Schlüssel physisch individualisiert werden (z. B. durch Smartcards). Auch die Verwendung des Schlüssels für weitere Zwecke (z. B. für die Zeiterfassung) reduziert das Risiko einer unbefugten Weitergabe.

Zu Absatz 3:

Absatz 3 verpflichtet zur Führung eines Protokolls, in das jeder Zugriff auf die nach den §§ 19 bis 22 gespeicherten Daten aufzunehmen ist, und verfolgt in erster Linie generalpräventive Zwecke. Verhindert werden sollen ein Missbrauch und eine unnötige Einsichtnahme in die Daten. Wie das Protokoll geführt wird, wird nicht näher ausgeführt, sodass bei entsprechender Ausgestaltung auch eine automatisierte Datei ausreichend ist.

Satz 2 legt die Inhalte des Protokolls fest. Aufzunehmen sind neben dem Zeitpunkt auch Art und Zweck des Zugriffs sowie eine Kennung, die einer individuellen, auf die Daten zugreifenden Person zugewiesen ist. Dadurch wird sichergestellt, dass jederzeit verfolgt werden kann, wer wann und warum auf die Daten zugegriffen hat und was mit den Daten geschehen ist. Auch dieses Protokoll dient nach Satz 3 ausschließlich der Kontrolle der Rechtmäßigkeit; die Einträge sind bereits nach zwölf Monaten entsprechend Satz 4 zu löschen.

Zu Absatz 4:

Absatz 4 sieht eine jährliche Vorlage über die nach den §§ 19 bis 22 und 25 erfolgten Verarbeitungsvorgänge sowie die Dokumentation nach § 26 bei der zuständigen Aufsichtsbehörde für den Datenschutz vor, damit eine unabhängige Instanz ein Lagebild erhält. Hierbei dürfte es sich grundsätzlich um die oder den LfD handeln. Jedoch sind z. B. die Gerichte von dieser Aufsicht ausgenommen (vergl. Erwägungsgrund 20, Artikel 5, 55 Abs. 3 DSGVO). Insoweit wurde hier eine offene Formulierung gewählt. Die Vorlage kann gebündelt von einer Stelle erfolgen oder durch die einzelne Behörde, die von der Ermächtigung Gebrauch macht.

Zu § 24 (Sicherheitskonzept):

§ 24 sieht vor der Nutzung der Ermächtigungen in den §§ 19 bis 22 die Vorlage eines Sicherheitskonzepts für das von der Behörde verwendete System zur Datenverarbeitung nach den §§ 19 bis 22 vor. Alle in diesem Sicherheitskonzept vorgesehenen technischen und organisatorischen Maßnahmen müssen umgesetzt worden sein. Die Umsetzung muss in den Akten vermerkt werden, damit sichergestellt ist, dass alle Schritte, die in dem Sicherheitskonzept vorgesehen sind, beachtet worden sind und die Daten dadurch so sicher wie möglich sind. Das Sicherheitskonzept dient der Ermittlung und Analyse von Risiken für die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Daten und der auf dieser Risikoabschätzung basierenden Festlegung von Maßnahmen, die zu einer Reduzierung des Risikos führen. Für die Anfertigung des Sicherheitskonzepts kann die Informationssicherheitsrichtlinie über die risikobasierte Konzeption der Informationssicherheit von Services, Fachverfahren und Sicherheitsdomänen (ISRL-Konzeption) herangezogen werden.

Nach Satz 2 muss das Sicherheitskonzept vor jeder Veränderung der genutzten technischen Systeme an die Veränderung angepasst werden. Auf diesem Wege ist gewährleistet, dass das Sicherheitskonzept und das technische System jederzeit übereinstimmen. Zudem ist das Sicherheitskonzept alle zwei Jahre einer Revision zu unterziehen, um insbesondere die Vollständigkeit und aktuelle Bewertung aller Risiken, die Vollständigkeit und Wirksamkeit der ausgewählten Maßnahmen und den aktuellen Stand der eingesetzten Technik sicherzustellen.

Satz 3 sieht weiterhin vor, dass auch jede Veränderung des Sicherheitskonzepts den Anforderungen aus Satz 1 gerecht werden muss, wonach diese und die Umsetzung der technischen und organisatorischen Maßnahmen entsprechend in den Akten vermerkt werden.

Zu § 25 (Benachrichtigung der betroffenen Personen und Behörden):

§ 25 sieht eine Benachrichtigung der nach diesem Gesetz betroffenen Personen und Behörden vor. Betroffene Personen sind gemäß Artikel 4 Nr. 1 DSGVO natürliche Personen, deren personenbezogene Daten betroffen sind. Grund für die Regelung in § 25 ist eine mögliche Kenntnisnahme der Inhaltsdaten. Jede betroffene Person soll insofern wissen, wer welche Daten über sie oder ihn kennt und die Möglichkeit haben, Maßnahmen einer Rechtmäßigkeitskontrolle unterziehen zu können oder sich an die oder den LfD zu wenden. Die Benachrichtigung kann gemäß Satz 1 unterbleiben, wenn die betroffene Person nicht identifiziert ist (dies dürfte bei externen Angriffen durch Schadprogramme der Regelfall sein) und ihre Identifizierung auch nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre. Die im Rahmen der Verbandsbeteiligung von dem Deutschen Gewerkschaftsbund Bezirk Niedersachsen – Bremen – Sachsen-Anhalt vorgebrachte Forderung nach einer Streichung des Satzteils

der Nichtbenachrichtigung bei unverhältnismäßigem Aufwand ist zu weitgehend, zumal die Ermittlung zur Identifizierung der Personen einen weiteren erheblichen Grundrechtseingriff darstellen kann.

Die Benachrichtigungspflicht wurde auf Forderung der LfD im Rahmen der Verbandsanhörung auf sämtliche Maßnahmen nach dem Gesetz ausgeweitet, um die notwendige Transparenz herzustellen.

Die Nichtbenachrichtigung wegen unverhältnismäßigen Aufwands wird im Rahmen der Stellungahme des Deutschen Gewerkschaftsbunds Bezirk Niedersachsen – Bremen – Sachsen-Anhalt kritisiert und es wird gefordert, diesen Satzteil zu streichen. Der Grundsatz soll die Benachrichtigung der Betroffenen sein. Sofern jedoch keine ausreichenden Daten zu den Betroffenen bestehen, um diese zu benachrichtigen, kann die hierzu durchzuführende Ermittlung bei einer vorbehaltlosen Benachrichtigungspflicht für die Betroffenen einen viel intensiveren Grundrechtseingriff darstellen, da erst erheblicher Rechercheaufwand betrieben werden muss, um Daten zu ermitteln. Insoweit wird weiter an der Ausnahme festgehalten.

Über die datenschutzrechtlichen Belange hinaus ist auch eine Benachrichtigung der betroffenen Behörden vorgesehen. Diese sollen über die Einsichtnahme in personenbeziehbare und sonstige vertrauliche Daten, die mit ihrem Geschäftsbetrieb zusammenhängen, informiert werden. Neben der eigentlichen Information soll ihnen damit insbesondere die Gelegenheit gegeben werden, auf Sicherheitsvorfälle zu reagieren und zur zukünftigen Vermeidung beitragen zu können.

Satz 2 sieht weiterhin eine Einschränkung vor, wonach die Benachrichtigung gemäß Nummer 1 unterbleiben kann, wenn sie eine Gefahr für die Ermittlungen in Straf- und Disziplinarverfahren oder die IT-Sicherheit bedeutet oder gemäß Nummer 2, wenn die Person nur unerheblich betroffen wurde, und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. Hiermit werden zwei Ausnahmen aufgenommen. Der Zweck der Datenverarbeitung darf durch eine mögliche Benachrichtigung nicht gefährdet werden, da ansonsten der gesamte Verarbeitungsvorgang irrelevant werden würde. Hinsichtlich der Ausnahme in Nummer 2 ist zu bedenken, dass eine Ermittlung der Betroffenen zur Benachrichtigung den Grundrechtseingriff sogar noch vertiefen würde. Insoweit wurde entsprechend § 5 Abs. 4 Satz 2 eine weitere Ausnahme aufgenommen.

Die Ausnahme in Nummer 1 wird seitens des Deutschen Gewerkschaftsbunds Bezirk Niedersachsen – Bremen – Sachsen-Anhalt abgelehnt. Es erscheint jedoch zur Abwehr von Gefahren für die IT-Sicherheit essentiell, Betroffene nicht zu benachrichtigen, um laufende Ermittlungen nicht zu gefährden. Nach Abschluss der Ermittlungen entfällt dieser Grund und eine Benachrichtigung ist grundsätzlich vorzunehmen.

Ebenso kann der grundsätzlichen Kritik, dass die IT-Sicherheit nicht über das Fernmeldegeheimnis gestellt werden darf, nicht gefolgt werden. Es kommt jeweils auf eine Abwägung im Einzelfall an. So ist zu berücksichtigen, dass im Rahmen der IT-Sicherheit die Daten einer Vielzahl von Bürgerinnen und Bürgern betroffen sein können, sollte eine Sicherheitslücke ausgenutzt werden. Um dem angemessen zu begegnen, ist in diesem Gesetz ein gestuftes System vorgesehen, das im Fall der höchsten Eingriffsstufe Anordnung mit einer vorherigen Einzelfallbewertung vorsieht.

Zum Vorbehalt der Anordnung in den Sätzen 3 bis 5 wird auf die Begründung zu § 21 Abs. 2 Sätze 3 bis 5 verwiesen.

Zu § 26 (Dokumentation):

§ 26 dient der Klarstellung und besagt, dass, sofern eine Entscheidung durch eine Beschäftigte oder einen Beschäftigten mit der Befähigung zum Richteramt nach den §§ 21, 22 und 25 erforderlich ist, diese Entscheidung ordnungsgemäß zu dokumentieren ist, um die Entscheidung im Fall einer anschließenden Überprüfung nachvollziehbar und beweissicher vorlegen zu können. Satz 2 stellt insoweit auch klar, dass die anschließende in Betracht kommende Überprüfung der alleinige Zweck der Dokumentation ist. Insofern ist aus anderen Gründen eine Einsichtnahme in die Unterlagen zur Dokumentation ausgeschlossen.

Satz 3 beinhaltet eine Verpflichtung zur Löschung der Dokumentation der Anordnung oder Genehmigung, wenn ausgeschlossen ist, dass die Entscheidung einer nachträglichen Überprüfung unterliegen kann. Die Löschung muss aber spätestens am 31. Dezember des auf die Dokumentation folgenden Jahres erfolgen.

Zu § 27 (Übermittlung personenbezogener Daten):

Zu Absatz 1:

Absatz 1 regelt die zweckändernde Übermittlung möglicher Zufallsfunde an die Strafverfolgungsbehörden, Polizei oder die Verfassungsschutzbehörde. Während das Ziel der Maßnahmen nach diesem Abschnitt des Gesetzes die Gewährleistung der IT-Sicherheit des Landesnetzes ist, ermöglicht die Übermittlung nach Absatz 1 auch die Verfolgung sonstiger Zwecke. Unter den genannten Voraussetzungen sollen Daten nach den §§ 21 und 22 übermittelt werden.

Die Übermittlung für die sonstigen Zwecke ist jeweils an hohe Tatbestandsvoraussetzungen geknüpft. Nur diese rechtfertigen den mit der Übermittlung einhergehenden Eingriff in das Fernmeldegeheimnis gemäß Artikel 10 des Grundgesetzes. Im Ergebnis wird die Übermittlung an Voraussetzungen geknüpft, die auch eine direkte Erhebung

der Daten für den jeweiligen Verwendungszweck erlaubt hätten. So wird für eine Übermittlung für Zwecke der Strafverfolgung auf die Katalogstraftaten gemäß § 100 a StPO abgestellt, die eine Telekommunikationsüberwachung rechtfertigen würden. Ähnlich verhält es sich mit den Zwecken der Gefahrenabwehr. Hier entsprechen die Tatbestandsvoraussetzungen jenen des § 33 a Nds. SOG. Eine Verwendung der Daten für die Aufgabenerfüllung des Verfassungsschutzes ist nur unter den zusätzlichen Voraussetzungen des Artikel 10-Gesetzes möglich.

Zu beachten sind insbesondere die Sätze 2 und 3. Für die Übermittlung an die Strafverfolgungsbehörden und an die Polizeibehörden ist eine vorherige gerichtliche Zustimmung erforderlich. Dabei werden die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend angewendet. Nach Satz 4 sind die §§ 9 bis 16 des Artikel 10-Gesetzes entsprechend anzuwenden. Dieser Richtervorbehalt und der Vorbehalt der G 10-Kommission entsprechend den Voraussetzungen der oben genannten Regelungen zur Telekommunikationsüberwachung.

Entgegen der Stellungnahme der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens ist die mit der Reglung verfolgte Zweckänderung ausreichend deutlich. Eine Anpassung wird als nicht erforderlich angesehen.

Zu Absatz 2:

Absatz 2 lässt in Satz 1 eine Übermittlung der nach den §§ 21 und 22 verarbeiteten Daten von Behörde zu Behörde oder an den damit beauftragten Betrieb zu, wenn sie erforderlich ist, um Gefahren für die IT-Infrastruktur zu beseitigen oder abzuwehren. Es soll damit den einzelnen Behörden die Möglichkeit eingeräumt werden, ihre Erkenntnisse an andere Behörden oder die damit beauftragten Betriebe, die Informationstechnik betreiben, zu übermitteln, damit die Empfänger die Erkenntnisse nutzen können, um Schwachstellen beheben und Gefahren eindämmen zu können. Soweit möglich, sollte der Personenbezug in den Informationen, die den anderen Behörden zur Verfügung gestellt werden, durch Anonymisierung beseitigt werden.

Satz 2 ermöglicht der das Landesdatennetz betreibenden Behörde und der vom Justizministerium zu bestimmenden Stelle im Rahmen ihrer Befugnis nach § 17 Abs. 2 und der ihnen nach § 13 zugewiesenen Aufgaben, ihre beim zentralen Betrieb von Sicherheitstechnologien gewonnenen Erkenntnisse den sie damit betrauenden Behörden zu übermitteln. Die Behörden sollen damit in die Lage versetzt werden, Schwachstellen und Gefahren für die Informationssicherheit zu beseitigen. Andere Zwecke als die Abwehr oder Beseitigung von Gefahren für die IT-Infrastruktur dürfen daher nicht verfolgt werden. Besonders beachtet werden muss der Grundsatz der Erforderlichkeit. Ist eine Übermittlung nicht erforderlich, so darf eine Übermittlung nicht, auch nicht informationshalber, stattfinden.

Zu § 28 (Einschränkung von Grundrechten):

Durch die Befugnisse nach den §§ 19 bis 22 und 27 wird in das Fernmeldegeheimnis aus Artikel 10 des Grundgesetzes eingegriffen. Durch § 28 wird dem Zitiergebot aus Artikel 19 Abs. 1 des Grundgesetzes Genüge getan.

Zu Artikel 2 (Änderung des Niedersächsischen Beamtengesetzes):

Die Vorschrift regelt die Beauftragung einer öffentlichen oder nicht öffentlichen Stelle mit der Wahrnehmung bestimmter Aufgaben der Personaldatenverarbeitung.

Zu § 92 a:

Zu Absatz 1:

Absatz 1 legt unter Bezugnahme auf Artikel 28 DSGVO fest, in welchen Fällen es zulässig ist, im Rahmen der Auftragsverarbeitung Personalaktendaten zu verarbeiten.

Die Datenschutz-Grundverordnung regelt, wie die Auftragsverarbeitung durchgeführt werden soll. In Absatz 1 Satz 1 wird abschließend festgelegt, für welche Aufgaben der Personalverwaltung die Auftragsverarbeitung durchgeführt werden darf. Die Auftragsverarbeitung ist demnach nur zulässig für Zwecke der Bewilligung, Festsetzung oder Zahlbarmachung von Geldleistungen, z. B. der Gewährung von Beihilfe, oder der automatisierten Erledigung von Aufgaben im Rahmen der Zweckbindung des § 88 Abs. 1 Satz 1. Mit der Regelung wird insbesondere ermöglicht, dass eine öffentliche oder nicht öffentliche Stelle zum Zweck der Beihilfegewährung eine Prüfung der vorgelegten Rechnungen und deren anschließende Zahlbarmachung vornimmt oder zum Zweck der Übertragung von Papierakten in elektronische Datenbestände Personalakten für die personalverwaltende Behörde einscannt.

Die personalverwaltende Behörde ist nach Satz 2 verpflichtet, die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den Auftragsverarbeiter regelmäßig zu kontrollieren. Der Rhythmus der Überprüfungen ist durch den Verantwortlichen nach sachgerechten Erwägungen festzulegen. Maßgeblich für den vom Verantwortlichen gewählten Rhythmus sind insbesondere die Art der personenbezogenen Daten, die durch den Auftragsverarbeiter verarbeitet werden, oder die bisherige Zusammenarbeit mit dem Auftragsverarbeiter. Anlassbezogene Kontrollen bleiben von der Regelung unberührt.

Zu Absatz 2:

Die Datenverarbeitung im Auftrag und die Genehmigung einer Unterauftragserteilung bedürfen der vorherigen Zustimmung der obersten Dienstbehörde des verantwortlichen Auftraggebers. Zu diesem Zweck hat der Verantwortliche der obersten Dienstbehörde die hierzu wesentlichen Umstände mitzuteilen. Hierzu zählen insbesondere:

- die Art der Daten, die für den Verantwortlichen verarbeitet werden sollen, und den Kreis der Beschäftigten, auf den sich diese Daten beziehen,
- die Aufgabe, zu deren Erfüllung der Auftragsverarbeiter die Daten verarbeiten soll, sowie
- die von dem Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen und die ergänzenden Festlegungen nach Artikel 28 Abs. 3 der Datenschutz-Grundverordnung.

Zu Absatz 3:

Die Datenverarbeitung im Auftrag durch eine nicht öffentliche Stelle ist nur unter der Voraussetzung möglich, dass die Datenverarbeitung andernfalls bei dem Verantwortlichen zu einer nicht unerheblichen Störung im Geschäftsablauf führen würde oder vom Auftragsverarbeiter erheblich wirtschaftlicher erledigt werden kann.

Eine Störung des Geschäftsablaufs ist beispielsweise gegeben, wenn die der personalverwaltenden Behörde obliegenden Aufgaben nicht mehr ordnungsgemäß wahrgenommen werden können. Die Verantwortung für die ordnungsgemäße Aufgabenerledigung verbleibt auch bei der Beauftragung einer nicht öffentlichen Stelle bei der personalverwaltenden Behörde, sodass auch im Fall einer Insolvenz der beauftragten nicht öffentlichen Stelle die auftraggebende Stelle ihren Verpflichtungen vollumfänglich nachkommen kann.

Zu Artikel 3 (Inkrafttreten):

Zu Absatz 1:

Im Rahmen der Prüfung eines möglichen konnexitätsrelevanten Mehraufwands der Kommunen sind den notwendigen (Investitions-)Aufwänden eintretende Entlastungen wie z. B. Personaleinsparungen und Verbesserung bei Prozessabläufen sowie vom Land zur Verfügung gestellte Dienste oder Mittel gegenüberzustellen. Eine solche Gegenüberstellung von Be- und Entlastungen erweist sich zum jetzigen Zeitpunkt als schwierig. Ergebnisse zeigen sich zumeist erst in mittel- bis langfristiger Perspektive, was es wiederum schwierig macht, sie im Rahmen einer Kostenfolgenabschätzung angemessen zu berücksichtigen.

Im Rahmen einer Evaluation sind die konnexitätsspezifischen Annahmen und Berechnungen der Kostenansätze der Kommunen daher daraufhin auszuwerten, ob sie auf Grundlage der tatsächlichen Kostenaufwendungen realitätsgerecht sind. Soweit es sich nach Auswertung der praktischen Erfahrungen mit dem Gesetzesvollzug als notwendig erweisen sollte, kann die Kostenfolgenabschätzung der Landesregierung angepasst werden.

Zu Absatz 2:

Das Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Satz 2 regelt das abweichende Inkrafttreten für einzelne Paragrafen des Artikels 1, um die erforderlichen technischen und organisatorischen Umsetzungsschritte bis zum Inkrafttreten abzuschließen. Das Datum des Inkrafttretens der Nummer 1 ergibt sich aus der Richtlinie 2014/55/EU. Artikel 11 Abs. 2 Satz 2 der Richtlinie ermöglicht den Mitgliedstaaten, die Anwendung in Bezug auf ihre subzentralen öffentlichen Auftraggeber und Auftraggeber um bis zu höchstens 30 Monate nach Veröffentlichung der Fundstelle der Europäischen Norm für die elektronische Rechnungsstellung im Amtsblatt der Europäischen Union aufzuschieben. Von dieser Möglichkeit wird hier Gebrauch gemacht. Nummer 2 regelt das Inkrafttreten der Verpflichtungen nach § 4 Abs. 2 bis 4, § 5 Abs. 2, § 6 Abs. 1 und 2 und § 12 Abs. 1 bis 3 am 1. Juli 2021, da eine Bereitstellung der notwendigen Basisdienste bis dahin gesichert erscheint. Für die Verpflichtung nach § 5 Abs. 3 ergibt sich das Datum der Nummer 3 aus den Vorgaben des Onlinezugangsgesetzes.

Entsprechend der Anregung des Verbands kommunaler Unternehmer e. V. Landesgruppe Niedersachsen/Bremen wurde die Frist des Inkrafttretens des Artikels 3 Satz 2 Nr. 1 auf den 18. April 2020 verschoben.