Entwurf

Niedersächsisches Gesetz zur IT-Sicherheit und zu elektronischen Rechnungen

Artikel 1

Niedersächsisches IT-Sicherheitsgesetz (NITG)

§ 1

Zweck und Geltungsbereich

(1) Dieses Gesetz dient der IT-Sicherheit des Landesdatennetzes.

(2) [1]Die Vorschriften dieses Gesetzes gelten für Behörden, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind. [2]Behörde im Sinne dieses Gesetzes ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt. [3]Die Vorschriften dieses Gesetzes gelten entsprechend für die Gerichte.

(3) Die Vorschriften dieses Gesetzes gelten nicht für die Hochschulen in staatlicher Verantwortung und die Landesbibliotheken.

§ 2

Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. IT-Sicherheit die Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten,
2. ein Schadprogramm ein Computerprogramm oder ein Programmteil, das bzw. der bei Ausführung unbefugt die Vertraulichkeit, Verfügbarkeit oder Integrität der verarbeiteten Daten gefährden kann,
3. das Landesdatennetz eine Kommunikationsinfrastruktur, die eine gesicherte 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,
4. Inhaltsdaten Informationen, die bei einem Telekommunikationsvorgang übertragen werden und um derentwillen die Telekommunikation stattfindet und die keine Verkehrsdaten sind,
5. besondere Arten personenbezogener Daten solche, 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.

§ 3

Allgemeine Bestimmungen

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

(2) Soweit die Auswertungen nach den §§ 4 bis 7 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 ausgewertet werden.

§ 4

Auswertung von gespeicherten Daten

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

1. Firewall-Systemen und Systeme 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.

(2) [1]Ergibt die automatisierte Auswertung nach § 4 Abs. 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]Eine Auswertung von Inhaltsdaten im Rahmen des Absatzes 1 ist nur unter den Voraussetzungen des § 7 zulässig.

§ 5

Erhebung und Auswertung des Datenverkehrs

(1) [1]Zur Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme oder Angriffe sind die Behörden ermächtigt, 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 werden. [3]Es dürfen

1. Erhebungszeitpunkt, IP-Adresse einschließlich Subnetzmaske, Präfixlänge, Port und Medienzugriffskontrolladresse (Media-Access-Control-Address, MAC-Adresse), vollständiger Domänennamen 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) zusätzlich zu Nummer 1

der vollständige einheitliche Ressourcenzeiger (Uniform Resource Locator, URL) und die Kopfdaten (ohne Cookie)

unverzüglich automatisiert ausgewertet werden.

(2) [1]Ergibt die automatisierte Auswertung nach § 5 Abs. 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 § 7 zulässig.

§ 6

Auswertung ohne Inhaltsdaten

(1) [1]Soweit die automatisierte Auswertung nach § 4 Abs. 1 oder § 5 Abs. 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass bestimmte Daten zur Abwehr von Gefahren im Sinne des § 4 Abs. 1 Satz 1 oder § 5 Abs. 1 Satz 1 erforderlich sind, dürfen diese weiter 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 § 4 Abs. 1 oder § 5 Abs. 1 durch einen Angriff oder ein Schadprogramm verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben, 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 einer Beschäftigten oder eines Beschäftigten mit der Befähigung zum Richteramt. [4]Die für die Zwecke der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse sind zu löschen, soweit sie nicht mehr erforderlich sind.

§ 7

Auswertung von Inhaltsdaten

(1) [1]Zur Abwehr von Gefahren für die IT-Sicherheit des Landes durch Schadprogrammen oder Angriffe sind die Behörden ermächtigt, die in § 4 Abs. 1 und § 5 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 Auswertung der Daten erfolgt nur automatisiert. [4]Die Datenverarbeitung nach Satz 1 bedarf der Genehmigung einer oder eines Beschäftigten mit der Befähigung zum Richteramt.

(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 durch eine Beschäftigte oder einen Beschäftigten mit der Befähigung zum Richteramt.

(4) Die für den Zweck der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse sind 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, nicht erhoben werden. [2]Werden aufgrund der Maßnahmen nach den Absätzen 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder besondere Arten personenbezogener Daten erlangt, dürfen diese nicht verwendet werden. [3]Die zum Zweck der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse, die den Kernbereich privater Lebensgestaltung betreffen, 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.

§ 8

Dokumentation

[1]Anordnungen nach § 6 Abs. 2 Satz 2, § 7 Abs. 2 Satz 4 und § 7 Abs. 3 Satz 2 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.

§ 9

Gewährleistung der Datensicherheit

(1) [1]Die nach den §§ 4 bis 7 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 Datenverarbeitung nach den §§ 4 bis 7 durch andere als die dafür bestimmten Personen ausgeschlossen ist,
2. sind die IT-Systeme für Datenverarbeitung nach den §§ 4 bis 7 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. ist der Zutritt zu den und Zugriff auf die Datenverarbeitungsanlagen auf Personen zu beschränken, die durch die jeweilige Behördenleitung hierzu besonders ermächtigt sind, und
7. darf der Zugriff auf die Daten nur gemeinsam durch mindestens zwei hierzu besonders ermächtigte Personen erfolgen.

(3) [1]Zum Zweck der Datenschutzkontrolle ist jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren von den nach den §§ 4 bis 7 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 oder dem Landesbeauftragten für den Datenschutz ist einmal im Jahr eine Aufstellung über die nach den §§ 4 bis 7 und 12 erfolgten Verarbeitungen 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.

§ 10

Sicherheitskonzept

[1]Eine Behörde darf von den Ermächtigungen der §§ 4 bis 7 nur Gebrauch machen, wenn ein Sicherheitskonzept erstellt wurde und sie 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.

§ 11

Benachrichtigung der Betroffenen

[1]Die von Maßnahmen nach § 7 Abs. 3 Betroffenen und betroffenen 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. [2]Die Benachrichtigung kann unterbleiben, solange hierdurch der Ermittlungszweck eines Straf- oder Disziplinarverfahrens oder die IT-Sicherheit gefährdet würde.

§ 12

Übermittlung personenbezogener Daten

(1) [1]Die Behörden sollen die Daten nach den §§ 6 und 7 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 Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,
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) Die Behörden können nach § 6 Abs. 2 und § 7 Abs. 3 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.

§ 13

Einschränkung von Grundrechten

Das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes wird durch die §§ 4 bis 7 und 12 eingeschränkt.

Artikel 2

Niedersächsisches Gesetz zu elektronischen Rechnungen (Niedersächsisches E-Rechnungsgesetz – NERG)

§ 1

Geltungsbereich

Dieses Gesetz gilt für die niedersächsischen Auftraggeber nach § 98 des Gesetzes gegen Wettbewerbsbeschränkungen in der Fassung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Artikel 6 Abs. 33 des Gesetzes vom 13. April 2017 (BGBl. I S. 872), in der jeweils geltenden Fassung.

§ 2

Empfang und Verarbeitung elektronischer Rechnungen

(1) [1]Auftraggeber nach § 1 sind ab dem 27. November 2019 verpflichtet, den Empfang und die Verarbeitung elektronischer Rechnungen zu geschlossenen Verträgen über Lieferungen und Leistungen nach Maßgabe der Verordnung nach Absatz 2 sicherzustellen. [2]Eine Rechnung ist elektronisch, wenn sie in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird und das Format die automatische und elektronische Verarbeitung der Rechnung ermöglicht. [3]Bei Vergaben ab dem 27. November 2019 im Anwendungsbereich des Niedersächsischen Tariftreue- und Vergabegesetzes sollen Auftraggeber die Übersendung von Rechnungen in elektronischer Form verlangen.

(2) [1]Die Landesregierung regelt die nähere Ausgestaltung des elektronischen Rechnungsverkehrs in einer Verordnung. [2]Die Ausgestaltung kann sich beziehen auf

1. die Art und Weise des Empfangs und 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, die Verbindlichkeit der elektronischen Form sowie
3. Ausnahmen von den Verpflichtungen nach Absatz 1 im Bereich von sicherheitsspezifischen Aufträgen.

Artikel 3

Inkrafttreten

[1]Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft. [2]Abweichend von Satz 1 tritt Artikel 2 am 27. November 2018 in Kraft.

Begründung

A. Allgemeiner Teil

I. Anlass und Ziele des Gesetzes

Die Digitalisierung führt zu grundlegenden Änderungen in der Gesellschaft. Sie schafft viele Möglichkeiten, birgt aber auch neue Risiken, insbesondere durch Hackerangriffe. Dies betrifft auch die öffentliche Verwaltung, wie man den Medien bereits entnehmen musste und auch zunehmend entnehmen muss. Diese Risiken können aber nur zu einem gewissen Teil getragen werden. Ein Restrisiko bleibt stets bestehen, jedoch muss dieses auf ein zumutbares Minimum reduziert werden, da in der öffentlichen Verwaltung Daten von Bürgerinnen und Bürgern, Unternehmen und Verbänden vorhanden sind, die im höchsten Maße sensibel sind und daher eines angemessenen und umfassenden Schutzes bedürfen.

Das Land Niedersachsen reagiert mit diesem Gesetz auf die Risiken, die sich aus der Digitalisierung ergeben. Dort, wo digitale Verwaltung stattfindet und Daten, insbesondere personenbezogene Daten, elektronisch gespeichert oder übermittelt werden, wird der Schutz der IT-Systeme zu einer fundamentalen Anforderung, um die 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 neuer gesetzlicher Regelungen. Diese Regelungen sind im Bereich der Landesverwaltung zwingend erforderlich, da aktuelle Angriffstechnologien mit den hier etablierten technischen Verfahren – wie portbasierten Firewalls, Virenscannern und Proxies – und im bestehenden Ermächtigungsrechtsrahmen nicht mehr zuverlässig abgewehrt werden können.

Artikel 2 setzt die Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen um. Öffentliche niedersächsische Auftraggeber europaweiter Vergabeverfahren werden dort verpflichtet, elektronische Rechnungen zu geschlossenen Verträgen über Lieferungen und Leistungen spätestens ab dem 27. November 2019 empfangen und verarbeiten zu können. Darüber hinaus sollen in Vergabeverfahren im Geltungsbereich des Niedersächsischen Tariftreue- und Vergabegesetzes bei der Vergabe öffentlicher Aufträge ab 10 000 Euro elektronische Rechnungen verlangt werden. Die Verpflichtung zum Empfang und zur Verarbeitung elektronischer Rechnungen erstreckt sich auch auf den sog. unterschwelligen Bereich, also für Vergaben mit Auftragshöhen unterhalb der jeweils maßgeblichen EU-Schwellenwerte.

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.

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

Auswirkungen auf die Verwirklichung der Gleichstellung von Frauen und Männern und auf Familien sind nicht zu erwarten.

IV. Auswirkungen auf Menschen mit Behinderungen

Dieses Gesetz hat keine Auswirkungen auf Menschen mit Behinderungen.

V. Gesetzesfolgen und voraussichtliche Kosten und haushaltsmäßige Auswirkungen

1. Wirtschaft und Bürgerschaft

Für Bürgerinnen, Bürger, Unternehmen und Verbände außerhalb der Verwaltung entstehen durch Artikel 1 keine Kostenfolgen. Für sie werden Maßnahmen, die einen Erfüllungsaufwand bedeuten würden, nicht eingeführt. Artikel 2 § 2 Satz 3 führt dazu, dass Unternehmen in der Regel Rechnungen in elektronischer Form übersenden müssen, wenn sie sich erfolgreich an Ausschreibungen der Verwaltung beteiligt haben. Dies kann in Ausnahmefällen zu geringfügigen Mehrkosten führen. In der Regel sind hierdurch Einsparungen bei den Unternehmen und in der Verwaltung zu erwarten.

2. Verwaltung

Zunächst ist zu beachten, dass die Landesregierung in ihrer IT-Strategie vom September 2016 die digitale Verwaltung anstrebt. Bereits mit der IT-Strategie hat die Landesregierung die Notwendigkeit anerkannt, umfassend und fortgesetzt in die Modernisierung der IT der Landesverwaltung investieren zu müssen, damit die Daten, die vorhanden sind, sicher gegen unbefugte Nutzung, Weitergabe Betrachtung und Bewertung sind. Entsprechende Maßnahmen werden daher im Rahmen der verfügbaren Haushaltsmittel einen Ausgabeschwerpunkt des Landeskabinetts darstellen.

Finanzielle Auswirkungen im Einzelnen:

Dieses Gesetz gibt den Behörden angesichts zunehmender Cybergefahren die Ermächtigung, zum Zweck der Wahrung der IT-Sicherheit ihrer IT-Infrastruktur Daten automatisiert auszuwerten. Die Regelungen erweitern die Möglichkeiten zur Aufrechterhaltung und Verbesserung der IT-Sicherheit und somit der Informationssicherheit. Es handelt sich um reine Ermächtigungsnormen, ohne zugleich eine Verpflichtung auszusprechen; insofern erzeugen diese Ermächtigungen keine unmittelbaren finanziellen Auswirkungen. Die Behörden müssen jedoch – insbesondere durch eine Risikobewertung – entscheiden, in welchem Umfang sie zur Wahrung der Informationssicherheit der ihnen anvertrauten Daten angesichts der steigenden Cyberbefahren und des zunehmenden Einsatzes von Informationstechnologien zusätzliche Sicherheitstechnologien einsetzen müssen. Die Kosten dafür sind abhängig von den eingesetzten Systemen und den dafür benötigten Personal- und Sachkosten. Eine valide Schätzung der Kosten ist nur bei Festlegung dieser Faktoren möglich, die durch das Gesetz bloß eingeräumten rechtlichen Möglichkeiten reichen dafür nicht aus. Bei der Umsetzung technischer Maßnahmen sollten Effizienzpotenziale genutzt werden, z. B. die zusätzliche Absicherung durch moderne Firewalls, verhaltensbasierte Detektionssysteme, Intrusion-Detection-Systeme und SIEM-Systeme einheitlich und weitgehend zentral und damit kostensparend vorzunehmen.

Die Behörden werden somit in eigener Bewertung entscheiden müssen, ob und inwieweit sie aufgrund der herrschenden Cybergefahren von der Ermächtigung Gebrauch machen. Im Übrigen obliegen diese Behörden ohnehin den Verpflichtungen nach § 7 des Niedersächsischesn Datenschutzgesetzes (NDSG) und ggf. § 109des

Telekommunikationsgesetzes (TKG), dem Stand der Technik entsprechende Sicherheitstechnologien einzusetzen.

Durch diese Regelungen entstehen somit unmittelbar keine neuen Kosten. Vielmehr ermöglichen sie es, Schäden und damit zusätzliche, ungeplante Kosten durch IT-Sicherheitsvorfälle zu vermeiden oder zumindest zu begrenzen. Ungeplante Kosten könnten etwa durch Datenverluste entstehen, die dazu führen, dass die Arbeitsfähigkeit nur mit erheblichen zusätzlichen Personalressourcen oder aufwändiger externer Hilfe wieder hergestellt werden kann. Denkbare Regressforderungen durch Datenmissbrauchsfälle werden vermieden.

Artikel 2 hingegen erfordert ein IT-Verfahren, das E-Rechnungen zu geschlossenen Verträgen über Lieferungen und Leistungen entgegen nehmen und mindestens visualisieren kann (Webportal, E-Poststelle und Ablage für die E-Rechnungen). Hierfür werden 1 200 000 Euro einmalige und 250 000 Euro jährliche Kosten für die Verwaltung erwartet. Dieses zentrale IT-System soll vom zentralen IT-Dienstleister eingeführt und betrieben sowie den Behörden im Geltungsbereich zur Nutzung bereitgestellt werden. Zusätzlich ist eine A 12-Stelle für Koordinierungsaufgaben erforderlich. Die Kosten sollen voraussichtlich von den nutzenden Behörden anteilig getragen werden, auch z. B. von den Kommunen. Gesetzlich zulässig ist auch der Aufbau dezentraler IT-Verfahren zur Annahme von E-Rechnungen. Da hierdurch aber Mehrkosten zu erwarten sind, sollte diese Variante vermieden werden.

Mit der Einführung der E-Rechnung sind Einsparungen zu erwarten, wenn die vollständige Rechnungsbearbeitung in der Verwaltung elektronisch durchgeführt wird. Hierfür müssen die beteiligten Behörden jedoch 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 Kosten hierfür werden hier nicht beziffert, da sie für die Umsetzung der Regelung selbst nicht erforderlich sind.

B. Besonderer Teil

Artikel 1 - Niedersächsisches IT-Sicherheitsgesetz (NITG)

Zu § 1 (Zweck und Geltungsbereich):

Zu Absatz 1:

Absatz 1 beschreibt als Gesetzeszweck die IT-Sicherheit des Landesdatennetzes, wobei der Begriff der IT-Sicherheit in den Begriffsbestimmungen definiert wird. Das Landesdatennetz als digitale Infrastruktur ermöglicht eine gesicherte Kommunikation zwischen den IT-Systemen in den lokalen Netzen der am Landesdatennetz angeschlossenen Behörden untereinander, in das Verbindungsnetz des Bundes und im Übergang zu anderen Behörden. Das Landesdatennetz wird durch das Land selbst zur Verfügung gestellt bzw. im Auftrag des Landes betrieben. Es handelt sich um einen gemeinsamen Sicherheitsverbund, der den teilnehmenden Behörden eine sichere Aufgabenwahrnehmung mit IT-Unterstützung ermöglicht. Zweck des Gesetzes ist daher der Schutz dieser umfassenden und für das Land wichtigen Infrastruktur, um die Aufgaben angemessen und umfassend erfüllen zu können und insbesondere auch, um die Daten der Bürgerinnen und Bürger entsprechend zu sichern.

Zu Absatz 2:

Insofern wurden bewusst nicht alle Behörden in Niedersachsen ermächtigt, sondern auf diejenigen mit einer Verbindung zum Landesdatennetz im Sinne dieses Gesetzes beschränkt, wie sich Absatz 2 entnehmen lässt.

Ein IT-System gilt im Sinne dieses Gesetzes mit dem Landesdatennetz verbunden, wenn es direkt oder über ein behördeneigenes Subnetz (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.

In Satz 2 wird zur Klarstellung der Behördenbegriff aufgenommen. Dieser ist identisch mit § 1 Abs. 4 des Niedersächsischen Verwaltungsverfahrensgesetzes. Um auch den Gerichten die Möglichkeit zu geben, Anomalieerkennungssysteme einzusetzen, dehnt Satz 3 den Geltungsbereich auf diese aus.

Zu Absatz 3:

Absatz 3 nimmt die Hochschulen in staatlicher Verantwortung und die Landesbibliotheken aus dem Geltungsbereich aus. Diese würden zwar auch von der Ermächtigung profitieren, Anomalieerkennungssysteme einsetzen zu können. Aufgrund der besonderen Strukturen, insbesondere der intensiven Vernetzung im Forschungsbereich, ist dort aber ein Sicherheitsmanagement erforderlich, das deutlich vom Sicherheitsmanagement der übrigen Verwaltung abweicht. In der Folge sind dort auch andere Maßnahmen und ggf. Rechtsgrundlagen als im übrigen Bereich der Landesverwaltung sinnvoll.

Zu § 2 (Begriffsbestimmungen):

In § 2 werden zentral die im Gesetz verwendeten Begriffe definiert.

In Nummer 4 werden die Inhaltsdaten legal definiert. Es handelt sich um einen Begriff, der zwar im Telekommunikationsbereich bekannt ist, der aber bisher in keinem vorhandenen Gesetz legal definiert wird. Inhaltsdaten sind die Daten, um derentwillen der Übermittlungsvorgang mittels Telekommunikation überhaupt veranlasst wird (Günther in Münchener Kommentar zur Strafprozessordnung, § 100 a Rn. 49) und um derentwillen die Telekommunikation stattfindet. Da aber auch Verkehrsdaten übertragen werden, wurde eine Negativabgrenzung zu den Verkehrsdaten aufgenommen. Da diese in § 3 Nr. 30 TKG legal definiert sind, werden sie nicht zusätzlich im Rahmen dieses Gesetzestextes definiert.

Zu § 3 (Allgemeine Bestimmungen):

Zu Absatz 1:

§ 3 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 Auswertung der Daten nach diesem Abschnitt ein Schadprogramm erkannt wird, kann dieses jederzeit gelöscht werden. Eine Strafbarkeit, etwa nach § 303 a des Strafgesetzbuchs, ist dann ausgeschlossen.

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 § 4 (Auswertung von gespeicherten Daten):

Zu Absatz 1:

Bei § 4 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 in § 7 NDSG bereits besteht und daher nicht erneut normiert werden muss und darf. Aufgrund der strengen Zweckbindung des § 7 NDSG dürfen die erhobenen Daten bisher nicht für den Zweck der IT-Sicherheit im Sinne dieses § 3 verwendet werden. Die Zweckänderung in diesem Absatz lässt die Auswertung zu diesem Zweck nunmehr zu. Die Behörden dürfen die Daten, mit Ausnahme der Inhaltsdaten, die nach den Anforderungen des § 7 dieses Gesetzes auszuwerten sind, auswerten, um Sicherheitslücken, Schadprogramme oder Angriffe zu erkennen. Satz 1 enthält daher selbst eine strenge Zweckbindung für die Verwendung der bereits auf anderer rechtlicher Grundlage erhobenen Daten.

Von der Ermächtigung können die Behörden, die dem Geltungsbereich dieses Gesetzes unterliegen, Gebrauch machen. Hier wäre auch zu erwägen gewesen, ob eine zentrale Behörde, etwa eine oberste Landesbehörde ermächtigt werden 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 ggf. zu einem erheblichen Eingriff in verfassungsmäßig statuierte Rechte führen. Da es sich allerdings allesamt um Behörden handelt, deren IT-Systeme mit dem Landesdatennetz verbunden sind, ist es notwendig, dass allen die Ermächtigung zur Verfügung steht. 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.

Darum erfasst die Regelung alle IT-Systeme der Behörden, die mit dem Landesdatennetz verbunden im Sinne dieses Gesetzes sind. Sie gilt für die jeweils eigenen IT-Systeme der Behörden, die auch im Auftrag durch Dritte bereitgestellt werden können. Ein IT-System gilt im Sinne dieses Gesetzes mit dem Landesdatennetz verbunden, wenn es direkt oder über ein behördeneigenes Subnetz (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.

Die Systeme, deren automatisierte Ereignisdokumentationen automatisiert untersucht werden können, sind in Absatz 1 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 beispielsweise Router und Switches.

Nummer 2 betrifft die sog. 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 sog. Spam-Filter ausgewertet werden. Spam-Filter arbeiten in der Regel mit sog. 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 u. a. 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 u. a. 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 beispielsweise das Active Directory oder LDAP, erfasst und die Anwendungsserver, die Anwendungsprogramme ausführen, wie beispielsweise die Steuerung von Vorgangsbearbeitungssystemen oder Web-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.

Zu Absatz 2:

Satz 1 trägt dem Grundsatz der Datensparsamkeit 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. Im Rahmen dieses Paragrafen werden nur die Kopien der Daten zu löschen sein, da die Daten selbst in Protokolldateien für andere Zwecke erhoben und ggf. noch gebraucht werden und aus diesem Grund nicht in der Urform gelöscht werden können. Sofern keine Kopien vorliegen, kann außer den Auswertungsergebnissen nichts weiter gelöscht werden, um keine Daten löschen zu müssen, die für die anderen Zwecke, für die sie ursprünglich erhoben wurden, noch benötigt 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 § 6.

Satz 2 stellt klar, dass sich die Auswertung von Inhaltsdaten nicht nach den §§ 5 und 6 richtet, sondern ausschließlich nach § 7. Grund dafür ist die besondere Sensibilität von Inhaltsdaten, sodass für deren Auswertung strengere und weitere Anforderungen zu erfüllen sind.

Zu § 5 (Erhebung und Auswertung des Datenverkehrs):

Zu Absatz 1:

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. Daher 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 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. Es handelt sich um eine automatisierte Erhebung. Satz 3 bringt zum Ausdruck, dass die näher benannten Daten automatisiert ausgewertet werden dürfen, auch dies allerdings nur im Rahmen der Zweckbindung nach Satz 1. Weitergehende Befugnisse bestehen zu diesem Zeitpunkt und nach diesem Absatz nicht, insbesondere ist keine Auswertung durch eine natürliche Person denkbar.

Die Daten, die ausgewertet werden dürfen, sind nach Satz 3 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. Betroffen von der Auswertung sind insofern die im IP-Datenstrom benötigten Informationen für die Steuerung der einzelnen Datenpakete.

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.

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 Datensparsamkeit zu agieren. An dieser Stelle sind anders als im Rahmen des § 4 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 § 7 ausgewertet werden dürfen.

Zu § 6 (Auswertung ohne Inhaltsdaten):

§ 6 trifft Regelungen zur Auswertung aller Daten, die nicht Inhaltsdaten sind. Die Auswertung von Inhaltsdaten erfolgt nur unter den Voraussetzungen und nach den Vorgaben des § 7.

Zu Absatz 1:

Satz 1 lässt eine weitere Auswertung zu, sofern „zureichende tatsächliche Anhaltspunkte“ für eine Gefahr im Sinne von § 4 Abs. 1 Satz 1 oder § 5 Abs. 1 Satz 1 vorliegen. Der Begriff „zureichende tatsächliche Anhaltspunkte“ stammt aus dem strafprozessualen Bereich, § 152 der Strafprozessordnung (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, da Schadprogramme häufig nicht sofort, sondern mit einem zeitlichen Verzug erkannt werden.

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 und dies technisch möglich ist. In den meisten Fällen werden die Daten allerdings bereits pseudonym sein. Durch Satz 2 wird dem Grundsatz der Datensparsamkeit 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 ggf. 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 einem Beschäftigten oder einer Beschäftigten mit der Befähigung zum Richteramt gesondert angeordnet werden muss. Da nach diesem Abschnitt keine heimliche, inhaltliche Überwachung verbunden ist, sondern nur die Suche nach Schadprogrammen erfolgen soll, ist kein Richtervorbehalt erforderlich.

Satz 4 regelt die Löschfrist für die 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 solche, die entweder bereits vorhanden waren und von denen Kopien für die Auswertung nach diesem Gesetz gefertigt wurden oder die im Rahmen des § 5 selbst für die Zwecke dieses Gesetzes erhobenen Daten. Satz 4 dient der Verhältnismäßigkeit der Maßnahme, insbesondere dem Grundsatz der Datensparsamkeit.

Zu § 7 (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 Schadprogramme oder Angriffe zu erhalten. Diese lassen sich in erster Linie anhand der Inhaltsdaten erkennen. Auch in § 7 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 der Daten, eine gesonderte Genehmigung durch eine Beschäftigte oder einen Beschäftigten mit der Befähigung zum Richteramt bereits für die Speicherung fordert. 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 Auswertung der Daten. Durch diese Erfordernisse wird eine natürliche Person nach diesem Absatz keine Kenntnis der Daten erhalten können. Zudem werden natürliche Personen, beispielsweise als Kommunikationsteilnehmer, durch die Pseudonymisierung nicht bekannt werden.

Zu Absatz 3:

Eine weitere Auswertung unter Personenbezug und mit einer Einsichtnahme bzw. 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 eine Beschäftigte oder einen Beschäftigten mit der Befähigung zum Richteramt erfolgen, da es sich nicht nur um technische Details handelt, sondern eine Abwägungen von rechtlichen Aspekten hinzukommt. Insoweit ist stets eine enge Zusammenarbeit zwischen dem technischen und dem juristischem Personal dringend erforderlich, da nur auf diese Weise sachgerechte Entscheidungen zu erwarten sind.

Zu Absatz 4:

Absatz 4 gibt die Löschfrist für die Kopien der Daten, die Daten selbst und die Auswertungsergebnisse vor. Auf die Ausführungen zu § 6 Abs. 2 Satz 4 wird verwiesen.

Zu Absatz 5:

Absatz 5 schützt den Kernbereich der privaten Lebensgestaltung. Dem Kernbereich kann die Kommunikation mit engen persönlichen Vertrauten wie u. a. Ehe- und Lebenspartnern und anderen engen Vertrauten bzw. 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 Bereich 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.

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 § 8 (Dokumentation):

§ 8 dient der Klarstellung und besagt, dass, sofern eine Entscheidung durch eine Beschäftigte oder einen Beschäftigten mit der Befähigung zum Richteramt nach den §§ 6 und 7 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 § 9 (Gewährleistung der Datensicherheit):

In § 9 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, die § 9 macht, resultieren insbesondere aus der Rechtsprechung.

Zu Absatz 1:

Absatz 1 sieht den weiteren Schutz der nach den §§ 4 bis 7 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 §§ 4 bis 7 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.

Zu Absatz 3:

Absatz 3 verpflichtet zur Führung eines Protokolls, in das jeder Zugriff auf die nach den §§ 4 bis 7 gespeicherten Daten aufzuzeichnen 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 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 §§ 4 bis 7 und 12 erfolgten Verarbeitungsvorgänge an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz vor, damit eine unabhängige Instanz ein Lagebild erhält. Diese Vorlage kann gebündelt von einer Stelle erfolgen oder durch die einzelne Behörde, die von der Ermächtigung Gebrauch macht.

Zu § 10 (Sicherheitskonzept):

§ 10 sieht vor der Nutzung der Ermächtigungen in den §§ 4 bis 7 die Vorlage eines Sicherheitskonzepts für das von der Behörde verwendete System zur Datenverarbeitung nach den §§ 4 bis 7 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, die beim Betrieb von IT-Systemen entstehen können, etwa das Risiko von Datenverlusten, 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 § 11 (Benachrichtigung des Betroffenen):

§ 11 sieht grundsätzlich eine Benachrichtigung der Betroffenen vor, deren Inhaltsdaten personenbezogen und nicht automatisiert ausgewertet wurden. Betroffene sind nach § 3 Abs. 1 NDSG natürliche Personen, deren personenbezogene Daten betroffen sind. Grund für die Regelung in § 11 ist eine mögliche Kenntnisnahme der Inhaltsdaten. Jede oder jeder Betroffene 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 Landesbeauftragte oder den Landesbeauftragten für den Datenschutz zu wenden. Eingeschränkt wird dieses Recht jedoch dadurch, dass die Betroffenen bekannt sein müssen oder eine Identifikation mit einem verhältnismäßigen Aufwand möglich ist. Wenn daher beispielsweise in einer E-Mail ein Name genannt wird und über diese Person etwas geschrieben wird, dann wird es in der Regel ein unverhältnismäßiger Aufwand sein, diese Person zu ermitteln. Eine Benachrichtigung kann dann unterbleiben.

Eine weitergehende Benachrichtigungspflicht wurde aus verschiedenen Gründen nicht aufgenommen. Es bedeutet einen erheblichen Aufwand, sämtliche Personen zu benachrichtigen, bei denen beispielsweise eine IP-Adresse erhoben wurde. Diese ist nicht automatisch mit einer E-Mail-Adresse hinterlegt. Zudem würde eine generelle Benachrichtigungspflicht für sämtliche Personen, deren personenbezogene Daten erhoben wurden, dazu führen, dass auch die „Angreifer“, also diejenigen, die Schadsoftware an die Behörden senden, benachrichtigt werden müssten. Es wäre paradox, die „Angreifer“ zu informieren, insbesondere wäre für diese dann klar, dass Schadprogramme nunmehr auf

anderem Wege zugestellt werden müssen. Insofern wurde die Benachrichtigungspflicht deutlich eingeschränkt.

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 unterbleiben kann, wenn sie eine Gefahr für die Ermittlungen in Straf- und Disziplinarverfahren bedeutet.

Zu § 12 (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 Gesetz die Gewährleistung der IT-Sicherheit des Landesnetzes gemäß § 1 Abs. 1 ist, ermöglicht die Übermittlung nach Absatz 1 auch die Verfolgung sonstiger Zwecke. Unter den genannten Voraussetzungen sollen Daten nach den §§ 6 und 7 übermittelt werden. Zu diesen Daten gehören auch solche nach den §§ 4 und 5, die im Rahmen der weiteren Auswertung nach den §§ 6 und 7 erhalten bleiben.

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 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung. 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 entsprechen den Voraussetzungen der o. g. Regelungen zur Telekommunikationsüberwachung.

Zu Absatz 2:

Absatz 2 lässt eine Übermittlung der nach § 6 Abs. 2 und § 7 Abs. 3 verarbeiteten Daten von Behörde zu Behörde bzw. an den damit beauftragten Betrieb zu, wenn sie erforderlich sind, 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 zu beheben und Gefahren eindämmen zu können. 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, etwa weil die andere Behörde oder der beauftragte Betrieb andere Hard- oder Software einsetzt und diese nicht gefährdet ist, so darf eine Übermittlung nicht, auch nicht informationshalber, stattfinden.

Zu § 13 (Einschränkung von Grundrechten):

Durch die Befugnisse nach den §§ 4 bis 7 und 12 wird in das Fernmeldegeheimnis aus Artikel 10 des Grundgesetzes eingegriffen. Durch § 13 wird dem Zitiergebot aus Artikel 19 Abs. 1 des Grundgesetzes Genüge getan.

Artikel 2 - Niedersächsisches E-Rechnungsgesetz (NERG)

Zu § 1 (Geltungsbereich):

Dieses Gesetz 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) in niedersächsisches Recht. Die Richtlinie ist für alle öffentlichen Auftraggeber, insbesondere auch für Konzessionsgeber und Sektorenauftraggeber, umzusetzen. Aus diesem Grund wird auf die entsprechenden Vorschriften im Gesetz gegen Wettbewerbsbeschränkungen (GWB) abgestellt. Es wird zudem klargestellt, dass die Verpflichtung nur für niedersächsische Auftraggeber gilt, die als Aufraggeber nach § 98 GWB einzustufen sind. Dabei sind sowohl Aufträge oberhalb als auch unterhalb der maßgeblichen EU-Schwellenwerte erfasst. Dieses Vorgehen setzt zum einen die Vorgaben der o. g. Richtlinie vollständig um, erweitert aber zum anderen auch den Bereich der Verpflichtung auf den sog. unterschwelligen Bereich.

Zu § 2 (Empfang und Verarbeitung elektronischer Rechnungen):

§ 2 setzt die Richtlinie 2014/55/EU in niedersächsisches Recht um. Hier wird an den Begriff des Auftraggebers in § 1 angeknüpft. Anders als bei der Richtlinie 2014/55/EU umfasst die Regelung nicht nur Rechnungen, die infolge einer europaweiten Ausschreibung entstehen, sondern alle Rechnungen, auch jene 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 (oberschwelliger Bereich) elektronisch angenommen werden und andere nicht. Insbesondere würde eine reine Erfassung lediglich des oberschwelligen Bereichs dazu führen können, das 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.

In Absatz 1 Satz 1 wird die Pflicht der Auftraggeber normiert, elektronische Rechnungen ab dem 27. November 2019 entgegenzunehmen und zu verarbeiten. Hier wird an den Begriff des Auftraggebers nach § 1 angeknüpft. Dieser Begriff wird auch in der umzusetzenden Richtlinie verwendet. Für die Verarbeitung reichen eine Visualisierung der Rechnung und eine anschließende papierbasierte Bearbeitung aus, obgleich dies in der Sache nicht zweckdienlich wäre und eine rein elektronische Weiterverarbeitung der zu bevorzugende Weg wäre.

In Satz 2 erfolgt eine Definition der elektronischen Rechnung. 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. In Satz 3 wird die Verpflichtung der o. g. Auftraggeber geregelt, in Vergabeverfahren die elektronische Rechnungsstellung zu verlangen. Diese sollen in ihren Vergabeunterlagen die E-Rechnung zur Pflicht machen. Die Regelung ist als Soll-Regelung formuliert, um Ausnahmen in Einzelfällen zuzulassen, z. B. wenn die elektronische Übersendung für Auftraggeber oder Auftragnehmer nicht zumutbar ist. Durch die Regelung in Satz 2 ist zudem klargestellt, dass das Verlangen elektronischer Rechnungen erst ab einem Betrag von 10 000 Euro (Eingangsschwelledes Niedersächsischen Tariftreue- und Vergabegesetzes) greift. Insofern sind kleinere und mittlere Unternehmen ausreichend geschützt und müssen nicht zwangsläufig elektronische Rechnungen stellen.

Die Verpflichtungen nach den Sätzen 1 und 3 gelten erst ab dem 27. November 2019. Damit wird der mögliche Spielraum für die Verschiebung der Verpflichtung (30 Monate nach Veröffentlichung der europäischen Norm durch das CEN) weitgehend ausgeschöpft. Hierdurch bleibt genügend Zeit zur Einführung eines geeigneten elektronischen Verfahrens.

In Absatz 2 wird eine Verordnungsermächtigung für die Einzelheiten, also das Verfahren der Verarbeitung, die Verwendung von Standards und die Möglichkeit von Ausnahmen, normiert. Dies ist u. a. erforderlich, weil sich der technische Standard der elektronischen Rechnung aufgrund der technischen Entwicklung verändern kann.

In Absatz 2 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 bestimmten Rahmen vorgegeben wird. Nummer 3 ermächtigt die Landesregierung, Ausnahmen von den Verpflichtungen nach Absatz 1 im Bereich von sicherheitsspezifischen Aufträgen zuzulassen.

Artikel 3 - Inkrafttreten

Satz 1 regelt das Inkrafttreten des Gesetzes. Das Niedersächsische IT-Sicherheitsgesetz tritt am Tag nach seiner Verkündung in Kraft.

Satz 2 regelt das abweichende Inkrafttreten des Artikels 2: das Niedersächsische E-Rechnungsgesetz tritt entsprechend den Vorgaben aus der Richtlinie 2014/55/EU am 27. November 2018 in Kraft.