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

Vom 24. Oktober 2019

Der Niedersächsische Landtag hat das folgende Gesetz beschlossen:

Artikel 1

Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG)*)

Inhaltsübersicht

*) § 6 Abs. 3 und 4 dieses Gesetzes dient der Umsetzung der 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).

Erster Teil

Allgemeines

§ 1

Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes bedeutet:

1. Angriff:
   ein Versuch, die IT-Sicherheit unbefugt zu beeinflussen,
2. Basisdienst:
   ein fachunabhängiges informationstechnisches Verfahren zur Unterstützung bei der Wahrnehmung von Aufgaben der öffentlichen Verwaltung,
3. Behörde:
   jede Stelle des Landes, einer Kommune oder einer sonstigen der Aufsicht des Landes unterstehenden juristischen Person des öffentlichen Rechts, die Aufgaben der öffentlichen Verwaltung wahrnimmt,
4. elektronische Rechnung:
   eine Rechnung, die in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird, das ihre automatische und elektronische Verarbeitung ermöglicht,
5. Informationssicherheit:
   die Vertraulichkeit, Verfügbarkeit und Integrität von Daten,
6. Informationstechnik (IT):
   technische Mittel zur Verarbeitung oder Übertragung von Informationen,
7. IT-Sicherheit:
   die Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten,
8. Landesdatennetz:
   eine in Netzabschnitte gegliederte Kommunikationsinfrastruktur, die eine Verbindung zwischen den lokalen Netzen der damit verbundenen Behörden ermöglicht und durch das Land betrieben wird,
9. Nutzerkonto:
   eine zentrale Identifizierungskomponente zur einmaligen oder dauerhaften Identifizierung der Nutzerinnen und Nutzer zu Zwecken der Inanspruchnahme von Leistungen der öffentlichen Verwaltung,
10. Schadprogramm:
    ein Computerprogramm, dessen Ausführung die IT-Sicherheit gefährden kann, oder ein Teil davon,
11. Sicherheitslücken:
    die Eigenschaften von Computerprogrammen oder sonstigen IT-Systemen, durch deren Ausnutzung es möglich ist, dass sich Unbefugte gegen den Willen der Berechtigten Zugang zu diesen IT-Systemen verschaffen oder die Funktion dieser IT-Systeme beeinflussen können,
12. Sicherheitsvorfall:
    ein Ereignis, das die IT-Sicherheit einschränkt oder beseitigt oder einschränken oder beseitigen könnte.

(2) Ein IT-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 der Behörden, soweit nicht besondere Rechtsvorschriften des Landes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten.

(2) Dieser Teil gilt nicht für die Strafverfolgung, die Verfolgung und Ahndung von Ordnungswidrigkeiten, die Rechtshilfe für das Ausland in Straf- und Zivilsachen und für Maßnahmen des Richterdienstrechts.

(3) Dieser Teil gilt nicht für

1. die Hochschulen in staatlicher Verantwortung,
2. die Teile von Behörden des Landes, die mit Forschungsaufgaben betraut und deren IT-Systeme nicht mit dem Landesdatennetz verbunden sind,
3. die Kirchen, Religionsgesellschaften und Weltanschauungsgemeinschaften sowie ihre Verbände und Einrichtungen,
4. die öffentlich-rechtlichen Kreditinstitute und öffentlich-rechtlichen Versicherungsanstalten,
5. die landesunmittelbaren Körperschaften der gesetzlichen Kranken-, Renten- und Unfallversicherung sowie der sozialen Pflegeversicherung,
6. Beliehene,
7. den Norddeutschen Rundfunk und die Niedersächsische Landesmedienanstalt,
8. die Nordwestdeutsche Forstliche Versuchsanstalt,
9. 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,
10. die den Landesbildungszentren angeschlossenen pädagogischen Bereiche, wenn deren IT-Systeme nicht mit dem Landesdatennetz verbunden sind, sowie
11. alle Einrichtungen im Sinne des § 1 Abs. 2 des Gesetzes über Tageseinrichtungen für Kinder.

(4) Aus diesem Teil gilt nur § 10 Abs. 4 für

1. das Justizministerium und seinen Geschäftsbereich,
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“.

(5) Für die in den Absätzen 3 und 4 genannten Stellen und Tätigkeiten bleibt, soweit Bundesrecht ausgeführt wird, das E-Government-Gesetz (EGovG) in der am 31. Oktober 2019 geltenden Fassung vom 25. Juli 2013 (BGBl. I S. 2749), zuletzt geändert durch Artikel 1 des Gesetzes vom 5. Juli 2017 (BGBl. I S. 2206), unberührt.

(6) Abweichend von den Absätzen 2 bis 4 gilt § 6 Abs. 3 und 4 für

1. die niedersächsischen Auftraggeber im Sinne des § 98 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) in Bezug auf öffentliche Aufträge und Konzessionen, 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 öffentliche Aufträge, deren geschätzter Auftragswert den jeweils maßgeblichen Schwellenwert gemäß § 106 GWB nicht erreicht.

§ 4

Elektronischer Zugang zur Verwaltung

(1) Jede Behörde ist verpflichtet, auch wenn sie nicht Bundesrecht ausführt, einen § 2 Abs. 1 EGovG entsprechenden Zugang für die Übermittlung elektronischer Dokumente zu eröffnen.

(2) [1]Jede Behörde ist verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente auch über Nutzerkonten zu eröffnen. [2]Die Nutzerkonten müssen eine Postfachfunktion enthalten, welche die Bereitstellung und Entgegennahme von Daten ermöglicht. [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) Jede Behörde ist verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente auch durch eine De-Mail-Adresse im Sinne des De-Mail-Gesetzes oder einen anderen schriftformersetzenden Dienst zu eröffnen.

(4) Jede Behörde des Landes ist verpflichtet, in elektronisch durchgeführten Verwaltungsverfahren, in denen sie die Identität einer Person aufgrund einer Rechtsvorschrift festzustellen hat oder aus anderen Gründen eine Identifizierung für notwendig erachtet, einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Abs. 5 des Aufenthaltsgesetzes anzubieten.

§ 5

Elektronische Informationen
und Verwaltungsportal

(1) Jede Behörde stellt, auch wenn sie nicht Bundesrecht ausführt, entsprechend § 3 Abs. 1 EGovG Informationen über ihre Aufgaben, ihre Anschrift, ihre Geschäftszeiten sowie ihre postalische, telefonische und elektronische Erreichbarkeit zur Verfügung.

(2) Jede Behörde hat 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) Jede Behörde hat die Informationen nach den Absätzen 1 und 2 sowie nach § 3 Abs. 1 und 2 EGovG aktuell zu halten.

(4) [1]Die obersten Landesbehörden stellen sicher, dass die landeseinheitlichen Informationen nach Absatz 2 für die Kommunen elektronisch bereitstehen, soweit diese für die Ausführung von Bundes- oder Landesrecht zuständig sind. [2]Die Kommunen können diese Informationen zur Erfüllung ihrer Pflichten nach Absatz 2 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]Jede Behörde bietet ihre Verwaltungsleistungen auch über das niedersächsische Verwaltungsportal an.

§ 6

Elektronische Bezahlmöglichkeiten und Rechnungen

(1) Jede Behörde ist verpflichtet, auch wenn sie nicht Bundesrecht ausführt, § 4 EGovG entsprechende elektronische Bezahlmöglichkeiten zu schaffen.

(2) Jede Behörde soll, wenn die Höhe der Gebühren oder der sonstigen Forderungen feststeht und die Verwaltungsleistung erst nach deren Zahlung erbracht wird, ermöglichen, dass nach Absatz 1 so bezahlt werden kann, dass die Gutschrift sofort bei der empfangenden Behörde erkennbar ist.

(3) Jeder Auftraggeber nach § 3 Abs. 6 stellt sicher, dass elektronische Rechnungen aufgrund von Aufträgen nach § 3 Abs. 6 nach Maßgabe der Verordnung nach Absatz 4 empfangen und verarbeitet werden können.

(4) [1]Die Landesregierung erlässt durch Verordnung Vorschriften zur Ausgestaltung des elektronischen Rechnungsverkehrs. [2]In der Verordnung können bestimmt werden

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

Nachweise können, auch wenn nicht Bundesrecht ausgeführt wird, entsprechend § 5 Abs. 1 EGovG elektronisch eingereicht oder von der zuständigen Behörde entsprechend § 5 Abs. 2 EGovG eingeholt werden.

§ 8

Elektronische Formulare

Für die Verwendung von Formularen gilt, auch wenn nicht Bundesrecht ausgeführt wird, § 13 EGovG entsprechend.

§ 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 amtlichen 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 sind solche, für die Daten aufgrund von Rechtsvorschriften des Landes erhoben oder gespeichert werden; dies können öffentliche und nichtöffentliche Register sein.

§ 10

Elektronische Aktenführung

(1) Jede Behörde kann ihre Akten elektronisch führen.

(2) [1]Jede Behörde des Landes soll 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]Jede in Satz 1 oder 2 genannte Behörde kann, wenn besondere Gründe vorliegen, im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung von den Sätzen 1 und 2 abweichende spätere Termine festlegen. [4]Die oder der IT-Bevollmächtigte der Landesregierung kann das Einvernehmen nur dann 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 ist die Einhaltung der Grundsätze der ordnungsgemäßen Aktenführung, insbesondere die Lesbarkeit, die Integrität und Authentizität, die Verfügbarkeit und die Vertraulichkeit der Akte, durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik 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 durch Verordnung zu regeln, soweit dies für den Austausch zwischen Behörden nach Satz 1 erforderlich ist.

(5) Soweit ein Recht auf Akteneinsicht besteht, kann jede Behörde, die ihre Akten elektronisch führt, Akteneinsicht dadurch gewähren, dass sie

1. einen Aktenausdruck zur Verfügung stellt,
2. die elektronischen Dokumente auf einem Bildschirm wiedergibt,
3. die elektronischen Dokumente übermittelt oder
4. den lesenden Zugriff auf den Inhalt der Akte ermöglicht.

§ 11

Übertragen und Vernichten von Dokumenten in Papierform

(1) [1]Jede Behörde des Landes muss, soweit sie Akten elektronisch führt, die Dokumente, die in Papierform vorliegen, in elektronische Dokumente übertragen und diese in der elektronischen Akte speichern; liegen Aktenbestandteile in anderer körperlicher Form vor, so ist deren elektronische Wiedergabe in der elektronischen Akte zu speichern. [2]Bei der Übertragung nach Satz 1 ist nach dem Stand der Technik sicherzustellen, dass die gespeicherten Daten mit den Dokumenten in Papierform oder den Aktenbestandteilen in anderer körperlicher Form bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. [3]Von der Übertragung nach Satz 1 kann abgesehen werden, wenn die Übertragung unverhältnismäßigen Aufwand erfordert.

(2) [1]Sind Dokumente in Papierform oder Aktenbestandteile in anderer körperlicher Form nach Absatz 1 übertragen und zur elektronischen Akte genommen worden, so sollen sie vernichtet oder zurückgegeben werden, wenn eine Aufbewah-

rung aus rechtlichen Gründen nicht erforderlich ist. [2]Für Maßnahmen der Qualitätssicherung kann die Vernichtung oder Rückgabe aufgeschoben werden.

(3) [1]Jede Behörde einer Kommune oder sonstigen der Aufsicht des Landes unterstehenden juristischen Person des öffentlichen Rechts kann, soweit sie Akten elektronisch führt, Dokumente in Papierform oder Aktenbestandteile in anderer körperlicher Form nach Maßgabe des Absatzes 1 Sätze 1 und 2 übertragen. [2]Sind Dokumente in Papierform oder Aktenbestandteile in anderer körperlicher Form nach Satz 1 übertragen und zur elektronischen Akte genommen worden, so können sie vernichtet oder zurückgegeben werden, wenn eine Aufbewahrung aus rechtlichen Gründen nicht erforderlich ist.

§ 12

Basisdienste

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

1. für die elektronischen Zugänge nach § 4 Abs. 1 bis 3 dieses Gesetzes und § 2 Abs. 1 EGovG,
2. für den elektronischen Identitätsnachweis nach § 4 Abs. 4,
3. für die Zurverfügungstellung von Informationen und Bereitstellung von Formularen über das niedersächsische Verwaltungsportal 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 elektronische Bezahlmöglichkeit nach § 6 Abs. 1 und 2 dieses Gesetzes sowie § 4 EGovG,
6. für den Empfang und die Verarbeitung elektronischer Rechnungen nach § 6 Abs. 3 und 4 sowie
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 nach § 9 bereit. [3]Jede Behörde des Landes kann im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung andere Basisdienste für die in den Sätzen 1 und 2 genannten Funktionen und Basisdienste für andere Funktionen bereitstellen. [4]Das Einvernehmen kann nur verweigert werden, wenn die Zweckmäßigkeit oder Wirtschaftlichkeit des Basisdienstes nicht erkennbar ist. [5]Die Behörden des Landes können sich bei der Bereitstellung von Basisdiensten Dritter bedienen.

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

(3) [1]Jede Behörde einer Kommune oder sonstigen der Aufsicht des Landes unterstehenden juristischen Person des öffentlichen Rechts hat ihre Verpflichtungen nach § 4 Abs. 2, § 5 Abs. 1 und 2 und § 9 dieses Gesetzes sowie nach § 3 Abs. 1 und 2 EGovG mit den nach Absatz 1 Sätze 1 und 2 bereitgestellten Basisdiensten zu erfüllen. [2]Der Basisdienst für den elektronischen Zugang über Nutzerkonten nach § 4 Abs. 2 sowie die Basisdienste nach Absatz 1 Satz 1 Nrn. 3 und 4 werden den in Satz 1 genannten Behörden kostenfrei zur Nutzung bereitgestellt.

Dritter Teil

Informationssicherheit

Erster Abschnitt

Allgemeine Vorschriften

§ 13

Sicherheitsverbund

(1) [1]Die Behörden und Gerichte des Landes, deren IT-Systeme mit dem Landesdatennetz verbunden sind, sind Mitglieder eines Sicherheitsverbundes. [2]Jedes Mitglied des Sicherheitsverbundes hat auf der Basis von Risikoanalysen eine dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene Informationssicherheit, auch in Hinblick auf andere Mitglieder des Sicherheitsverbundes, zu gewährleisten. [3]Jedes Mitglied des Sicherheitsverbundes hat die nach Satz 2 erforderlichen technischen und organisatorischen Maßnahmen unverzüglich zu veranlassen und regelmäßig zu überprüfen und anzupassen.

(2) Die das Landesdatennetz betreibende Behörde kann einer Stelle, die nicht Mitglied des Sicherheitsverbundes ist, die Verbindung ihrer IT-Systeme mit dem Landesdatennetz gestatten, wenn sie sich verpflichtet, die in Absatz 1 Sätze 2 und 3 sowie in § 14 Abs. 2 genannten Pflichten einzuhalten.

§ 14

Zentralstelle für Informationssicherheit

(1) Bei dem für die zentrale IT-Steuerung zuständigen Ministerium ist eine Zentralstelle für Informationssicherheit eingerichtet, die

1. fortlaufend ein Sicherheitslagebild über Bedrohungen für und Angriffe auf IT-Systeme erstellt,
2. das Sicherheitslagebild mit dem Ziel analysiert, Veränderungen der Gefahrenlage zu erkennen, und aus dieser Analyse, auch unter Berücksichtigung einer Gesamtschau der Risikoanalysen, Hinweise zur Anpassung der Gesamtheit der technischen und organisatorischen IT-Sicherheitsmaßnahmen entwickelt sowie
3. die Mitglieder des Sicherheitsverbundes zu Fragen der IT-Sicherheit berät und bei Sicherheitsvorfällen unterstützt.

(2) Jedes Mitglied des Sicherheitsverbundes ist verpflichtet, der Zentralstelle für Informationssicherheit Sicherheitsvorfälle in einer von ihr vorgegebenen Form unverzüglich mitzuteilen, wenn diese geeignet sind, auch die IT-Sicherheit bei anderen Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, zu beeinträchtigen.

(3) Jede Stelle, die Befugnisse nach dem Zweiten Abschnitt wahrnimmt, ist verpflichtet, der Zentralstelle für Informationssicherheit den Betrieb von IT-Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit anzuzeigen.

§ 15

Förderung der IT-Sicherheit

(1) [1]Die das Landesdatennetz betreibende Behörde fördert die IT-Sicherheit im Landesdatennetz mit Ausnahme des Netzabschnitts des Geschäftsbereichs des Justizministeriums. [2]Im Netzabschnitt des Geschäftsbereichs des Justizministeriums fördert eine vom Justizministerium bestimmte Stelle die IT-Sicherheit.

(2) Die in Absatz 1 genannten Stellen haben jeweils für ihren Netzabschnitt die Aufgabe,

1. durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit 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 IT-Systeme mit dem Landesdatennetz verbunden sind, zur Verfügung zu stellen,
3. Sicherheitsvorkehrungen für das Landesdatennetz zu planen, um künftige Gefahren für die IT-Sicherheit abwehren zu können,
4. die Zentralstelle für Informationssicherheit nach deren Vorgaben zu unterstützen.

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

1. sicherheitstechnische Anforderungen an die von den Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, einzusetzende Informationstechnik und an die Verbindung von Netzen und IT-Systemen mit dem Landesdatennetz zu entwickeln und fortzuschreiben,
2. den Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, informationstechnische Verfahren und Geräte für die IT-Sicherheit (IT-Sicherheitsprodukte) bereitzustellen,
3. die Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, im Benehmen mit der Zentralstelle für Informationssicherheit bei der Förderung der IT-Sicherheit zu unterstützen sowie
4. die Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, in herausgehobenen Fällen bei der Wiederherstellung der IT-Sicherheit zu unterstützen.

(4) Die in Absatz 1 genannten Stellen sind verpflichtet, in ihrem jeweiligen Netzabschnitt dem Stand der Technik entsprechende IT-Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit zu betreiben.

§ 16

Vorübergehende und unaufschiebbare Maßnahmen

[1]Bei einer gegenwärtigen Gefahr für die IT-Sicherheit kann die oder der IT-Bevollmächtigte der Landesregierung ein Mitglied des Sicherheitsverbundes anweisen, vorübergehende und unaufschiebbare Maßnahmen zu ergreifen, die zur Gewährleistung der IT-Sicherheit bei anderen Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, erforderlich sind. [2]Satz 1 gilt nicht für Maßnahmen nach dem Zweiten Abschnitt.

Zweiter Abschnitt

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

§ 17

Übertragung und Beschränkung der Befugnisse nach diesem Abschnitt

(1) Jede Behörde kann ihre Befugnisse nach diesem Abschnitt im Einvernehmen mit der das Landesdatennetz betreibenden Behörde auf diese übertragen; das Recht der kommunalen Zusammenarbeit bleibt unberührt.

(2) Soweit der Datenverkehr mit dem Landesrechnungshof, mit der von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde oder mit der Landtagsverwaltung betroffen ist, dürfen die Befugnisse nach diesem Abschnitt nur im Einvernehmen mit dieser Behörde wahrgenommen werden.

(3) Im Netzabschnitt des Geschäftsbereichs des Justizministeriums und in den damit verbundenen lokalen Netzen der Stellen aus dem Geschäftsbereich des Justizministeriums werden die Befugnisse nach diesem Abschnitt von einer vom Justizministerium bestimmten Stelle wahrgenommen.

(4) Die Befugnisse nach diesem Abschnitt stehen den Hochschulen und Einrichtungen des Landes, die mit Forschungsaufgaben betraut sind, nicht zu.

§ 18

Automatisierte Erhebung und Auswertung von Daten eines Verzeichnis- und Berechtigungsdienstes

(1) Jede Behörde kann den personenbezogenen Datenverkehr eines Verzeichnis- und Berechtigungsdienstes auf einem von ihr betriebenen, mit dem Landesdatennetz verbundenen IT-System automatisiert erheben und auswerten, soweit dies zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren, erforderlich ist.

(2) Die nach Absatz 1 erhobenen Daten sowie die Auswertungsergebnisse sind unverzüglich zu löschen, soweit sie zu dem in Absatz 1 genannten Zweck nicht mehr erforderlich sind.

§ 19

Automatisierte Auswertung von Ereignisdokumentationen und Datenverkehr

(1) [1]Jede Behörde kann auf den von ihr betriebenen, mit dem Landesdatennetz verbundenen IT-Systemen die dort zum Erkennen und Nachverfolgen von Auffälligkeiten gespeicherten personenbezogenen Daten nach Maßgabe der Sätze 2 und 3 automatisiert auswerten, soweit dies zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren, erforderlich ist. [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. Betriebssoftware und Anwendungen von Computersystemen

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

(2) [1]Jede Behörde kann an den von ihr betriebenen, mit dem Landesdatennetz verbundenen Übergabe- und Knotenpunkten nach Maßgabe des Satzes 2 nach auffälligem Datenverkehr suchen, soweit dies zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren, erforderlich ist. [2]Der an den Übergabe- und Knotenpunkten anfallende personenbezogene Datenverkehr darf automatisiert erhoben, entschlüsselt und unverzüglich automatisiert ausgewertet werden.

(3) Werden nach Absatz 1 oder 2 Inhalte einer Telekommunikation (Inhaltsdaten) verarbeitet, so ist die Auswertung ihrer kommunikativen Bedeutung unzulässig.

(4) [1]Ergibt die Auswertung nach Absatz 1 oder 2 keine zureichenden tatsächlichen Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so sind die nach Absatz 1 oder 2 erhobenen und ausgewerteten Daten sowie die Auswertungsergebnisse unverzüglich zu löschen. [2]Die Speicherung und sonstige Verarbeitung der nach Absatz 1 ausgewerteten Daten nach dem ursprünglichen Verwendungszweck bleiben von Satz 1 unberührt.

§ 20

Weitere Auswertung ohne Inhaltsdaten in Verdachtsfällen

(1) [1]Ergibt eine automatisierte Auswertung nach § 18 Abs. 1 oder § 19 Abs. 1 oder 2 zureichende tatsächliche Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so kann die Behörde die nach § 18 Abs. 1 oder § 19 Abs. 1 oder 2 erhobenen und ausgewerteten Daten sowie die Auswertungsergebnisse zusammenführen, höchstens 30 Tage speichern und in dieser Zeitspanne weiter einzelfallbezogen automatisiert auswerten, soweit dies zur Erkennung oder Abwehr der Gefahr erforderlich ist. [2]Die nach Satz 1 gespeicherten Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind. [3]Ergibt die Auswertung nach Satz 1 keine hinreichenden tatsächlichen Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so sind die gespeicherten Daten sowie die Auswertungsergebnisse unverzüglich zu löschen.

(2) [1]Ergibt eine automatisierte Auswertung nach § 18 Abs. 1 oder § 19 Abs. 1 oder 2 oder eine weitere automatisierte Auswertung nach Absatz 1 hinreichende tatsächliche Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so dürfen die Daten über den Ablauf der in Absatz 1 Satz 1 bestimmten Frist hinaus gespeichert, auch nicht automatisiert ausgewertet und entpseudonymisiert werden, soweit und solange dies zur Erkennung oder Abwehr der Gefahr erforderlich ist. [2]Die weitere Auswertung nach Satz 1 bedarf der Anordnung der Behördenleitung im Einvernehmen mit einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [3]Wenn eine solche Person nicht beschäftigt ist oder aus anderen Gründen nicht zur Verfügung steht, tritt an deren Stelle eine bei der Aufsichtsbehörde beschäftigte und von deren Behördenleitung bestimmte Person mit der Befähigung zum Richteramt. [4]Ergibt die Auswertung nach Satz 1 tatsächliche Anhaltspunkte für eine andere durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so dürfen die Daten auch gespeichert und nicht automatisiert ausgewertet werden, soweit und solange dies zur Erkennung oder Abwehr der anderen Gefahr erforderlich ist; die Sätze 2 und 3 gelten entsprechend.

(3) Nach den Absätzen 1 und 2 dürfen keine Inhaltsdaten gespeichert oder ausgewertet werden.

(4) Soweit die nach Absatz 2 ausgewerteten Daten sowie die Auswertungsergebnisse nicht mehr für die dort genannten Zwecke oder eine Übermittlung nach § 29 erforderlich sind, sind sie unverzüglich zu löschen.

§ 21

Weitere Auswertung von Inhaltsdaten in Verdachtsfällen

(1) [1]Ergibt eine automatisierte Auswertung nach § 19 Abs. 1 oder 2 zureichende tatsächliche Anhaltspunkte dafür, dass die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr für die IT-Sicherheit erforderlich sind, so kann die Behörde abweichend von § 20 Abs. 3 auch Inhaltsdaten und Auswertungsergebnisse höchstens 30 Tage speichern und in dieser Zeitspanne weiter einzelfallbezogen automatisiert auswerten, soweit und solange dies zur Erkennung oder Abwehr der Gefahr erforderlich ist; die Auswertung der kommunikativen Bedeutung der Inhaltsdaten ist unzulässig. [2]Die nach Satz 1 gespeicherten Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind. [3]Die Speicherung nach Satz 1 bedarf der unverzüglichen Genehmigung der Behördenleitung im Einvernehmen mit einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]Wenn eine solche Person nicht beschäftigt ist oder aus anderen Gründen nicht zur Verfügung steht, tritt an deren Stelle eine bei der Aufsichtsbehörde beschäftigte und von deren Behördenleitung bestimmte Person mit der Befähigung zum Richteramt. [5]Wird die Genehmigung abgelehnt oder nicht unverzüglich erteilt, so sind die gespeicherten Inhaltsdaten sowie die Auswertungsergebnisse unverzüglich zu löschen. [6]Ergibt die Auswertung nach Satz 1 keine hinreichenden tatsächlichen Anhaltspunkte dafür, dass die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr für die IT-Sicherheit erforderlich sind, so sind die gespeicherten Inhaltsdaten sowie die Auswertungsergebnisse unverzüglich zu löschen.

(2) [1]Ergibt eine automatisierte Auswertung nach § 19 Abs. 1 oder 2 oder eine weitere automatisierte Auswertung nach Absatz 1 hinreichende tatsächliche Anhaltspunkte dafür, dass die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr für die IT-Sicherheit erforderlich sind, so dürfen die Daten über den Ablauf der in Absatz 1 Satz 1 bestimmten Frist hinaus gespeichert, auch nicht automatisiert ausgewertet und entpseudonymisiert werden, soweit und solange dies zur Erkennung oder Abwehr der Gefahr erforderlich ist; die Auswertung der kommunikativen Bedeutung der Inhaltsdaten ist unzulässig. [2]Die weitere Auswertung nach Satz 1 bedarf der Anordnung der Behördenleitung im Einvernehmen mit einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [3]Wenn eine solche Person nicht beschäftigt ist oder aus anderen Gründen nicht zur Verfügung steht, tritt an deren Stelle eine bei der Aufsichtsbehörde beschäftigte und von deren Behördenleitung bestimmte Person mit der Befähigung zum Richteramt. [4]Ergibt die Auswertung nach Satz 1 tatsächliche Anhaltspunkte für eine andere durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so dürfen die Daten auch gespeichert und nicht automatisiert ausgewertet werden, soweit und solange dies zur Erkennung oder Abwehr der anderen Gefahr erforderlich ist; die Sätze 2 und 3 gelten entsprechend.

(3) Soweit die nach Absatz 2 ausgewerteten Daten sowie die Auswertungsergebnisse nicht mehr für die dort genannten Zwecke oder eine Übermittlung nach § 29 erforderlich sind, sind sie unverzüglich zu löschen.

(4) [1]Sind nach Absatz 2 ausgewertete Daten dem Kernbereich privater Lebensgestaltung oder besonderen Kategorien personenbezogener Daten (Artikel 9 der Datenschutz-Grundverordnung) zuzurechnen oder geeignet, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen, so dürfen diese nicht gespeichert, verändert, genutzt oder übermittelt werden; sie sind unverzüglich zu löschen. [2]Satz 1 gilt auch in Zweifelsfällen. [3]Die Tatsache, dass in den Sätzen 1 und 2 genannte Daten ausgewertet wurden, und die Löschung dieser Daten sind zu dokumentieren. [4]Die in der Dokumentation enthaltenen Daten dürfen ausschließlich zur Datenschutzkontrolle verwendet werden. [5]Sie sind zu löschen, wenn seit einer Benachrichtigung nach § 26 Abs. 1 Satz 1 ein Jahr vergangen ist, frühestens jedoch zwei Jahre nach der Dokumentation, es sei denn, die oder der Landesbeauftragte für den Datenschutz zeigt an, dass die Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden.

§ 22

Ergänzende Auswertung durch das Bundesamt für Sicherheit in der Informationstechnik

[1]Jede Behörde, die selbst IT-Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit betreibt, kann das Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragen, den von ihr nach § 19 Abs. 2 erhobenen Datenverkehr, dessen automatisierte Auswertung keine zureichenden

oder hinreichenden tatsächlichen Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit ergeben hat, ergänzend auszuwerten und den Datenverkehr zu diesem Zweck an das BSI übermitteln. [2]Der Auftrag darf nur erteilt werden, wenn

1. die ergänzende Auswertung durch das BSI nur nach Maßgabe der §§ 20 und 21 erfolgt und über die dabei erforderlichen Anordnungen oder Genehmigungen von der beauftragenden Behörde entschieden wird,
2. das BSI die Auswertungsergebnisse der beauftragenden Behörde unverzüglich zur Verfügung stellen wird,
3. eine Verwendung der personenbezogenen Daten durch das BSI zu anderen Zwecken als zur ergänzenden Auswertung unzulässig ist,
4. die Daten nach Maßgabe des § 25 verarbeitet sowie nach Abschluss der ergänzenden Auswertung unverzüglich gelöscht werden und
5. das BSI in geeigneter Weise Nachweise dafür erbringen kann, dass die übermittelten Daten ordnungsgemäß verarbeitet und gelöscht werden.

[3]Die ergänzende Auswertung des BSI erfolgt ausschließlich nach Weisung der beauftragenden Behörde.

§ 23

Speicherung und Auswertung von Daten zur Abwehr einer dringenden Gefahr für die IT-Sicherheit

(1) [1]Jede Behörde kann den nach § 19 Abs. 2 erhobenen Datenverkehr zu dem Zweck, durch Schadprogramme oder Angriffe verursachte, im Hinblick auf das Ausmaß des zu erwartenden Schadens und die Wahrscheinlichkeit des Schadenseintritts erhöhte Gefahren für die IT-Sicherheit im gesamten Landesdatennetz (dringende Gefahren für die IT-Sicherheit) abzuwehren, automatisiert speichern. [2]Die gespeicherten Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind; nach höchstens 30 Tagen sind die Daten zu löschen.

(2) [1]Soweit und solange es zur Abwehr einer dringenden Gefahr für die IT-Sicherheit unerlässlich ist, dürfen die nach Absatz 1 Satz 1 gespeicherten Daten automatisiert und nicht automatisiert ausgewertet, entpseudonymisiert sowie über den Ablauf der in Absatz 1 Satz 2 bestimmten Frist hinaus gespeichert werden; die Auswertung der kommunikativen Bedeutung von Inhaltsdaten ist unzulässig. [2]§ 21 Abs. 4 gilt entsprechend.

(3) [1]Maßnahmen nach Absatz 2 bedürfen der Anordnung des Amtsgerichts, in dessen Bezirk die Behörde ihren Sitz hat. [2]Im Antrag der Behörde sind der Sachverhalt und eine Begründung anzugeben. [3]Die Anordnung ergeht schriftlich. [4]Sie muss den Sachverhalt und die wesentlichen Gründe enthalten. [5]Für das gerichtliche Verfahren gilt § 19 Abs. 4 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) entsprechend. [6]Bei Gefahr im Verzug kann die Behördenleitung die Anordnung treffen; die Sätze 3 und 4 gelten entsprechend mit der Maßgabe, dass die Anordnung auch eine Begründung der Gefahr im Verzug enthalten muss. [7]Die richterliche Bestätigung der Anordnung ist unverzüglich zu beantragen. [8]Wird die Bestätigung abgelehnt, so tritt die Anordnung außer Kraft. [9]Die Daten und die Auswertungsergebnisse dürfen in diesem Fall nicht mehr verwendet werden und sind unverzüglich zu löschen; die Speicherung nach Absatz 1 bleibt unberührt.

(4) Soweit die nach Absatz 2 verarbeiteten Daten sowie die Auswertungsergebnisse nicht mehr für den dort genannten Zweck oder eine Übermittlung nach § 29 erforderlich sind, sind sie unverzüglich zu löschen; die Speicherung nach Absatz 1 bleibt unberührt.

§ 24

Beseitigung von Schadprogrammen

[1]Soweit die Auswertungen nach den §§ 18 bis 23 ein Schadprogramm identifizieren, kann dieses jederzeit beseitigt oder in seiner Funktionsweise gehindert werden. [2]Soweit Daten von dem Schadprogramm nicht oder nur mit unverhältnismäßigem Aufwand getrennt werden können, kann die Behörde diese Daten gemeinsam mit dem Schadprogramm löschen.

§ 25

Datensicherheit, Protokollierung

(1) [1]Die nach den §§ 18 bis 23 verarbeiteten Daten sowie die Auswertungsergebnisse 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. sind der Zutritt zu den und der Zugriff auf die Datenverarbeitungsanlagen auf Personen zu beschränken, die durch die jeweilige Behördenleitung hierzu besonders ermächtigt sind,
2. ist organisatorisch sicherzustellen, dass eine Kenntnisnahme der nach den §§ 18 bis 23 verarbeiteten Daten sowie der Auswertungsergebnisse durch andere als die nach Nummer 1 ermächtigten Personen ausgeschlossen ist,
3. ist sicherzustellen, dass die für Datenverarbeitung nach den §§ 18 bis 23 verwendeten IT-Systeme von den für die üblichen betrieblichen Aufgaben verwendeten IT-Systemen getrennt sind, insbesondere die Speicherung in gesonderten Speichereinrichtungen erfolgt,
4. sind besondere Sicherungsmaßnahmen gegen den unberechtigten Zugriff aus anderen Netzen, insbesondere aus dem Internet, zu treffen,
5. sind nach dem Stand der Technik als besonders sicher geltende Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit der gespeicherten Daten einzusetzen und
6. ist technisch und organisatorisch sicherzustellen, dass der Zugriff auf die Daten nur gemeinsam durch mindestens zwei nach Nummer 1 ermächtigte Personen erfolgen kann.

(3) [1]Eine Behörde darf von den Ermächtigungen der §§ 18 bis 23 nur Gebrauch machen, wenn sie ein Sicherheitskonzept für die dazu eingesetzten technischen Systeme erstellt und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen aktenkundig gemacht hat. [2]Das Sicherheitskonzept ist alle zwei Jahre einer Revision zu unterziehen. [3]Für jede Veränderung der eingesetzten technischen Systeme gilt Satz 1 entsprechend.

(4) [1]Jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Übermitteln, Löschen und Sperren von nach den §§ 18 bis 23 verarbeiteten Daten sowie von Auswertungsergebnissen ist zu protokollieren. [2]Das Protokoll enthält Zeitpunkt, Art und Zweck des Zugriffs sowie eine eindeutige Kennung der auf die Daten zugreifenden Person. [3]Das Protokoll darf ausschließlich zur Datenschutzkontrolle verwendet werden. [4]Jeder Eintrag in das Protokoll ist zwei Jahre nach seiner Aufnahme zu löschen, es sei denn, die oder der Landesbeauftragte für den Datenschutz zeigt an, dass die Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden.

§ 26

Benachrichtigung der betroffenen Personen

(1) [1]Die von Maßnahmen nach den §§ 18 bis 23 und 29 betroffenen Personen sind unverzüglich, spätestens nach der Abwehr der durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr für die IT-Sicherheit,

zu benachrichtigen. [2]Satz 1 gilt nicht, soweit zur Durchführung der Benachrichtigung in unverhältnismäßiger Weise weitere Daten der betroffenen Personen erhoben werden müssten.

(2) [1]Die Benachrichtigung kann unterbleiben,

1. solange ihr ein in § 29 Abs. 2 Satz 1 genannter Zweck entgegensteht,
2. solange durch das mit der Benachrichtigung verbundene Bekanntwerden einer Sicherheitslücke die IT-Sicherheit gefährdet würde oder
3. wenn die Person nur unerheblich betroffen ist und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat.

[2]Soll eine Benachrichtigung nach Satz 1 Nr. 1 oder 2 unterbleiben, so bedarf dies der Zustimmung des Amtsgerichts, in dessen Bezirk die Behörde ihren Sitz hat; für das gerichtliche Verfahren gilt § 19 Abs. 4 NPOG entsprechend. [3]Soll eine Benachrichtigung nach Satz 1 Nr. 3 unterbleiben, so bedarf dies der Anordnung der Behördenleitung im Einvernehmen mit einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]Wenn eine solche Person nicht beschäftigt ist oder aus anderen Gründen nicht zur Verfügung steht, tritt an deren Stelle eine bei der Aufsichtsbehörde beschäftigte und von deren Behördenleitung bestimmte Person mit der Befähigung zum Richteramt.

§ 27

Dokumentation

[1]Anordnungen, Genehmigungen, Bestätigungen und Zustimmungen nach § 20 Abs. 2 Satz 2, § 21 Abs. 1 Satz 3 und Abs. 2 Satz 2, § 23 Abs. 3 Sätze 1, 6 und 7, § 26 Abs. 2 Sätze 2 und 3 sowie § 29 Abs. 2 Sätze 3 bis 6 sind zu dokumentieren. [2]Die in der Dokumentation enthaltenen personenbezogenen Daten dürfen ausschließlich zur Datenschutzkontrolle verwendet werden. [3]Sie sind zu löschen, wenn seit einer Benachrichtigung nach § 26 Abs. 1 Satz 1 ein Jahr vergangen ist, frühestens jedoch zwei Jahre nach der Dokumentation, es sei denn, die oder der Landesbeauftragte für den Datenschutz zeigt an, dass die Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden.

§ 28

Beteiligung der oder des Landesbeauftragten für den Datenschutz

[1]Jede Behörde, die ihre Befugnisse nach diesem Abschnitt wahrnimmt, legt der oder dem Landesbeauftragten für den Datenschutz einmal jährlich eine Aufstellung über die Datenverarbeitung nach den §§ 18 bis 23, 26 und 29 Abs. 2 sowie die Dokumentation nach § 27 vor. [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.

§ 29

Zweckbindung, Übermittlung personenbezogener Daten

(1) [1]Die nach den §§ 18 bis 23 verarbeiteten personenbezogenen Daten sowie die Auswertungsergebnisse dürfen nicht zu anderen als den dort genannten Zwecken verarbeitet werden. [2]Insbesondere ist die Erstellung von personenbezogenen Profilen zur Vorhersage des Nutzungsverhaltens von natürlichen Personen untersagt.

(2) [1]Jede Behörde soll abweichend von Absatz 1 die nach § 20 Abs. 2, § 21 Abs. 2 oder § 23 Abs. 2 ausgewerteten personenbezogenen Daten sowie die Auswertungsergebnisse übermitteln

1. an die Strafverfolgungsbehörden, wenn dies zur Verfolgung einer Straftat erforderlich ist und die Strafverfolgungsbehörden die Daten mit einer Maßnahme nach § 100 a oder § 100 g der Strafprozessordnung (StPO) hätten erheben dürfen,
2. an die Polizeibehörden des Bundes und der Länder, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,
3. an die Verfassungsschutzbehörde des Landes, wenn dies zur Erfüllung der Aufgabe nach § 3 Abs. 1 des Niedersächsischen Verfassungsschutzgesetzes erforderlich ist und die Verfassungsschutzbehörde die Daten mit einer Maßnahme nach § 20 des Niedersächsischen Verfassungsschutzgesetzes oder § 3 des Artikel 10-Gesetzes hätte erheben dürfen.

[2]Die Übermittlung von Daten einer in § 53 oder § 53 a StPO genannten Person, über die diese das Zeugnis verweigern dürfte, ist unzulässig. [3]Eine Übermittlung nach Satz 1 Nr. 1 oder 2 bedarf der vorherigen Zustimmung des Amtsgerichts, in dessen Bezirk die übermittelnde Behörde ihren Sitz hat; für das gerichtliche Verfahren gilt § 19 Abs. 4 NPOG entsprechend. [4]Eine Übermittlung nach Satz 1 Nr. 3 bedarf der vorherigen Zustimmung der nach § 3 Abs. 1 Sätze 1 bis 4 des Niedersächsischen Gesetzes zur Ausführung des Artikel 10-Gesetzes (Nds. AG G 10) bestellten G 10-Kommission; § 3 Abs. 1 Sätze 5 bis 7 und Abs. 2 bis 4 Nds. AG G 10 gilt entsprechend. [5]Bei Gefahr im Verzug kann die Behördenleitung anordnen, dass die Daten vor der nach Satz 3 oder 4 erforderlichen Zustimmung übermittelt werden. [6]In diesem Fall ist unverzüglich die nachträgliche Zustimmung einzuholen. [7]Wird die nachträgliche Zustimmung abgelehnt, so tritt die Anordnung außer Kraft. [8]Die bereits übermittelten Daten dürfen in diesem Fall nicht verwendet werden und sind unverzüglich zu löschen; die empfangende Stelle ist darüber zu unterrichten.

(3) Wurde durch Maßnahmen nach den §§ 18 bis 23 eine Sicherheitslücke, ein Schadprogramm oder ein Angriff festgestellt, so kann jede Behörde Auswertungsergebnisse, soweit erforderlich auch einschließlich der darin enthaltenen personenbezogenen Daten, an Stellen übermitteln, deren IT-Systeme mit dem Landesdatennetz verbunden sind, wenn dies zur Abwehr von durch die Sicherheitslücke, das Schadprogramm oder den Angriff verursachten Gefahren für die IT-Sicherheit erforderlich ist.

§ 30

Einschränkung von Grundrechten

Das Fernmeldegeheimnis nach Artikel 10 Abs. 1 des Grundgesetzes wird durch die §§ 19 bis 24 und 29 eingeschränkt.

Artikel 2

Änderung des Niedersächsischen Beamtengesetzes

Nach § 92 des Niedersächsischen Beamtengesetzes vom 25. März 2009 (Nds. GVBl. S. 72), zuletzt geändert durch Artikel 2 des Gesetzes vom 18. Dezember 2018 (Nds. GVBl. S. 317), wird der folgende § 92 a eingefügt:

„§ 92 a

Verarbeitung von Personalaktendaten im Auftrag

(1) [1]Die personalverwaltende Behörde darf nur bei

1. der Bewilligung, Festsetzung oder Zahlbarmachung von Geldleistungen und
2. der automatisierten Erledigung von Aufgaben für Zwecke nach § 88 Abs. 1 Satz 1

gemäß Artikel 28 der Datenschutz-Grundverordnung Personalaktendaten im Auftrag verarbeiten lassen. [2]Eine nicht öffentliche Stelle darf nur beauftragt werden, wenn bei der personalverwaltenden Behörde sonst Störungen im Geschäftsablauf auftreten können oder der Auftragsverarbeiter die Verarbeitungsleistungen erheblich kostengünstiger erbringen kann.

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

(3) Die personalverwaltende Behörde hat die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den oder die Auftragsverarbeiter regelmäßig zu kontrollieren.“

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.

Hannover, den 24. Oktober 2019

Die Präsidentin des Niedersächsischen Landtages

Gabriele Andretta

Das vorstehende Gesetz wird hiermit verkündet.

Der Niedersächsische Ministerpräsident

Stephan Weil