Schriftlicher Bericht

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

Gesetzentwurf der Landesregierung - Drs. 18/1598

Beschlussempfehlung des Ausschusses für Inneres und Sport - Drs. 18/4678

Berichterstattung: Abg. Bernd Lynack (SPD)

Der Ausschuss für Inneres und Sport empfiehlt Ihnen in der Drucksache 18/4678, den Gesetzentwurf mit den aus der Beschlussempfehlung ersichtlichen Änderungen anzunehmen. Diese Beschlussempfehlung kam im federführenden Ausschuss mit den Stimmen der Ausschussmitglieder der Fraktionen von SPD und CDU gegen die Stimmen der Ausschussmitglieder der Fraktionen von Bündnis 90/Die Grünen und FDP bei Enthaltung des Ausschussmitglieds der Fraktion der AfD zustande. Die mitberatenden Ausschüsse für Rechts- und Verfassungsfragen sowie für Haushalt und Finanzen schlossen sich dieser Beschlussempfehlung jeweils mit demselben Abstimmungsergebnis an.

Der Gesetzentwurf wurde am 13. September 2018 direkt an den Ausschuss für Inneres und Sport überwiesen und dort am 20. September 2018 von einem Vertreter des Ministeriums für Inneres und Sport (MI) mündlich eingebracht und im Sinne der Gesetzesbegründung erläutert. Er dient dazu, auch in Niedersachsen die elektronische Kommunikation mit der Verwaltung zu erleichtern sowie Land und Kommunen die Möglichkeit zu eröffnen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten. Zudem sollen die gesetzlichen Vorgaben geschaffen werden, um die Ziele des (Bundes-)Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG) in Niedersachsen vollständig, rechtzeitig und systematisch umzusetzen. Darüber hinaus setzt das Gesetz die EU-Richtlinie über die elektronische Rechnungsstellung bei öffentlichen Aufträgen aus dem Jahr 2014 in Niedersachsen um. Ein gewichtiger Teil des Gesetzes dient der Abwehr von Risiken, die sich aus der Digitalisierung der Verwaltung ergeben. Den immer ausgereifteren Hackerangriffen kann nur erfolgreich begegnet werden, wenn die Verwaltung angemessene Abwehrmaßnahmen treffen kann. Das Gesetz enthält die dazu erforderlichen neuen Regelungen.

Der federführende Ausschuss hat zu dem Gesetzentwurf am 21. Februar 2019 eine mündliche Anhörung mehrerer Vertreterinnen und Vertreter von Behörden und Unternehmen durchgeführt, u. a. der Arbeitsgemeinschaft der kommunalen Spitzenverbände und der Landesbeauftragten für den Datenschutz (LfD).

Die Fraktionen der SPD und der CDU haben zu dem Gesetzentwurf einen Änderungsvorschlag eingebracht, der insbesondere eine Öffnungsklausel ergänzt, die es ermöglichen soll, auch die spezielle Technik zur Erkennung von Schadsoftware sowie die langjährige Expertise des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) bei der Auswertung des Netzverkehrs zu nutzen (vgl. im Einzelnen die Empfehlung zu Artikel 1 § 22/1). Zudem enthält der Änderungsvorschlag eine Vorschrift, die es ermöglichen soll, den Netzverkehr der Behörden für bis zu 30 Tage zu speichern, um dessen retrograde Auswertung zu ermöglichen. Dadurch soll es möglich werden, Angriffe auf die IT-Sicherheit - insbesondere mittels der Schadsoftware Emotet - wirksam zu bekämpfen (vgl. dazu im Einzelnen die Empfehlung zu Artikel 1 § 22/2). Zu diesem Änderungsvorschlag wurde eine ergänzende schriftliche Anhörung der Landesbeauftragten für den Datenschutz durchgeführt.

Die Ausschussmitglieder der Fraktionen von Bündnis 90/Die Grünen und FDP begründeten ihre Ablehnung des Gesetzentwurfs in der Fassung der Beschlussempfehlung mit verfassungsrechtlichen Bedenken zu den darin enthaltenen Grundrechtseingriffen, auf die auch der Gesetzgebungs- und Beratungsdienst (GBD) hingewiesen hatte. Das Ausschussmitglied der Grünen kritisierte über-

dies die - aus seiner Sicht konnexitätsrelevanten - finanziellen Folgen für die Kommunen sowie die im Gesetz enthaltenen Soll-Vorschriften.

Den Änderungsempfehlungen liegen im Einzelnen folgende Erwägungen zugrunde:

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

Zur Überschrift:

Da § 6 Abs. 3 und 4 des Entwurfs ausweislich der Begründung (vgl. Drs. 18/1598, S. 18 und 46) im Hinblick auf europaweite Ausschreibungen (oberschwelliger Bereich) der Umsetzung von Unionsrecht dienen, soll dieser Umstand in einer Fußnote zur Überschrift des Gesetzes deutlich gemacht werden (vgl. dazu - auf Bundesebene - auch BT-Drs. 18/9945 sowie BGBl. I 2017, S. 770).

Zum Ersten Teil (Allgemeines):

Zu § 1 (Begriffsbestimmungen):

Zu Absatz 1:

Zu Nummer 1:

Ein Angriff im Sinne der Nummer 1 liegt auch dann vor, wenn der Versuch einer unbefugten Beeinflussung erfolgreich war (Versuch als notwendiges Durchgangsstadium des erfolgreichen Angriffs). Dies bedarf aus Sicht des Ausschusses keiner ausdrücklichen Klarstellung im Wortlaut des Gesetzes. Die Worte „eines Computersystems“ sollen gestrichen werden, denn sie sind einerseits ungenau, weil auch andere IT-Systeme (vgl. zu diesem Begriff die Erläuterung zu Nummer 14) betroffen sein können. Andererseits ist damit keine Einschränkung beabsichtigt; jede unbefugte Beeinflussung der IT-Sicherheit soll erfasst werden.

Zu Nummer 2:

Nummer 2 soll sprachlich verbessert und an Nummer 3 angeglichen werden.

Zu Nummer 3:

Die Empfehlung zu Nummer 3 soll klarstellen, dass, wenn im Gesetz nur der Begriff „Behörde“ verwendet wird, sowohl die Behörden der unmittelbaren Landesverwaltung (Behörden des Landes) als auch die Behörden der mittelbaren Landesverwaltung (Behörden der Kommunen und sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts) gemeint sind. Soweit in diesem Gesetz nur die Behörden der unmittelbaren Landesverwaltung oder nur die Behörden der mittelbaren Landesverwaltung angesprochen werden (vgl. z. B. § 11 Abs. 1 und 3 sowie § 12 Abs. 2 und 3), sollen diese als „Behörde des Landes“ oder als „Behörde einer Kommune oder sonstigen der Aufsicht des Landes unterstehenden juristischen Person des öffentlichen Rechts“ bezeichnet werden.

Zu Nummer 4:

Der Ausschuss empfiehlt, Nummer 4 des Entwurfs zu streichen, weil diese den Wortlaut von Artikel 9 Abs. 1 der europäischen Datenschutz-Grundverordnung (DSGVO) wiederholt. Solche Wiederholungen von unmittelbar geltenden Bestimmungen einer unionsrechtlichen Verordnung in innerstaatlichen Rechtsvorschriften sind grundsätzlich unzulässig (vgl. nur *Calliess/Ruffert*, EUV/AEUV, 5. Aufl. 2016, Rn. 20 zu Art. 288 AEUV; BMJ, Handbuch der Rechtsförmlichkeit, 3. Aufl. 2008, Rn. 289). Hier wird die Wiederholung weder zur Wahrung der Kohärenz noch zur Verbesserung der Verständlichkeit benötigt (vgl. Erwägungsgrund Nr. 8 zur DSGVO).

Zu Nummer 5/1:

Die im Gesetzentwurf gewählten Begriffe „Informationssicherheit“ und „IT-Sicherheit“ stellen keine Synonyme dar. Der Begriff der „Informationssicherheit“ soll den Oberbegriff bilden und allgemein (ohne Technikbezug) die Vertraulichkeit, Verfügbarkeit und Integrität von Daten kennzeichnen. Von diesem Oberbegriff soll die IT-Sicherheit umfasst werden, die sich als Unterbegriff auf die mithilfe der Informationstechnik verarbeiteten Daten beschränkt. Diese für das Verständnis vieler Regelungen des Gesetzes elementare Unterscheidung soll im Gesetz deutlich werden, indem beide Begriffe in § 1 legaldefiniert werden (im Entwurf ist das nur für die IT-Sicherheit in Nummer 8 der Fall).

Zu Nummer 6:

Der Ausschuss empfiehlt, das Wort „elektronisch“ zu streichen, um eine Abweichung von § 2 Abs. 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) zu vermeiden. Damit soll auch eine Anregung aus der Anhörung aufgegriffen werden. Zudem soll durch Aufnahme des Klammerzusatzes „(IT)“ die im Gesetz vielfach verwendete Abkürzung (vgl. die Begriffe „IT-Sicherheit“, „IT-System“, „IT-Dienstleister“, „IT-Bevollmächtigte“ usw.) eingeführt werden.

Zu Nummer 7:

Die Definition der „Inhaltsdaten“ ist entbehrlich und soll daher gestrichen werden. Sowohl das Telekommunikationsgesetz (TKG) als auch die Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV) verwenden ähnliche Begriffe, ohne diese im Gesetz näher zu bestimmen (vgl. § 5 Abs. 1 TKÜV [„dem Inhalt … der Telekommunikation“], § 7 Abs. 1 und § 8 Abs. 2 Nr. 5 TKÜV [„Telekommunikationsinhalte“] sowie § 88 Abs. 1 TKG [„Inhalt der Telekommunikation“]). Die Entwurfsdefinition würde die (ungeklärte) Frage aufwerfen, ob Sender und/oder Empfänger (oder ein objektiver Dritter) die Informationen festlegt, „um derentwillen die Telekommunikation stattfindet“. Die Entwurfsdefinition dürfte zudem dazu führen, dass Inhaltsdaten, die zugleich Verkehrsdaten sind (z. B. URL bei Internet-Suchanfragen), aus dem Bereich der Inhaltsdaten (wohl unbeabsichtigt) herausfielen. Dies könnte bei den Eingriffsbefugnissen der §§ 17 ff. des Entwurfs zu verfassungsrechtlichen Schwierigkeiten führen.

Zu Nummer 8:

Die Worte „Gewährleistung der“ sollen gestrichen werden, um zu verdeutlichen, dass es sich bei der „IT-Sicherheit“ (wie bei der öffentlichen Sicherheit im Sinne des Gefahrenabwehrrechts) um einen Zustand und nicht um ein Tun handelt. Durch diese Empfehlung werden zudem redundante Formulierungen wie in § 14 („zur Gewährleistung der IT-Sicherheit erforderlich“) vermieden.

Zu Nummer 9:

Die Gliederung des Landesdatennetzes in „Netzabschnitte“ soll in die Begriffsbestimmung eingefügt werden, um zu verdeutlichen, dass es nur ein (einheitliches) Landesdatennetz in Niedersachsen gibt (betrieben derzeit von IT.N), das in mehrere Netzabschnitte gegliedert ist (derzeit zwei). Für den Netzabschnitt des Geschäftsbereichs des Justizministeriums (MJ) bestimmt dieses die zuständige Stelle (vgl. § 13 Abs. 1 Satz 2), im Übrigen ist die „das Landesdatennetz betreibende Behörde“ (derzeit IT.N) zuständig (vgl. § 13 Abs. 1 Satz 1). Die lokalen Netzwerke der angebundenen Behörden sind hingegen kein Bestandteil des Landesdatennetzes (vgl. auch die Begründung, Drs. 18/1598, S. 32) oder der Netzabschnitte.

Die Bezugnahme auf die „Netze anderer Verwaltungen“ soll entfallen. Solche Netze (wie z. B. das KDO-Netz oder die Datennetze anderer Bundesländer) sind für die Begriffsbestimmung nicht von Bedeutung, insbesondere da die über solche Netze mit dem Landesdatennetz verbundenen IT-Systeme nicht von Absatz 2 erfasst werden (vgl. auch die Begründung, a. a. O., S. 32 f.).

Mit der Empfehlung, die Worte „oder im Auftrag des Landes“ zu streichen, folgt der Ausschuss dem Vorschlag des MI, das mitgeteilt hat, das Landesdatennetz solle ausschließlich durch das Land selbst betrieben werden.

Zu Nummer 10:

Die Empfehlung dient dazu, Nummer 10 stärker an die Definition des Nutzerkontos in § 2 Abs. 5 OZG anzulehnen, weil nach Mitteilung des MI insoweit keine Abweichungen beabsichtigt sind. Dadurch soll sichergestellt werden, dass nicht allein natürliche oder juristische Personen oder Personengesellschaften, sondern auch Behörden ein Nutzerkonto erhalten können (vgl. BT-Drs. 18/11135, S. 92). Die Frage, von wem die Nutzerkonten bereitgestellt werden (nach § 2 Abs. 5 OZG von einer staatlichen Stelle), soll nach Mitteilung des MI (nur) in § 12 Abs. 1 Satz 1 Nr. 1 geregelt werden.

Zu Nummer 11:

Durch die Nutzung der Begriffsbestimmung in Nummer 8 kann Nummer 11 vereinfacht werden.

Zu Nummer 12:

Nummer 12 ist entbehrlich und soll daher gestrichen werden. Der Begriff „Sicherheitsdomäne“ wird nur in § 16 Abs. 2 des Entwurfs verwendet und soll dort bzw. in § 12/2 Abs. 2 der Empfehlung durch den passenderen Begriff „Mitglieder des Sicherheitsverbunds“ ersetzt werden (vgl. die Empfehlungen zu § 12/2 Abs. 2 bzw. § 16 Abs. 2).

Zu Nummer 13:

Auch Nummer 13 ist entbehrlich und soll deswegen gestrichen werden. Der Begriff „Sicherheitsarchitektur“ wird nur in § 16 Abs. 1 des Entwurfs verwendet. Der Inhalt der Begriffsbestimmung soll daher in diese Regelung (in § 12/2 Abs. 1) übernommen werden (vgl. die Empfehlung zu § 12/2 Abs. 1 bzw. § 16 Abs. 1).

Zu Nummer 14:

Da nach Mitteilung des MI kein inhaltlicher Unterschied zwischen dem „informationstechnischen System“ (vgl. § 1 Abs. 1 Nr. 14 und Abs. 2, § 3 Abs. 2 Nrn. 1 und 9, § 13 Abs. 2 Nr. 2 sowie Abs. 3 und 4, § 14 sowie § 15 Abs. 1 und 3 des Entwurfs) und dem „IT-System“ (vgl. § 16 Abs. 1, § 19 Abs. 1 und § 23 Abs. 2 Nr. 2 des Entwurfs) besteht, soll im gesamten Gesetz einheitlich der Begriff des „IT-Systems“ verwendet werden.

Zu Nummer 15:

Der Begriff des „Sicherheitsvorfalls“ soll durch Bezugnahme auf die IT-Sicherheit (Nummer 8) vereinfacht werden. Dadurch wird zudem in § 16 Abs. 1 und 2 des Entwurfs bzw. § 12/2 Abs. 1 und 2 der Empfehlung das dem „Sicherheitsvorfall“ vorangestellte Adjektiv „informationstechnisch“ entbehrlich (vgl. die Empfehlung zu § 12/2 Abs. 1 und 2).

Zu Absatz 2:

Vgl. die Erläuterung zu Absatz 1 Nr. 14.

Zum Zweiten Teil (Digitale Verwaltung):

Zu § 3 (Geltungsbereich):

Zu Absatz 1:

Durch die empfohlene Bezugnahme auf die „Behörden“ (nach der Empfehlung zu § 1 Abs. 1 Nr. 3 erfasst dies die unmittelbare und die mittelbare Landesverwaltung), soll die Regelung vereinfacht (und überdies mit § 1 Abs. 1 des Niedersächsischen Verwaltungsverfahrensgesetzes [NVwVfG] harmonisiert) werden.

Zu Absatz 1/1:

Der empfohlene Absatz 1/1 enthält die Geltungsbereichsausnahme aus Absatz 2 Nr. 10 des Entwurfs (vgl. auch § 1 Abs. 5 Nr. 1 des [Bundes-]Gesetzes zur Förderung der elektronischen Verwaltung [E-Government-Gesetz - EGovG]). Diese passt nicht in die Auflistung der Ausnahmen in Absatz 2, weil sie anders als die übrigen Nummern nicht eine Behörde (oder einen Teil davon) betrifft,

sondern einen sachlichen Zuständigkeitsbereich. Eine solche (auch in § 1 Abs. 5 EGovG nicht enthaltene) Vermischung verschiedener Ausnahmen soll vermieden werden.

Zu Absatz 2:

Nummer 1 des Entwurfs soll in die Nummern 1 und 1/1 aufgeteilt werden, um zu verdeutlichen, dass sich der Satzteil „die mit Forschungsaufgaben betraut und deren informationstechnischen Systeme nicht mit dem Landesdatennetz verbunden sind“ nicht auf die Hochschulen in staatlicher Verantwortung, sondern allein auf die „Teile von Behörden des Landes“ bezieht. Im Übrigen soll in Nummer 1/1 der Begriff des „IT-Systems“ verwendet werden (vgl. dazu die Erläuterung zu § 1 Abs. 1 Nr. 14).

Zu dem in Nummer 9 empfohlenen Begriff „IT-System“ vgl. die Erläuterung zu § 1 Abs. 1 Nr. 14.

Nummer 10 des Entwurfs soll hier gestrichen und als inhaltliche Ausnahme in Absatz 1/1 aufgenommen werden (vgl. die Empfehlung zu Absatz 1/1).

Zu Absatz 3:

Die Empfehlung zum einleitenden Satzteil dient dazu, die Reichweite des Absatzes 3 unter Einbeziehung des Satzteils nach der Nummerierung klarzustellen. Absatz 3 soll nach Mitteilung des MI die Geltung des Zweiten Teils (§§ 3 bis 12) für bestimmte Stellen und Tätigkeiten auf den Austausch elektronischer Akten nach § 10 Abs. 4 beschränken, soweit für diese die Geltung des Zweiten Teils nicht bereits aufgrund der Absätze 1/1 und 2 ausscheidet. Durch die empfohlene Verlagerung der Rechtsfolge in den einleitenden Satzteil soll die Regelung zudem leichter verständlich werden. In Nummer 1 ist der Satzteil „soweit diese nicht bereits von den Absätzen 1 und 2 erfasst sind“ entbehrlich und soll daher gestrichen werden.

Zu Absatz 3/1:

Die Empfehlung zu Absatz 3/1 betrifft das Verhältnis des Gesetzentwurfs zum E-Government-Gesetz des Bundes, an dem sich die §§ 4 ff. des Entwurfs überwiegend orientieren. Die Entwurfsregelungen ergänzen dieses, insbesondere für die vom E-Government-Gesetz nicht erfasste Ausführung von Landesrecht. Der im Gesetzentwurf vielfach verwendete Satzteil „auch wenn die Behörden kein Bundesrecht ausführen“ (vgl. § 4 Abs. 1, § 5 Abs. 1 und 2, § 6 Abs. 1, § 7 Abs. 1 und 2 sowie § 8 des Entwurfs) soll dies ausdrücken. Ausweislich der Entwurfsbegründung (Dr. 18/1598, S. 38) soll dadurch klargestellt werden, dass das Gesetz nicht in den Wirkungsbereich des E-Government-Gesetzes eingreifen soll. Dessen Regelungen sollen mithin (wie in § 1 Abs. 2 EGovG angeordnet) grundsätzlich auch für die Behörden des Landes (unmittelbare und mittelbare Landesverwaltung) gelten, soweit diese Bundesrecht ausführen. Die von Artikel 84 Abs. 1 Satz 2 des Grundgesetzes (GG) eingeräumte Möglichkeit, die Einrichtung der Behörden und das Verwaltungsverfahren abweichend vom Bundesrecht zu regeln (sog. Abweichungskompetenz; diese gilt allerdings nicht bei der Bundesauftragsverwaltung nach Artikel 85 GG), nimmt der Gesetzentwurf mithin nicht im größtmöglichen Umfang in Anspruch (anders z. B. Bayern; vgl. Artikel 3 des Bayerischen Gesetzes über die elektronische Verwaltung [BayEGovG]; dazu auch BayLT-Drs. 17/7537, S. 17; *Denkhaus/Geiger*, Bayerisches E-Government-Gesetz, 2016, S. 74). Daraus folgt, dass nach dem Gesetzentwurf die in Absatz 2 oder 3 genannten Stellen und Tätigkeiten, soweit Bundesrecht ausgeführt wird, nicht von den Vorgaben der „Digitalen Verwaltung“ bzw. des „E-Government“ befreit sind. Auch bei den in Absatz 2 oder 3 genannten Stellen und Tätigkeiten muss mithin das E-Government-Gesetz angewendet werden, d. h. bei der Ausführung von Bundesrecht müssen der elektronische Zugang zur Verwaltung eröffnet (§ 2 Abs. 1 EGovG), Informationen über öffentlich zugängliche Netze gewährt (§ 3 Abs. 1, 2 und 3 EGovG), elektronische Bezahlmöglichkeiten eingerichtet (§ 4 EGovG) sowie elektronische Nachweise und Formulare anerkannt werden (§§ 5 und 13 EGovG). Dies ist nach Mitteilung des MI auch beabsichtigt, weil das MI davon ausgeht, dass die seit dem Jahr 2013 bestehenden Verpflichtungen des E-Government-Gesetzes bei den in den Absätzen 2 und 3 genannten Stellen und Tätigkeiten bereits umgesetzt worden sind.

Der Ausschuss empfiehlt vor diesem Hintergrund, das auch mithilfe der Gesetzesbegründung nicht leicht erkennbare Verhältnis der in den Absätzen 2 und 3 genannten Stellen und Tätigkeiten zum E-Government-Gesetz des Bundes durch Absatz 3/1 klarzustellen. Da mithin die Behörden der unmittelbaren und mittelbaren Landesverwaltung das E-Government-Gesetz anzuwenden haben,

soweit sie Bundesrecht als eigene Angelegenheit oder im Rahmen der Bundesauftragsverwaltung ausführen, empfiehlt der Ausschuss zur Rechtsvereinfachung, die Regelungen des NDIG so weit wie möglich an das E-Government-Gesetz anzulehnen (auch durch Verweisungen) und nur dort abweichende Formulierungen aufzunehmen, wo abweichende Regelungen für die Ausführung von Landesrecht gewollt sind (vgl. zu dieser Regelungstechnik z. B. § 1 Abs. 1 NVwVfG mit der dortigen Verweisung auf das [Bundes-]Verwaltungsverfahrensgesetz [VwVfG]).

Zu Absatz 4:

Die empfohlene Änderung im einleitenden Satzteil dient zur Klarstellung, dass Absatz 4 eine Gegenausnahme zu den Ausnahmeregelungen in den Absätzen 1/1 bis 3 enthält.

Nach Mitteilung des fachlich zuständigen Ministeriums für Wirtschaft, Arbeit, Verkehr und Digitalisierung (MW) sind in Nummer 1 mit den in Bezug genommenen Aufträgen im Sinne des Teils 4 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) nicht nur öffentliche Aufträge im engeren Sinne gemeint, sondern alle von Teil 4 des GWB erfassten Konstellationen (d. h. auch Konzessionen, Wettbewerbe usw.), weil die Verweisung in Artikel 1 Abs. 1 UAbs. 1 der Richtlinie 2014/55/EU diese ebenfalls erfasst. Dies soll durch die Empfehlung verdeutlicht werden, die sich an den Wortlaut der Überschrift von Teil 4 des GWB sowie von § 97 Abs. 1 Satz 1 GWB anlehnt.

Mit seiner Empfehlung zu Nummer 2 folgt der Ausschuss dem Vorschlag des MW, an der (Ketten-) Verweisung auf § 2 Abs. 5 des Niedersächsischen Tariftreue- und Vergabegesetzes (NTVergG) festzuhalten (und nicht direkt auf die GWB-Normen zu verweisen). Dadurch soll der Gleichklang zwischen NDIG und NTVergG betont werden. Da Konzessionsgeber im Sinne des § 101 GWB von § 2 Abs. 5 NTVergG nicht erfasst werden, sollen hier neben den „öffentlichen Aufträgen“ die Konzessionen nicht genannt werden.

Die in der Entwurfsregelung enthaltene Einschränkung („in Bezug auf Aufträge, deren geschätzter Auftragswert den jeweils maßgeblichen Schwellenwert gemäß § 106 GWB nicht erreicht“) führt dazu, dass die Vorgaben des elektronischen Rechnungsverkehrs (§ 6 Abs. 3 und 4 des Entwurfs) auch dann für die öffentlichen Auftraggeber im Sinne des § 2 Abs. 5 NTVergG gelten, wenn das NTVergG sachlich nicht anwendbar ist, z. B. wegen Unterschreitens der 10 000 Euro-Grenze (§ 2 Abs. 1 NTVergG) oder bei freiberuflichen Leistungen (§ 2 Abs. 2 Satz 2 NTVergG). Dies lässt sich der Begründung (Drs. 18/1598, S. 38, 46) zwar nicht eindeutig entnehmen, ist jedoch nach Mitteilung von MI und MW so beabsichtigt, um den Unternehmen (Auftragnehmern) unabhängig von der Höhe des Auftrags das Recht einzuräumen, elektronische Rechnungen zu stellen; dazu verpflichtet werden sie nicht (vgl. die Begründung, a. a. O., S. 46).

Zu § 4 (Elektronischer Zugang zur Verwaltung):

Zu Absatz 1:

Die Empfehlung zu Satz 1 mit der statischen Verweisung auf § 2 Abs. 1 EGovG (vgl. dessen erste Zitierung in der Empfehlung zu § 3 Abs. 3/1) soll klarstellen, dass die Behörden hier denselben elektronischen Zugang zu eröffnen haben wie bei der Ausführung von Bundesrecht. Die empfohlene Formulierung im Singular („Jede Behörde …“) ist ebenfalls an das E-Government-Gesetz angelehnt. Satz 2 wird dadurch entbehrlich und soll gestrichen werden.

Zu Absatz 2:

Die Empfehlung zu Satz 1 dient zur besseren redaktionellen Abstimmung auf Absatz 1.

Nach Mitteilung des MI wird mit Satz 2 die Einführung einer Postfachfunktion in den Nutzerkonten beabsichtigt. Dies soll im Wortlaut verdeutlicht werden. Der mit dem Datenaustausch verfolgte Zweck („Inanspruchnahme von Behördenleistungen“) ergibt sich bereits aus der Begriffsbestimmung in § 1 Abs. 1 Nr. 10 und soll hier nicht wiederholt werden.

Nach Mitteilung des MI ergänzen die Regelungen des Absatzes 2 die (bundesrechtliche) Verpflichtung, sämtliche Verwaltungsleistungen elektronisch über Verwaltungsportale anzubieten (§ 1 Abs. 1

OZG) und für die Nutzerinnen und Nutzer zur einheitlichen Identifizierung Nutzerkonten bereitzustellen (§ 3 Abs. 2 Satz 1 OZG). Die landesrechtlichen Ergänzungen, die dazu dienen, das OZG in Niedersachsen umzusetzen (vgl. auch die Begründung, Drs. 18/1598, S. 18), gelten nach dem Gesetzentwurf allerdings nicht für die in § 3 Abs. 2 und 3 genannten Stellen und Tätigkeiten, obwohl auch diese in den Anwendungsbereich des OZG fallen dürften, denn dieser wird von der wohl überwiegenden und vom MI geteilten Auffassung in der juristischen Literatur (unter Berufung auf die Entwurfsbegründung; vgl. BT-Drs. 18/11135, S. 91: „alle Verwaltungsleistungen sämtlicher Behörden“) weit verstanden (vgl. *Herrmann/Stöber*, NVwZ 2017, 1401, 1402; *Petersen*, DVBl 2018, 1534, 1536; *Siegel*, DÖV 2018, 185, 187 f.; *Wischmeyer*, in: v. Mangoldt/Klein/Starck, GG, Bd. 3, 7. Aufl. 2018, Art. 91 c Rn. 33 f.; *Jarass/Pieroth*, GG, 15. Aufl. 2018, Art. 91 c Rn. 6; die Gegenauffassung hält die für das OZG zeitgleich in das Grundgesetz aufgenommene Gesetzgebungskompetenz in Artikel 91 c Abs. 5 GG für nicht ausreichend; vgl. dazu ausführlich *Martini/Wiesner*, ZG 2017, 193, 195 ff.; krit. auch *Siekmann*, in: Sachs, GG, 8. Aufl. 2018, Art. 91 c Rn. 30; *Schliesky/ Hoffmann*, DÖV 2018, 193, 195). Das OZG selbst sieht keine Ausnahmen wie in § 3 Abs. 2 und 3 des Entwurfs vor (dies war in § 1 Abs. 1 Satz 2 OZG-Entwurf noch anders, der Verwaltungsleistungen von der Regelung ausnahm, die sich für ein elektronisches Angebot - aus rechtlichen oder tatsächlichen Gründen - nicht eignen [vgl. BT-Drs. 18/11135, S. 31, 91]; nachdem der Bundesrat vorgeschlagen hatte, diese Ausnahme noch zu erweitern [a. a. O., S. 138], wurde Satz 2 allerdings in der Beschlussempfehlung und im beschlossenen Gesetz ganz gestrichen [vgl. BT-Drs. 18/12589, S. 55, 143]). Der Ausschuss ist mit seiner Empfehlung der Auffassung des MI gefolgt, dass die Verpflichtungen des OZG bei den in § 3 Abs. 2 und 3 genannten Stellen und Tätigkeiten auch ohne die hier vorgesehenen landesrechtlichen Ergänzungen erfüllt werden können.

Zu Absatz 3:

Die Entwurfsregelung weicht von § 2 Abs. 2 EGovG ab (der allerdings nur für Behörden des Bundes gilt), indem anstelle der De-Mail-Adresse auch ein „anderer schriftformersetzender Dienst“ eröffnet werden kann. Da die Behörde diese Alternative bereits durch die Eröffnung eines Zugangs für die Übermittlung von Dokumenten mit qualifizierter elektronischer Signatur erfüllt (vgl. § 3 a Abs. 2 VwVfG i. V. m. § 1 Abs. 1 NVwVfG), zu der sie nach Absatz 1 ohnehin verpflichtet ist, ist kein eigenständiger Regelungsgehalt der Vorschrift erkennbar. Der Ausschuss ist hier dennoch dem Vorschlag des MI gefolgt, an der Regelung festzuhalten, und empfiehlt daher lediglich, die Regelung redaktionell besser auf die Absätze 1 und 2 abzustimmen.

Zu Absatz 4:

Auch hier weicht die Entwurfsregelung von § 2 Abs. 3 EGovG ab (der ebenfalls nur für Behörden des Bundes gilt), indem die Regelung auf „elektronisch durchgeführte Verwaltungsverfahren“ beschränkt wird (vgl. dazu Drs. 18/1598, S. 47). Damit ist nach Mitteilung des MI beabsichtigt, die Anwendung des Absatzes 4 auf Verwaltungsverfahren auszuschließen, in denen ein persönliches Erscheinen vorgeschrieben ist. Die Empfehlung enthält daher lediglich redaktionelle Anpassungen an die Absätze 1 bis 3.

Zu § 5 (Elektronische Informationen und Verwaltungsportal):

Zu Absatz 1:

Der Ausschuss empfiehlt, die Satzeinleitung redaktionell an die Empfehlungen zu § 4 des Entwurfs bzw. § 3 Abs. 1 EGovG anzupassen. Darüber hinaus soll durch die Verweisung auf § 3 Abs. 1 EGovG klargestellt werden, dass die Verpflichtungen identisch sind (vgl. die Erläuterung zu § 3 Abs. 3/1). Das MI hat mitgeteilt, dass Absatz 1 zugleich als landesrechtliche Anordnung nach § 3 Abs. 3 EGovG dienen soll, die § 3 Abs. 1 EGovG auch für Gemeinden und Gemeindeverbände Anwendung finden lässt, soweit diese Bundesrecht ausführen (vgl. Artikel 84 Abs. 1 Satz 7 und Artikel 85 Abs. 1 Satz 2 GG). § 3 Abs. 1 EGovG gilt in Niedersachsen demnach unmittelbar für alle Behörden (auch Kommunen), soweit sie Bundesrecht (als eigene Angelegenheit oder im Auftrag des Bundes) ausführen (und nach Absatz 1 entsprechend, soweit sie Landesrecht ausführen).

Zu Absatz 2:

Auch hier soll die Satzeinleitung redaktionell an die Empfehlungen zu § 4 des Entwurfs bzw. § 3 Abs. 2 EGovG angepasst werden. Die Wendung „auch wenn sie nicht Bundesrecht ausführen“ soll hier gestrichen werden. Anders als Absatz 1 enthält Absatz 2 des Entwurfs nicht nur eine ergänzende Regelung für die Ausführung von Landesrecht (vgl. zu dem Verhältnis von NDIG-Entwurf und EGovG die Erläuterung zu § 3 Abs. 3/1), sondern eine inhaltliche Abweichung von § 3 Abs. 2 EGovG. An die Stelle der dortigen Soll-Regelung (vgl. dazu BT-Drs. 17/11473, S. 36) soll nach Mitteilung des MI eine Muss-Regelung treten, um eine vollständige Beschreibung der Leistungen sowie Darstellung der Informationen sicherzustellen. Dementsprechend soll Absatz 2 auch nicht nach § 3 Abs. 3 EGovG die Geltung von § 3 Abs. 2 EGovG für Kommunen anordnen (anders als Absatz 1), sondern selbst unmittelbar für die Kommunen gelten (auch bei der Ausführung von Bundesrecht als eigene Angelegenheit). Dieser Regelungsgehalt soll wie empfohlen verdeutlicht werden. § 3 Abs. 2 EGovG soll demnach in Niedersachsen nur noch für Behörden (außer Kommunen) gelten, die Bundesrecht im Auftrag des Bundes ausführen (eine Abweichungskompetenz wie in Artikel 84 Abs. 1 Satz 2 GG ist in Artikel 85 GG nicht vorgesehen).

Zu Absatz 3:

Der Ausschuss empfiehlt lediglich redaktionelle Anpassungen.

Zu Absatz 4:

Das zu Satz 1 empfohlene Wort „landeseinheitlich“ soll klarstellen, dass die obersten Landesbehörden nur sicherzustellen haben, dass die landeseinheitlichen Informationen für die Kommunen bereitstehen (nicht sämtliche Informationen; vgl. auch § 3 Abs. 2a EGovG).

In den Sätzen 1 und 2 soll berücksichtigt werden, dass § 3 Abs. 2 EGovG für die Kommunen nach § 3 Abs. 3 EGovG keine Anwendung findet (vgl. dazu die Erläuterung zu Absatz 2).

Die Empfehlung zu Satz 2 soll im Übrigen dem Umstand Rechnung tragen, dass Absatz 2 keine Zwecke, sondern Pflichten enthält.

Zu Absatz 5:

Zu Satz 2 empfiehlt der Ausschuss redaktionelle Anpassungen an die Absätze 1 bis 4 sowie an § 4. Zu dem Verhältnis von Satz 2 zu § 1 Abs. 1 OZG vgl. die Erläuterung zu § 4 Abs. 2.

Zu § 6 (Elektronische Bezahlmöglichkeiten und Rechnungen):

Zu Absatz 1:

Da nach Mitteilung des MI hier trotz der teilweise missverständlichen Formulierung („Verwaltungskosten“ statt „Gebühren“) keine Abweichung von § 4 EGovG beabsichtigt ist, der von den Behörden ohnehin angewendet werden muss, soweit sie Bundesrecht ausführen, empfiehlt der Ausschuss eine Harmonisierung mit § 4 EGovG (vgl. die Erläuterung zu § 3 Abs. 3/1), die hier am einfachsten durch eine Verweisung vorgenommen werden kann.

Zu Absatz 2:

Hier soll, wie auch in § 4 EGovG, auf den in Absatz 1 verwiesen wird, der Begriff „Verwaltungskosten“ durch den Begriff „Gebühren“ ersetzt werden, weil dieser sowohl zum Niedersächsischen Verwaltungskostengesetz (vgl. § 1 NVwKostG) als auch zum Niedersächsischen Kommunalabgabengesetz passt (vgl. die §§ 1 und 4 NKAG). Zudem sollen die „sonstigen Forderungen“ aufgenommen werden, um einen Gleichlauf mit Absatz 1 zu schaffen (und z. B. Auslagen zu erfassen). Im Übrigen soll sprachlich durch die vorgeschlagene Umstellung von Tatbestand und Rechtsfolge das Gemeinte deutlicher werden.

Zu Absatz 3:

Der Ausschuss empfiehlt eine redaktionelle Anpassung an die Empfehlungen zu den Absätzen 1 und 2 sowie den §§ 4 und 5.

Zu Absatz 4:

Satz 1 soll zu einer Verpflichtung der Landesregierung zum Erlass der Verordnung umgestaltet werden, denn es genügt zur hier beabsichtigten Umsetzung der Vorgaben der Richtlinie 2014/55/EU nicht, den Erlass der Verordnung, ohne die Absatz 3 leerläuft, in das Ermessen der Landesregierung zu stellen. Zu Satz 2 empfiehlt der Ausschuss lediglich eine sprachliche Anpassung.

Zu § 7 (Nachweise):

Da mit § 7 des Entwurfs nach Mitteilung des MI keine Abweichung von § 5 Abs. 1 und 2 EGovG beabsichtigt ist, der von den Behörden ohnehin angewendet werden muss, soweit sie Bundesrecht ausführen, empfiehlt der Ausschuss eine Harmonisierung mit § 5 Abs. 1 und 2 EGovG (vgl. die Erläuterung zu § 3 Abs. 3/1), die hier am einfachsten durch eine Verweisung vorgenommen werden kann (vgl. auch die Empfehlung zu § 6 Abs. 1).

Auf eine Verweisung auf § 5 Abs. 3 EGovG, der die Möglichkeit einer elektronischen Einwilligung in die Einholung der Nachweise regelt, soll indes verzichtet werden. Das MI hat dazu mitgeteilt, dass § 5 Abs. 3 EGovG obsolet geworden sei, weil stattdessen die unmittelbar anwendbaren Artikel 7 und 8 DSGVO gälten.

Zu § 8 (Elektronische Formulare):

Da hier nach Mitteilung des MI keine inhaltliche Abweichung von § 13 EGovG beabsichtigt ist, der von den Behörden ohnehin angewendet werden muss, soweit sie Bundesrecht ausführen, empfiehlt der Ausschuss eine Harmonisierung mit § 13 EGovG durch eine Verweisung (vgl. auch die Erläuterungen zu § 3 Abs. 3/1, § 6 Abs. 1 und § 7).

Zu § 9 (Georeferenzierung):

Zu Absatz 1:

Das MI hat mitgeteilt, dass der (von § 14 Abs. 1 EGovG abweichende) Einschub „auf der Grundlage der Angaben des amtlichen Vermessungswesens (Geobasisdaten)“ auf § 1 Abs. 3 des Niedersächsischen Gesetzes über das amtliche Vermessungswesen (NVermG) beruhe. Damit solle die Interoperabilität von Geodaten und Geodatendiensten sowie Fachdaten gewährleistet werden. Da sich der Begriff „Angaben“ in der Praxis als zu unspezifisch erwiesen habe, hat das MI vorgeschlagen, im Vorgriff auf eine zukünftige Änderung des NVermG hier den Begriff der „amtlichen Geobasisdaten“ zu verwenden. Was unter Geobasisdaten zu verstehen sei, könne Ziffer 1.2 des RdErl. d. MI v. 1. 11. 2017 - 47-23050/101 - VORIS 21160 - (Nds. MBl. 2017 Nr. 45, S. 1478) entnommen werden. Diesem Vorschlag ist der Ausschuss mit seiner Empfehlung gefolgt.

Zu Absatz 2:

Nach Mitteilung des MI soll die Georeferenzierung sowohl für öffentliche als auch für nichtöffentliche Register gelten. Da dies in § 14 Abs. 2 EGovG ausdrücklich klargestellt worden ist und die Regelungen des NDIG so weit wie möglich an das E-Government-Gesetz des Bundes angelehnt werden sollen, wenn keine Abweichungen beabsichtigt sind (vgl. dazu die Erläuterung zu § 3 Abs. 3/1), empfiehlt der Ausschuss, den Wortlaut des Absatzes 2 an § 14 Abs. 2 EGovG anzupassen.

Zu § 10 (Elektronische Aktenführung):

Zu Absatz 1:

Die Regelung soll redaktionell an die Empfehlungen zu den §§ 4 ff. angepasst werden. Das MI hat überdies mitgeteilt, dass mit den hier genannten Behörden die unmittelbare und mittelbare Landes-

verwaltung gemeint sei (vgl. § 1 Abs. 1 Nr. 3), soweit die Geltung dieses Teils nicht durch § 3 Abs. 1/1 bis 3 ausgeschlossen werde. Damit sei allerdings nicht beabsichtigt, für die dort genannten Stellen und Tätigkeiten die elektronische Aktenführung zu verbieten. Es bedürfe für diese lediglich keiner Klarstellung, dass sie ihre Akten elektronisch führen dürfen.

Zu Absatz 2:

Satz 1 soll redaktionell an die Empfehlungen zu Absatz 1 sowie zu den §§ 4 ff. angepasst werden. Nach Mitteilung des MI ist die Soll-Regelung neben der in Satz 3 enthaltenen Möglichkeit der Terminverschiebung beabsichtigt. Ob ein atypischer Fall vorliege, müsse behördenintern entschieden werden.

Satz 3 soll sprachlich angepasst werden (Aktiv statt Passiv), um das Gemeinte zu verdeutlichen. Nach Mitteilung des MI solle jede einzelne Behörde des Landes die Möglichkeit haben, eine Vereinbarung mit der oder dem IT-Bevollmächtigten der Landesregierung zu schließen.

In Satz 4 sollen die Worte „nur dann“ eingefügt werden, denn nach Mitteilung des MI sei beabsichtigt, dass das Einvernehmen nur dann verweigert werden dürfe, wenn sowohl die Begründung nicht ausreiche als auch eine erhebliche Beeinträchtigung vorliege.

Zu Absatz 3:

Durch Satz 1 des Entwurfs werden Lesbarkeit, Integrität, Authentizität, Verfügbarkeit und Vertraulichkeit zur Maßgabe für die elektronische Aktenführung. Nach Mitteilung des MI handelt es sich dabei um Beispielsfälle der ebenfalls einzuhaltenden Grundsätze der ordnungsgemäßen Aktenführung (vgl. zur Integrität der Akte VG Wiesbaden, Urteil vom 28. Dezember 2016 - 6 K 332/16.W -, juris, Rn. 23 f.; *Kopp/Ramsauer*, VwVfG, 16. Auflage 2015, § 29 Rn. 1a: „Verbot der Aktenverfälschung“; zur Verfügbarkeit der Akte *Kopp/Ramsauer*, a. a. O.: „Gebot der Aktenstabilität“). Dies soll durch das Wort „insbesondere“ im Wortlaut verdeutlicht werden.

Zudem soll Satz 1 durch Einfügung der Worte „durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik“ an § 6 Satz 3 EGovG angepasst werden. Nach Mitteilung des MI solle hier auf Bundes- und Landesebene kein unterschiedlicher Maßstab gelten.

Zu Absatz 4:

Zu Satz 1 hat das MI mitgeteilt, dass mit den Behörden (nur) die in § 1 Abs. 1 Nr. 3 bezeichneten Behörden der unmittelbaren und mittelbaren Landesverwaltung gemeint seien. Satz 1 solle also nicht den elektronischen Austausch von elektronischen Akten mit Bundesbehörden oder Behörden anderer Länder erfassen.

Satz 2 erfasst nach seinem Wortlaut (anders als Satz 1) nicht den Austausch innerhalb einer Behörde. Insoweit gebe es laut MI kein Regelungsbedürfnis, weil innerhalb einer Behörde der Austausch mithilfe des jeweiligen E-Akte-Systems erfolge, sodass keine technischen Standards für die Übermittlung festgelegt werden müssten. Der Ausschuss empfiehlt allerdings, die Verordnungsermächtigung in Satz 2 im Hinblick auf die nach Artikel 43 Abs. 1 Satz 2 der Niedersächsischen Verfassung (NV) erforderliche Bestimmtheit von Inhalt, Zweck und Ausmaß der Ermächtigung zu präzisieren. Der Inhalt der „technischen Verfahren und Standards“ lässt sich durch Auslegung ermitteln (vgl. zu der Parallelregelung in § 32 Abs. 3 der Strafprozessordnung [StPO] die Begründung, BT-Drs. 18/9416, S. 44: „zulässige Dateiformate“, „Definition von Softwareschnittstellen“, „gleichzeitige Übertragung von Metadaten“ usw.). Durch die empfohlene Fassung soll sowohl der Zweck verdeutlicht (Ermöglichung des elektronischen - d. h. medienbruchfreien - Austauschs im Sinne des Satzes 1) als auch das Ausmaß begrenzt werden („soweit … erforderlich“).

Zu Absatz 5:

Da nach Mitteilung des MI mit Absatz 5 des Entwurfs keine Abweichung von § 8 EGovG beabsichtigt sei (mit Ausnahme der Nummer 4, dazu gleich), soll der Wortlaut an das Bundesrecht angeglichen werden, allerdings unter Beibehaltung des Singulars („jede Behörde“). Dadurch soll auch - anders als in der Entwurfsfassung - deutlich werden, wem die Entscheidung obliegt, eine der Varianten der Einsichtnahme auszuwählen. Die empfohlene Fassung verdeutlicht zudem, dass mit der Regelung - wie auch mit § 8 EGovG - kein neuer Anspruch auf Akteneinsicht geschaffen wer-

den soll. Nach Nummer 4 soll - abweichend von § 8 Nr. 4 EGovG - nicht der „elektronische Zugriff“, sondern der „lesende Zugriff“ auf den Inhalt der Akte gewährt werden. Diese Abweichung vom Bundesrecht hat das MI damit begründet, dass der Zugriff auf eine E-Akte stets elektronisch sei, das Adjektiv sei daher überflüssig. Demgegenüber sei aber von Bedeutung, dass durch den Zugriff keine Änderungen an der Akte vorgenommen werden könnten. Dies solle der Wortlaut verdeutlichen, jedenfalls für die Ausführung von Landesrecht sowie von Bundesrecht als eigene Angelegenheit. Für die Ausführung von Bundesrecht im Auftrag des Bundes bleibt es allerdings in Ermangelung einer Abweichungskompetenz (vgl. Artikel 84 Abs. 1 Satz 2 GG einerseits und Artikel 85 GG andererseits) bei der Anwendung von § 8 EGovG.

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

Zu Absatz 1:

Satz 1 soll redaktionell an die Empfehlungen zu den §§ 4 ff. angepasst werden („Jede Behörde…“). Auf das Wort „erforderlichenfalls“ soll verzichtet werden, weil ihm nach Mitteilung des MI kein Regelungsgehalt zukommt. Werden Akten elektronisch geführt, müssen alle zur Akte gehörenden Dokumente in elektronischer Form vorliegen. In einem neuen Halbsatz 2 soll die Regelung über Aktenbestandteile, die in anderer körperlicher Form vorliegen (z. B. Röntgen- oder Filmaufnahmen; vgl. Drs. 18/1598, S. 55), aufgenommen werden, zu denen die Übertragung „in elektronische Dokumente“ sprachlich wohl nicht in allen Fällen passt. Gespeichert werden soll in diesen Fällen die „elektronische Wiedergabe“ des nicht in Papierform vorliegenden Aktenbestandteils.

Der Ausschuss empfiehlt, in den Sätzen 2 und 3 klarzustellen, dass diese Regelungen nur für das ersetzende Scannen von Dokumenten und anderen Gegenständen nach Satz 1 gelten sollen. Im Übrigen handelt es sich um Folgeänderungen zu Satz 1.

Zu Absatz 2:

Zu Satz 1 empfiehlt der Ausschuss Folgeänderungen, die sich aus der Empfehlung zu Absatz 1 Satz 1 ergeben.

In Satz 2 soll auch die Rückgabe aufgenommen werden. Auch diese soll nach Mitteilung des MI aufgeschoben werden können.

Zu Absatz 3:

Die Satzeinleitung von Satz 1 soll redaktionell an Absatz 1 angepasst werden (vgl. auch die Erläuterung zu § 1 Abs. 1 Nr. 3). Das MI hat zudem mitgeteilt, dass sich die Behörden der unmittelbaren Landesverwaltung, wenn sie das ersetzende Scannen einführen wollen, nach den Vorgaben des Absatzes 1 Satz 2 richten müssen. Dies empfiehlt der Ausschuss im Wortlaut klarzustellen.

In Satz 1/1 soll die in Satz 1 des Entwurfs enthaltene Regelung über die Rückgabe bzw. Vernichtung aufgenommen werden.

Die Verweisung in Satz 2 des Entwurfs soll gestrichen werden. Da der Behörde durch Satz 1/1 ein Ermessensspielraum eingeräumt wird, bedarf es einer Absatz 2 Satz 2 entsprechenden Ausnahmeregelung hier nicht.

Zu § 12 (Basisdienste):

Zu Absatz 1:

Der Ausschuss empfiehlt, in Satz 1 Nr. 1 einen Verweis auf § 2 Abs. 1 EGovG aufzunehmen, sodass der Basisdienst auch für die Zugänge, die bei der Ausführung von Bundesrecht maßgeblich sind, genutzt werden kann.

In Satz 1 Nr. 2 soll die Verweisung vereinfacht werden.

Der in Satz 1 Nr. 3 enthaltene Basisdienst soll sich nach Mitteilung des MI (vgl. auch die Gesetzesbegründung, Drs. 18/1598, S. 58) nur auf Informationen und Formulare im niedersächsischen Ver-

waltungsportal beziehen (hier ist der sog. Bürger- und Unternehmensservice [BUS] gemeint; vgl. dazu Drs. 18/1598, S. 21 f.). Dies soll durch die empfohlene Fassung klargestellt werden.

Satz 1 Nr. 5 soll auch auf § 4 EGovG verweisen, denn der Basisdienst soll nach Mitteilung des MI auch für die Bezahlmöglichkeit bei der Ausführung von Bundesrecht genutzt werden können.

Im Wortlaut von Satz 1 Nr. 6 soll klargestellt werden, dass sich der Empfang und die Verarbeitung elektronischer Rechnungen auch nach § 6 Abs. 4 und der auf dieser Grundlage zu erlassenden Verordnung richtet.

Zu der in Satz 1 Nr. 7 enthaltenen Wendung „Aktenführung … unter Berücksichtigung der Vorgangsbearbeitung“ hat das MI erläutert, dass diese der Klarstellung diene, weil gelegentlich unter dem Begriff der „Aktenführung“ lediglich die Aktenablage und nicht auch die Vorgangsbearbeitung verstanden werde. Dies schließe allerdings nicht das ersetzende Scannen nach § 11 ein; insoweit solle derzeit keine Verpflichtung zur Bereitstellung eines Basisdienstes vorgesehen werden.

In Satz 2 soll zur Klarstellung die Verweisung auf § 9 eingefügt werden.

Durch die empfohlene redaktionelle Umstellung des Satzes 3 soll klargestellt werden, dass jede einzelne Behörde des Landes die Möglichkeit hat, weitere Basisdienste zu entwickeln und bereitzustellen (die Nutzung dieser Basisdienste richtet sich hingegen nach Absatz 2 Satz 2). Nach Mitteilung des MI könne eine der hier genannten anderen Funktionen beispielsweise das ersetzende Scannen nach § 11 sein.

Auch die Empfehlung zu Satz 4 dient zur Verdeutlichung des Regelungsgehalts.

Zu Absatz 2:

In Satz 1 soll die Verweisung auf § 4 a EGovG gestrichen werden, weil diese Vorschrift für niedersächsische öffentliche Auftraggeber nicht gilt und nach Absatz 1 Satz 1 Nr. 6 auch kein Basisdienst zur Ausführung von § 4 a EGovG bereitgestellt wird.

In Satz 2 soll klargestellt werden, dass jede Behörde des Landes für den Einsatz eines anderen Basisdienstes das - von der Bereitstellung des Basisdienstes nach Absatz 1 Satz 3 unabhängige - Einvernehmen mit der/dem IT-Bevollmächtigten der Landesregierung herstellen muss. Mit der Empfehlung zu Satz 2 ist der Ausschuss überdies dem Änderungsvorschlag der Fraktionen von SPD und CDU gefolgt. Demnach sollen die Behörden des Landes (unmittelbare Landesverwaltung) in demselben Umfang zur Nutzung der vom Land bereitgestellten Basisdienste verpflichtet werden wie die Behörden der Kommunen und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (mittelbare Landesverwaltung). Die Verpflichtungen nach § 4 Abs. 2, § 5 Abs. 1 und 2 und § 9 dieses Gesetzes sowie nach § 3 Abs. 1 und 2 EGovG sollen sowohl in der unmittelbaren Landesverwaltung (vgl. Satz 1) als auch in der mittelbaren Landesverwaltung (vgl. Absatz 3 Satz 1) zwingend mit den nach Absatz 1 Sätze 1 und 2 bereitgestellten Basisdiensten erfüllt werden. Die Abweichungsmöglichkeit in Satz 2 soll daher auf die von den Behörden des Landes zusätzlich (zur Erfüllung ihrer 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) zu nutzenden Basisdienste beschränkt werden. Das MI geht davon aus, dass infolgedessen die Behörden des Landes von der nach § 12 Abs. 1 Satz 3 bestehenden Möglichkeit, andere Basisdienste bereitzustellen, für die Verpflichtungen nach § 4 Abs. 2, § 5 Abs. 1 und 2 und § 9 dieses Gesetzes sowie § 3 Abs. 1 und 2 EGovG keinen Gebrauch machen werden, denn diese Basisdienste dürften nach der Empfehlung zu Satz 2 nicht genutzt werden.

Die Empfehlung zu Satz 3 dient zur Verdeutlichung des Regelungsgehalts.

Zu Absatz 3:

Die Satzeinleitung von Satz 1 soll an Absatz 2 Satz 1 angeglichen werden (zu den erfassten Behörden vgl. die Empfehlung zu § 1 Abs. 1 Nr. 3). Dasselbe gilt für die Aufzählung der Verpflichtungen, zu deren Erfüllung die nach Absatz 1 Sätze 1 und 2 bereitgestellten Basisdienste zu nutzen sind (die nach Absatz 1 Satz 3 bereitgestellten Basisdienste sollen nach Mitteilung des MI für die Behörden der mittelbaren Landesverwaltung nicht zur Verfügung stehen). In der Aufzählung der

Verpflichtungen soll § 3 Abs. 1 und 2 EGovG ergänzt werden (auch wenn § 3 Abs. 2 EGovG nicht für Kommunen gilt; vgl. dazu die Erläuterung zu § 5 Abs. 2).

Die in Satz 2 enthaltene Verpflichtung, bestimmte Basisdienste kostenfrei zur Verfügung zu stellen, gehört zwar inhaltlich eher zu Absatz 1, weil sie an die dortigen, zur Bereitstellung der Basisdienste verpflichteten Behörden gerichtet ist, soll jedoch auf Wunsch des MI an dieser Stelle verbleiben. Allerdings soll der Bezug durch eine möglichst weitgehende Verweisung auf Absatz 1 (Satz 1 Nrn. 3 und 4) verdeutlicht werden. Dadurch erledigt sich auch die Korrektur eines redaktionellen Fehlers (in Satz 2 Nr. 4 des Entwurfs ist § 5 Abs. 5 Satz 2 gemeint).

Zu Absatz 4:

Der Ausschuss empfiehlt auf Vorschlag des MI, Absatz 4 insgesamt zu streichen. Da Nummer 1 weder zum Zweck der weiteren Verpflichtungen noch zu deren Ausmaß Näheres enthält (und auch der Inhalt teilweise unklar ist), begegnet die Verordnungsermächtigung verfassungsrechtlichen Bedenken im Hinblick auf das Bestimmtheitsgebot (Artikel 43 Abs. 1 Satz 2 NV), zumal damit - jedenfalls bei den Kommunen - ein Eingriff in die Selbstverwaltungsgarantie (Artikel 57 NV) verbunden sein dürfte. Überdies ist nach der Begründung (Drs. 18/1598, S. 62) derzeit nicht absehbar, wo weiterer Bedarf für (verpflichtend zu nutzende) Basisdienste bestehen könnte. Nummer 2 des Entwurfs lässt zudem nicht klar erkennen, an wen sich die Vorgaben der Verordnung richten sollen. Wenn die Behörden gemeint sein sollten, die die Basisdienste bereitstellen, so handelt es sich bei diesen überwiegend um oberste Landesbehörden (vgl. Absatz 1 Sätze 1 und 2). Um diese entsprechend zu instruieren, bedarf es wohl keiner Verordnung.

Zum Dritten Teil (Informationssicherheit):

Zum Ersten Abschnitt (Allgemeine Vorschriften):

Zur Überschrift:

Die Ausschussempfehlung beruht darauf, dass die Abgrenzung der beiden Abschnitte des Dritten Teils anhand der Überschriften des Entwurfs kaum möglich ist, da der Regelungsgehalt des Zweiten Abschnitts („Einsatz von Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit“) ebenfalls der „Gewährleistung der Informationssicherheit“ (Erster Abschnitt) zugeordnet werden kann, der im Übrigen der Überschrift des Dritten Teils („Informationssicherheit“) ähnelt. Die empfohlene Überschrift beruht auf einem Vorschlag des MI.

Zu § 12/1 (Sicherheitsverbund):

Da § 15 des Entwurfs die grundlegende Vorschrift für die Einrichtung eines Sicherheitsverbundes im Landesdatennetz darstellt, innerhalb dessen die verschiedenen Pflichten nach den §§ 13, 14 und 16 des Entwurfs erfüllt werden, soll diese Regelung den Ersten Abschnitt einleiten. Zudem soll die Überschrift vereinfacht werden, zumal die Worte „Verpflichtung zu Sicherheitsmaßnahmen“ den beabsichtigten Regelungsgehalt von Absatz 3 des Entwurfs (vertragliche Anbindung von Nichtmitgliedern) nicht eindeutig wiedergeben (vgl. dazu die Empfehlung zu Absatz 2).

Zu Absatz 1:

Satz 1 soll nach Mitteilung des MI zum Ausdruck bringen, dass die Behörden und Gerichte des Landes, deren IT-Systeme mit dem Landesdatennetz verbunden sind, allesamt Mitglieder eines Sicherheitsverbundes sind. Dies soll durch die Empfehlung deutlicher hervortreten, zumal die Mitglieder des Sicherheitsverbundes in den weiteren Sätzen in Bezug genommen werden.

Satz 2 enthält nach Mitteilung des MI die grundlegende Bestimmung, dass die Mitglieder des Sicherheitsverbundes gemeinsam die Verantwortung für die Informationssicherheit im Landesdatennetz tragen; dies soll durch die geänderte Satzeinleitung („Jedes Mitglied…“) hervorgehoben werden. Abweichend vom Entwurfswortlaut ist hier laut MI anstelle der „IT-Sicherheit“ die „Informationssicherheit“ (zu diesen Begriffen § 1 Abs. 1 Nrn. 5/1 und 8) gemeint (so auch die Begründung, Drs. 18/1598, S. 66). Durch die Worte „auf der Basis von Risikoanalysen“ kann zudem der Rege-

lungsgehalt von § 15 Abs. 2 Satz 1 des Entwurfs in Satz 2 einbezogen und die Regelung dadurch vereinfacht werden. Das MI hat in diesem Zusammenhang darauf hingewiesen, dass neben dieser gesetzlichen Grundsatzregelung die Leitlinie zur Gewährleistung der Informationssicherheit (ISLL, Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 09.11.2016 - CIO-02850-0007 - VORIS 20500, Nds. MBl. 2016 S. 1193) und die Informationssicherheitsleitlinie (ISLL) Justiz (AV d. MJ v. 06.05.2014 - 1510 - 103.232 [SH 6], Nds. Rpfl. 2014 S. 180) für die darin genannten Behörden und Stellen verbindlich blieben.

Der empfohlene Satz 3 entspricht § 15 Abs. 2 Satz 2 des Entwurfs. Die Vorschrift soll (wie auch Satz 2) im Aktiv stehen, um zu verdeutlichen, dass jedes Mitglied des Sicherheitsverbundes verpflichtet ist, seine Verantwortung wahrzunehmen. Nach Mitteilung des MI soll der zentrale IT-Dienstleister (derzeit IT.N) nicht ein einheitliches Schutzniveau festlegen, an das alle Mitglieder des Sicherheitsverbundes gebunden sind; insbesondere sollen dadurch die Mitglieder nicht verpflichtet werden, die sicherheitstechnischen Anforderungen nach § 13 Abs. 3 Nr. 1 einzuhalten oder die nach § 13 Abs. 3 Nr. 2 bereitgestellten IT-Sicherheitsprodukte einzusetzen. Das Wort „Risikobehandlung“ soll allerdings durch eine Verweisung auf Satz 2 ersetzt werden, um das Gemeinte zu verdeutlichen und den inhaltlichen Zusammenhang mit Satz 2 klarzustellen.

Zu Absatz 2:

Die Ausschussempfehlung beruht darauf, dass das MI zu § 15 Abs. 3 des Entwurfs mitgeteilt hat, dass die Stellen, die zwar keine Mitglieder des Sicherheitsverbundes sind, deren IT-Systeme jedoch mit dem Landesdatennetz verbunden sind, auf vertraglicher Grundlage und nicht - wie der Wortlaut des Entwurfs andeutet - durch Verwaltungsakt zur Gewährleistung der Informationssicherheit verpflichtet werden sollen (vgl. auch die Begründung, Drs. 18/1598, S. 67). Beabsichtigt sei, dass die Stellen im Sinne dieser Regelung (dies können öffentliche und nicht öffentliche Stellen sein [vgl. die Gesetzesbegründung, a. a. O.], nach Mitteilung des MI auch gemeinsame Einrichtungen der Länder, z. B. der NDR) nur dann mit dem Landesdatennetz verbunden werden, wenn sie sich im Gegenzug verpflichten, den Stand der Informationssicherheit im Sicherheitsverbund nach Maßgabe des Absatzes 1 Sätze 2 und 3 einzuhalten sowie der Meldepflicht nach § 16 Abs. 2 des Entwurfs bzw. § 12/2 Abs. 2 der Empfehlung zu entsprechen. Diese beabsichtigte Verknüpfung soll durch die Empfehlung im Wortlaut des Absatzes 2 abgebildet werden. Zudem sollen die Worte „oder eine von ihr beauftragte Stelle“ gestrichen werden (Folgeänderung zu § 1 Abs. 1 Nr. 9; vgl. die dortige Erläuterung).

Zu § 12/2 (Zentralstelle für Informationssicherheit):

§ 16 des Entwurfs soll vor den §§ 13 und 14 verortet werden. Dadurch sollen die Vorschriften, die sich auf die Informationssicherheit beziehen (§§ 12/1 und 12/2), sowie die Vorschriften, die sich auf die IT-Sicherheit beziehen (§§ 13 und 14), sinnvoll geordnet werden. Infolgedessen werden die Verweisungen „nach unten“ in § 13 Abs. 2 Nr. 4 und Abs. 3 Nr. 3 entbehrlich (vgl. die dortigen Empfehlungen).

Zu Absatz 1:

Die in Absatz 1 gewählten Begriffe sollen an die Überschrift angepasst werden („Zentralstelle für Informationssicherheit“). Die Aufgaben der Zentralstelle, die dem Niedersächsischen Computer Emergency Response Team (N-CERT) im Sinne der Nummer 6.5 ISLL entspricht, sollen zudem durch die vorgeschlagene Nummerierung leichter verständlich gefasst werden.

Überdies sollen in Nummer 1 nach Mitteilung des MI die Bedrohungen und Angriffe auf IT-Systeme bezogen und der Begriff „Sicherheitslagebild“ gewählt werden. Das MI hat dazu mitgeteilt, dass es sich hier um ein strategisches Lagebild handele, das sich aus einer Vielzahl von Quellen zusammensetze. Das Lagebild, das nach § 13 Abs. 2 Nr. 2 des Entwurfs erstellt werde, sei hingegen ein operatives (das in das strategische Lagebild einfließe).

In Nummer 2 soll der in § 1 Abs. 1 Nr. 13 des Entwurfs näher bestimmte Begriff „Sicherheitsarchitektur“ ausformuliert werden, weil der Begriff an keiner anderen Stelle des Gesetzes verwendet wird. Das MI hat zur Vereinfachung hier den Begriff „IT-Sicherheitsmaßnahmen“ vorgeschlagen.

Die Begriffsbestimmung in § 1 Abs. 1 Nr. 13 des Entwurfs kann infolgedessen entfallen (vgl. die dortige Empfehlung).

Aufgrund der Empfehlung zu § 1 Abs. 1 Nr. 15 (Begriffsbestimmung des Sicherheitsvorfalls) wird das Wort „informationstechnisch“ in Nummer 3 entbehrlich und soll gestrichen werden. Zu dem Begriff „IT-Sicherheit“ (§ 1 Abs. 1 Nr. 8) anstelle des Begriffs „Sicherheit in der Informationstechnik“ vgl. die Empfehlung zur Überschrift von § 13.

Zu Absatz 2:

Zur Verdeutlichung des Regelungsgehalts sollen die „Behörden und Gerichte des Landes“ durch die Mitglieder des Sicherheitsverbundes ersetzt werden. Die vertraglich nach § 12/1 Abs. 2 der Empfehlung angebundenen Stellen werden durch die Vereinbarung bzw. die Anschlussbedingungen zur Mitteilung nach Absatz 2 verpflichtet (vgl. die Erläuterung dort). Die „Zentralstelle für Informationssicherheit“ soll einheitlich als solche bezeichnet werden (vgl. die Absätze 1 und 3 sowie § 13 Abs. 2 Nr. 4 und Abs. 3 Nr. 3).

Das Wort „informationstechnisch“ soll als Folgeänderung zu § 1 Abs. 1 Nr. 15 (Begriffsbestimmung des Sicherheitsvorfalls) gestrichen werden. Da sich Sicherheitsvorfälle allein auf die IT-Sicherheit auswirken (vgl. § 1 Abs. 1 Nr. 15), soll hier anstelle der Informationssicherheit (§ 1 Abs. 1 Nr. 5/1) der Begriff IT-Sicherheit (§ 1 Abs. 1 Nr. 8) Verwendung finden.

Zudem soll der Begriff „Sicherheitsdomäne“, der nur hier verwendet wird, ersetzt werden. Nach Mitteilung des MI soll es hier nicht nur auf eine mögliche Beeinträchtigung der IT-Sicherheit bei (anderen) Mitgliedern des Sicherheitsverbunds ankommen, sondern es sollen (wie bei § 14) auch mögliche Beeinträchtigungen bei vertraglich nach § 12/1 Abs. 2 angeschlossenen Stellen infrage kommen.

Zu Absatz 3:

Die Empfehlung zu Absatz 3 beruht auf einem Änderungsvorschlag der Fraktionen von SPD und CDU. Die Änderung wurde wie folgt begründet:

> *„Anomalieerkennungssysteme zur Wahrnehmung der Befugnisse nach dem zweiten Abschnitt sind ein integraler Bestandteil einer Sicherheitsarchitektur für Netz- und IT-Systeme in der öffentlichen Verwaltung. Eine Gesamtschau von derartigen Komponenten ist zur Aufgabenerfüllung der Zentralstelle für Informationssicherheit zwingend erforderlich. Eine effiziente Folgenabschätzung von Bedrohungssituationen erfordert die möglichst genaue Kenntnis der Sicherheitsarchitektur. Die Anzeigepflicht für den Betrieb umfasst die Inbetriebnahme, den laufenden Betrieb und die Außerbetriebnahme.“*

Der Ausschuss empfiehlt, den Änderungsvorschlag aufzunehmen und lediglich in redaktioneller Hinsicht anzupassen, um Redundanzen zu vermeiden und die im Dritten Teil verwendeten Begriffe aufzugreifen.

Zu § 13 (Förderung der IT-Sicherheit):

Zur Überschrift:

Da nach Mitteilung des MI zwischen den Begriffen „Sicherheit in der Informationstechnik“ (so die Überschrift), „Sicherheit der Informationstechnik“ (so Absatz 1) und „IT-Sicherheit“ (§ 1 Abs. 1 Nr. 8) keine inhaltlichen Unterschiede bestehen, soll eine einheitliche Bezeichnung im Gesetz gewählt werden. Der Ausschuss empfiehlt auf Vorschlag des MI den in § 1 Abs. 1 Nr. 8 definierten Begriff „IT-Sicherheit“.

Zu Absatz 1:

Zu dem einheitlich zu verwendenden Begriff „IT-Sicherheit“ vgl. die Empfehlung zur Überschrift. Zu der Gliederung des Landesdatennetzes in „Netzabschnitte“ vgl. die Empfehlung zu § 1 Abs. 1 Nr. 9. Das MI hat in diesem Zusammenhang darauf hingewiesen, dass hier eine reine Aufgabenbeschreibung beabsichtigt sei. Konkrete Verpflichtungen ergäben sich aus den Absätzen 2 bis 4.

Zu Absatz 2:

Der einleitende Satzteil soll sprachlich vereinfacht und durch die Bezugnahme auf die jeweiligen „Netzabschnitte“ (vgl. die Erläuterung zu Absatz 1) präzisiert werden. Nummer 1 soll begrifflich auf die §§ 18/1 ff. abgestimmt werden. Dort geht es um die Abwehr von durch Sicherheitslücken, Schadprogrammen oder Angriffen verursachten Gefahren für die IT-Sicherheit. Zu Nummer 2 („IT-Systeme“) vgl. die Erläuterung zu § 1 Abs. 1 Nr. 14. In Nummer 3 soll auf Vorschlag des MI klargestellt werden, dass es hier um Gefahrenvorsorge (vgl. § 1 Abs. 1 Satz 2 NPOG) geht (in Abgrenzung zu der in Nummer 1 geregelten Gefahrenabwehr). Zu Nummer 4 empfiehlt der Ausschuss eine redaktionelle Anpassung; da die Zentralstelle von § 16 nach § 12/2 verlagert werden soll, ist die Verweisung „nach unten“ (Klammerzusatz) hier entbehrlich.

Zu Absatz 3:

Zum einleitenden Satzteil vgl. die Erläuterungen zu den Absätzen 1 und 2 sowie zu § 1 Abs. 1 Nr. 9. Zu dem Begriff „IT-Systeme“ in den Nummern 1 bis 4 vgl. die Anmerkung zu § 1 Abs. 1 Nr. 14. Zu Nummer 2 empfiehlt der Ausschuss auf Vorschlag des MI, die Legaldefinition des Begriffs „IT-Sicherheitsprodukte“ aus § 3 Abs. 1 Satz 2 Nr. 3 BSIG zu übernehmen. In Nummer 3 sollen - wie in den Nummern 1, 2 und 4 - zur Vereinfachung die „Stellen“ als Adressat der Unterstützung genannt werden, nicht die „für Sicherheit der Informationstechnik Verantwortlichen“. Zudem soll der Ausdruck „in Abstimmung“ durch die im Verwaltungsrecht gebräuchlichen Worte „im Benehmen“ ersetzt werden (nach Mitteilung des MI ist das „Einvernehmen“ mit der Zentralstelle nicht erforderlich). Überdies soll präzisiert werden, worauf sich die Unterstützung bezieht (laut MI die Förderung der IT-Sicherheit). Im Übrigen soll Nummer 3 mit Absatz 2 Nr. 4 harmonisiert werden (Klammerzusatz entbehrlich). Zu Nummer 4 hat das MI mitgeteilt, dass der Funktionsfähigkeit neben der Sicherheit kein eigener Anwendungsbereich zukomme; es gehe bei der hier genannten Unterstützung allein um die Wiederherstellung der IT-Sicherheit (in herausgehobenen Fällen).

Zu Absatz 4:

Die empfohlene Fassung soll den beabsichtigten Regelungsgehalt deutlicher zum Ausdruck bringen. Das MI hat mitgeteilt, dass die Regelung dazu diene, die in Absatz 1 genannten Stellen zu verpflichten, für ihren jeweiligen Netzabschnitt die nach Maßgabe des Zweiten Abschnitts (§§ 17 ff.) einzusetzenden IT-Systeme („Intrusion Detection System“ [IDS] bzw. „Security Incident and Event Management-System“ [SIEM-System]) vorzuhalten.

Zu § 14 (Vorübergehende und unaufschiebbare Maßnahmen):

Die Überschrift soll vereinfacht werden, zumal die Formulierung „Gewährleistung der IT-Sicherheit“ unpräzise ist; es geht um die Abwehr einer Gefahr.

Die Empfehlung zu Satz 1 soll durch die redaktionelle Umstellung Tatbestand und Rechtsfolge verständlicher zum Ausdruck bringen. Die empfohlene Fassung stellt zudem klar, dass es laut MI um Weisungen der oder des IT-Bevollmächtigten der Landesregierung („CIO“) gegenüber den Mitgliedern des Sicherheitsverbundes (§ 12/1 Abs. 1 Satz 1) geht, im Rahmen ihrer eigenen Zuständigkeiten und Befugnisse in einer bestimmten, von der/dem CIO vorgegebenen Weise zur Abwehr der gegenwärtigen Gefahr für die IT-Sicherheit tätig zu werden. Die im Gesetzentwurf in zweifacher Hinsicht qualifizierte Gefahr (erstens durch die Gegenwärtigkeit, zweitens durch die Eignung zur Gefährdung anderer Stellen) ist unnötig kompliziert formuliert; sie soll dadurch vereinfacht werden (ohne inhaltliche Änderung), dass die zu ergreifenden Maßnahmen zur Gewährleistung der IT-Sicherheit bei anderen Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, erforderlich sein müssen. Zu dem Begriff „IT-Systeme“ vgl. die Erläuterung zu § 1 Abs. 1 Nr. 14.

Die nach § 12/1 Abs. 2 der Empfehlung an das Landesdatennetz angeschlossenen Dritten können von der/dem IT-Bevollmächtigten nach dem Wortlaut von Satz 1 zwar nicht angewiesen werden (sie sind keine Mitglieder des Sicherheitsverbundes). Das MI hat dazu jedoch mitgeteilt, dass beabsichtigt sei, im Rahmen der Ermessensausübung nach § 12/1 Abs. 2 bzw. bei den vertraglichen Anschlussbedingungen dafür Sorge zu tragen, dass der Anschluss rückgängig gemacht bzw. kurzfristig unterbrochen werden kann, wenn bestimmte dringliche IT-Sicherheitsmaßnahmen (die bei

Landesbehörden Gegenstand von Weisungen nach Satz 1 wären) von angeschlossenen Dritten nicht vollzogen werden.

Der empfohlene Satz 2 soll klarstellen, dass die/der IT-Bevollmächtigte nicht zu Weisungen ermächtigt wird, die nach den §§ 19 ff. zu Eingriffen in Artikel 10 Abs. 1 GG führen (sonst müsste § 14 in § 28 [Einschränkung von Grundrechten] genannt werden, um dem Zitiergebot nach Artikel 19 Abs. 1 Satz 2 GG zu entsprechen).

Zu § 15 des Entwurfs (Sicherheitsverbund, Verpflichtung zu Sicherheitsmaßnahmen):

Die Regelung soll in § 12/1 verlagert werden (vgl. die dortigen Erläuterungen).

Zu § 16 des Entwurfs (Zentralstelle für Informationssicherheit):

Die Regelung soll in § 12/2 verlagert werden (vgl. die dortigen Erläuterungen).

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

Zur Überschrift:

Da es sich bei den einzusetzenden Systemen um „IT-Systeme“ handelt, soll dieser Begriff auch in der Überschrift verwendet werden (vgl. dazu die Erläuterung zu § 1 Abs. 1 Nr. 14).

Zu § 17 (Übertragung und Beschränkung der Befugnisse nach diesem Abschnitt):

Zur Überschrift:

Die Überschrift soll an den empfohlenen Regelungsgehalt der Vorschrift angepasst werden (vgl. die Erläuterungen zu den Absätzen 1 bis 3).

Zu Absatz 1:

Der Ausschuss empfiehlt, Absatz 1 des Entwurfs zu streichen. Zum einen ist die Regelung eines „Geltungsbereichs“ hier missverständlich, da nicht nur die genannten Behörden und Stellen Adressaten der Regelungen dieses Abschnitts sind, sondern auch die von den Maßnahmen betroffenen Personen. Für diese „gilt“ dieser Abschnitt ebenfalls, weil aufgrund der in diesem Abschnitt geregelten Rechtsgrundlagen in ihre Grundrechte eingegriffen werden kann. Zum anderen bedarf es einer Regelung der „Befugnis, Maßnahmen nach dem Zweiten Abschnitt zu treffen“ (Drs. 18/1598, S. 68), hier nicht, weil sich die Befugnis jeder Behörde unmittelbar aus den §§ 19 bis 22 des Entwurfs ergibt (jede Behörde nimmt die Befugnisse für ihre eigenen bzw. die von ihr betriebenen IT-Systeme wahr). Satz 1 des Entwurfs ist damit entbehrlich.

Satz 2 des Entwurfs bestimmt zwar, dass die §§ 19 bis 22 auch für die Gerichte entsprechend gelten sollen, die in den §§ 19 bis 22 des Entwurfs nicht ausdrücklich neben den Behörden genannt werden. Da jedoch Absatz 2 Satz 3 des Entwurfs bzw. Absatz 2/2 der Empfehlung für den gesamten Geschäftsbereich des MJ die Befugnisse auf die dort genannte, vom MJ bestimmte Stelle überträgt, bedarf es auch der Regelung in Satz 2 nicht.

Zu Absatz 2:

Auch Absatz 2 Satz 1 des Entwurfs soll gestrichen werden. Der Begriff des Landesdatennetzes (§ 1 Abs. 1 Nr. 9) erfasst nur die Kommunikationsstrukturen oberhalb der lokalen Netze. Soweit die dazu notwendigen IT-Systeme und Übergabe- und Knotenpunkte von der das Landesdatennetz betreibenden Behörde (derzeit IT.N) betrieben werden (z. B. an den zentralen Übergängen ins Internet, sog. Perimeterschutz), ergibt sich die Zuständigkeit des IT.N unmittelbar aus den §§ 19 bis 22 des Entwurfs (vgl. dazu die Erläuterung zu § 19 Abs. 1 Satz 1). Weitergehende Befugnisse seien nach Mitteilung des MI hier nicht vorgesehen. Insbesondere solle mit Satz 1 nicht die Befugnis be-

gründet werden, Maßnahmen nach den §§ 19 bis 22 auf den von anderen Behörden betriebenen IT-Systemen sowie an deren Übergabe- und Knotenpunkten (gegen deren Willen) durchzuführen (zu der Möglichkeit der Übertragung der Zuständigkeit durch Vereinbarung vgl. die Empfehlung zu Satz 1/1). Satz 1 des Entwurfs ist daher entbehrlich.

Die Empfehlung zu Satz 1/1 beruht auf der Begründung des Gesetzentwurfs, in der ausgeführt wird, dass durch IT.N anderen (insbesondere kleineren) Behörden die Sicherheitstechnologie „in Form einer Dienstleistung“ angeboten werden soll (Drs. 18/1598, S. 69). Dazu sind unterschiedliche Wege denkbar. Wenn die IT-Systeme bzw. Übergabe- und Knotenpunkte von IT.N für die andere Behörde (im Rahmen einer Dienstleistung) betrieben werden, ergibt sich die Befugnis des IT.N zum Einsatz der Sicherheitstechnologie unmittelbar aus den §§ 19 bis 22 des Entwurfs (siehe oben zu Satz 1 des Entwurfs sowie die Erläuterung zu § 19 Abs. 1 Satz 1). Wenn die Behörde ihre IT-Systeme sowie Übergabe- und Knotenpunkte hingegen selbst betreibt, und nur im Hinblick auf die Sicherheitstechnologie (§§ 19 bis 22) auf eine Dienstleistung von IT.N zurückgreifen will, bedarf die damit verbundene Zuständigkeitsvereinbarung wegen der Abweichung von der gesetzlich festgeschriebenen Zuständigkeit einer gesetzlichen Ermächtigung (vgl. dazu *Schmitz*, in: Stelkens/ Bonk/Sachs, VwVfG, 8. Aufl. 2014, § 3 Rn. 13; *Schliesky*, in: Knack/Henneke, VwVfG, 10. Aufl. 2014, vor § 3 Rn. 40 f.). Der Ausschuss empfiehlt auf Vorschlag des MI, diese in der Begründung (a. a. O.) angesprochene Möglichkeit der Befugnisübertragung durch Zuständigkeitsvereinbarung in Satz 1/1 Halbsatz 1 ausdrücklich zu regeln (und die Möglichkeit der Übertragung in die Überschrift aufzunehmen). Ein Anspruch der Behörde gegenüber IT.N soll damit allerdings nicht begründet werden.

Die Empfehlung zu Satz 1/1 Halbsatz 2 dient der Klarstellung. Für die Kommunen, die an das Landesdatennetz angeschlossen sind (nach Mitteilung des MI, das sich insoweit auf die kommunalen Spitzenverbände beruft, sollen mittlerweile sämtliche Kommunen an den Kommunalabschnitt des Landesdatennetzes angeschlossen sein), ergeben sich nach der Konzeption des Gesetzentwurfs drei Möglichkeiten: Zunächst bleibt ihnen die eigenständige Wahrnehmung der Befugnisse im Rahmen ihrer Organisationshoheit überlassen (vgl. die Begründung, Drs. 18/1598, S. 68). Sie können zudem auf eine entsprechende Dienstleistung von IT.N zurückgreifen, indem sie die Befugnisse nach Satz 1/1 Halbsatz 1 übertragen (allerdings nicht in der Anfangsphase des Einsatzes von Anomalieerkennungssystemen; a. a. O., S. 69). Drittens soll ihnen die Möglichkeit kommunaler Zusammenarbeit nach dem Niedersächsischen Gesetz über die kommunale Zusammenarbeit (NKomZG) nicht genommen werden (z. B. - wie bei der KDO - durch einen Zweckverband nach den §§ 7 ff. NKomZG). Auf diese dritte Möglichkeit soll Satz 1/1 Halbsatz 2 (redaktionell angelehnt an § 163 Abs. 2 Halbsatz 2 des Niedersächsischen Kommunalverfassungsgesetzes [NKomVG]) hinweisen. Damit soll zugleich die Möglichkeit der Mitgliedsgemeinden, Aufgaben des eigenen Wirkungskreises auf die Samtgemeinde zu übertragen (§ 98 Abs. 1 Satz 2 NKomVG) unberührt bleiben (vgl. § 1 Abs. 1 Satz 2 NKomZG).

Absatz 2 Sätze 2 und 3 des Entwurfs sollen in die empfohlenen Absätze 2/1 und 2/2 verlagert werden (vgl. die dortigen Erläuterungen).

Zu Absatz 2/1:

Die Empfehlung enthält die in Absatz 2 Satz 2 des Entwurfs enthaltene Beschränkung der Befugnisse nach den §§ 19 bis 22 des Entwurfs im Hinblick auf die von der Landesregierung unabhängigen Behörden (Landesrechnungshof, Landesbeauftragte für den Datenschutz, Landtagsverwaltung) und verdeutlicht diese in ihrem Regelungsgehalt. Soweit die genannten Behörden ihre IT-Systeme sowie Übergabe- und Knotenpunkte selbst betreiben, bedarf es keiner Sonderregelung, weil sie nach den §§ 19 bis 22 des Entwurfs selbst zuständig sind (vgl. dazu die Erläuterung zu § 19 Abs. 1 Satz 1). Einer Sonderregelung bedarf es nur für den Fall, dass durch die Protokollierung bzw. Erhebung des Datenverkehrs an Übergabe- und Knotenpunkten anderer Behörden (z. B. des IT.N) auch der Datenverkehr der hier genannten Behörden erfasst wird; dies sei laut MI mit dem Wort „betroffen“ gemeint. Die empfohlene Fassung soll dies klarstellen. Zudem soll anstelle von „Zustimmung“ der im Verwaltungsrecht übliche Begriff „Einvernehmen“ verwendet werden. Ob das Einvernehmen allgemein oder im Einzelfall erteilt wird (und ggf. mit welchen Maßgaben) und ob es sich z. B. auch auf die Löschung von Daten nach § 18 Abs. 2 des Entwurfs bzw. § 22/1 der Empfehlung erstreckt, bleibt den betroffenen Behörden überlassen. Dass es sich um eine Be-

schränkung der Befugnisse handelt, soll zudem in der Überschrift der Vorschrift zum Ausdruck kommen.

Zu Absatz 2/2:

Die Empfehlung dient dazu, die Regelung aus Absatz 2 Satz 3 des Entwurfs wegen ihrer Eigenständigkeit in einen eigenen Absatz auszugliedern. Sie führt dazu, dass im gesamten Geschäftsbereich des MJ (Gerichte, Staatsanwaltschaften, Justizvollzugseinrichtungen, Rechtsanwalts- und Notarkammern usw.) allein die vom MJ „bestimmte“ Stelle (vgl. § 13 Abs. 1) die Befugnisse nach den §§ 19 bis 22 des Entwurfs wahrnimmt (vgl. dazu bereits die Erläuterung zu Absatz 1), und zwar sowohl für den Netzabschnitt des MJ im Landesdatennetz (vgl. § 1 Abs. 1 Nr. 9 und § 13 Abs. 1) als auch für die im Geschäftsbereich befindlichen lokalen Netze, die mit dem Landesdatennetz verbunden sind.

Zu Absatz 3:

Nach Absatz 3 des Entwurfs sind die Hochschulen und die Einrichtungen des Landes, die mit Forschungsaufgaben betraut sind, die einzigen Stellen der unmittelbaren und mittelbaren Landesverwaltung, die auf den von ihnen betriebenen IT-Systemen die Befugnisse nach den §§ 19 bis 22 nicht wahrnehmen dürfen (vgl. die Begründung, Drs. 18/1598, S. 68). Dies ist nach Mitteilung des fachlich zuständigen Ministeriums für Wissenschaft und Kultur (MWK) wegen deren Einbindung in den Netzbetreiberverbund des Deutschen Forschungsnetzes (DFN) so beabsichtigt. Nur auf einzelnen Rechnern, die an das Landesdatennetz angeschlossen seien und von IT.N betrieben würden, könnten die Befugnisse nach den §§ 19 bis 22 des Entwurfs ausgeübt werden (dann allerdings von IT.N). Dies ergebe sich unmittelbar aus den §§ 19 bis 22 des Entwurfs und werde durch Absatz 3 nicht ausgeschlossen. Die Empfehlung zu Absatz 3, die zudem auf die Regelung eines „Geltungsbereichs“ verzichtet (vgl. dazu die Erläuterung zu Absatz 1), soll diese Reichweite der Ausnahme verdeutlichen. Nach Mitteilung des MI soll die Ausnahmeregelung allerdings die Möglichkeit unberührt lassen, auf den (von IT.N betriebenen) Übergabe- und Knotenpunkten die Befugnisse nach den §§ 19 bis 22 des Entwurfs auszuüben (durch IT.N). Eine Einschränkung wie in Absatz 2 Satz 2 des Entwurfs bzw. Absatz 2/1 der Empfehlung für den Fall, dass dabei der Datenverkehr mit den Hochschulen und Einrichtungen des Landes, die mit Forschungsaufgaben betraut sind, betroffen ist, sieht der Gesetzentwurf nicht vor.

Zu § 18 (Allgemeine Bestimmungen):

Zu Absatz 1:

Der Ausschuss empfiehlt aufgrund rechtlicher Bedenken, Absatz 1 des Entwurfs zu streichen. Der Ausschuss hält die Regelung überdies für entbehrlich. Der Begründung (Drs. 18/1598, S. 69) ist schon nicht zu entnehmen, welcher Regelungszweck hier verfolgt wird, welche „digitalen Daten“ also nicht den folgenden Regelungen unterfallen sollen. Da nach Mitteilung des MI jede IP-Adresse, IMSI o. ä. letztlich einen Personenbezug aufweist, ist weder klar, um welche Daten es gehen soll, noch wozu diese von den folgenden Regelungen ausgenommen werden sollen. Ohne nachvollziehbaren Regelungszweck ist die Regelung entbehrlich. Hinzu treten begriffliche Unklarheiten, z. B. wie sich der Begriff der „Verwendung“ zu der „Verarbeitung“ verhält (vgl. auch die Begründung, Drs. 18/1598, S. 48) oder warum hier auf „digitale“ Daten abgestellt wird (in der Anhörung wurde dieser Begriff kritisiert). Verfassungsrechtlich ist zudem nicht klar, welche Daten „dem Fernmeldegeheimnis … unterliegen *oder* einen Personenbezug aufweisen“ sollen. Das Fernmeldegeheimnis (Artikel 10 Abs. 1 GG) geht dem Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG) als speziellere Garantie vor (so das BVerfG in ständiger Rechtsprechung; vgl. nur BVerfGE 125, 260, 310). Da die dem Fernmeldegeheimnis unterliegenden Inhalts- und Verkehrsdaten zugleich personenbezogene Daten sind, dürfte die Differenzierung („oder“) in die Irre führen. Zur Klarstellung wird der Absatz nicht gebraucht, wenn - wie z. B. bei der Telekommunikationsüberwachung nach § 33 a des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) - im Tatbestand der Befugnisse der §§ 19 ff. hervorgehoben wird, dass diese zur Erhebung personenbezogener Daten ermächtigen. Überdies begegnet eine Regelung, die ausdrücklich auf die Reichweite des Fernmeldegeheimnisses nach Artikel 10 Abs. 1 GG Bezug nimmt, erheblichen verfassungsrechtlichen Bedenken im Hinblick auf das Gebot der Normenklar-

heit und -bestimmtheit. Das BVerfG hat es für unzulässig gehalten, dass sich der Gesetzgeber seiner Aufgabe, die einschlägigen Grundrechte durch gesetzliche Vorkehrungen zu konkretisieren, entzieht, indem er die Entscheidung darüber, wie das Grundrecht auszufüllen und umzusetzen ist, an die Verwaltung weiterreicht (BVerfGE 120, 274, 317). Auch aus diesem Grund soll die Regelung gestrichen werden.

Zu Absatz 2:

Der Regelungsgehalt besteht nach Mitteilung des MI darin, den Anwenderinnen/Anwendern Rechtssicherheit im Hinblick auf eine mögliche Strafbarkeit nach § 303 a des Strafgesetzbuchs (StGB) zu verschaffen (vgl. auch die Begründung, Drs. 18/1598, S. 70). Nach Mitteilung des MI soll die Ermächtigung auch für Daten gelten, die gemeinsam mit dem Schadprogramm gelöscht werden müssen, weil ihre „Rettung“ technisch nicht mit zumutbarem Aufwand möglich ist. Der Ausschuss empfiehlt, die Löschung dieser „mitbetroffenen“ Daten ausdrücklich zu regeln. Um die Chronologie des Vorgehens im Gesetz abzubilden, soll die Regelung allerdings erst hinter den §§ 19 bis 22 des Entwurfs sowie den Empfehlungen zu den §§ 22/1 und 22/2, die der Identifizierung von Schadprogrammen dienen, verortet werden. Der Ausschuss empfiehlt daher, die Regelung in einen neuen § 22/3 zu verlagern.

Zu Absatz 3:

Der Wortlaut der Entwurfsregelung gibt den beabsichtigten Regelungsgehalt nicht vollständig wieder. Nach § 19 des Entwurfs dürfen „personenbezogene Daten … ausgewertet werden“, die zuvor zu einem bestimmten Zweck gespeichert worden sind. Zu welchen anderen Zwecken diese Daten verarbeitet werden dürfen, richtet sich nach dem jeweils einschlägigen Recht und soll nicht durch das NDIG modifiziert werden. Mit Absatz 3 des Entwurfs wird nach Mitteilung des MI bezweckt, dass die Ergebnisse der Auswertung einschließlich der dazu erhobenen und/oder gespeicherten Daten nicht für andere Zwecke verarbeitet werden dürfen (sie dürfen z. B. nicht im Hinblick auf das Leistungsverhalten der Mitarbeiterinnen/Mitarbeiter ausgewertet werden). Dieser Zweckbindungsgrundsatz wird allerdings durch § 27 des Entwurfs durchbrochen, der eine Übermittlung der Daten (und damit eine Verarbeitung für andere Zwecke als zur Gewährleistung der Sicherheit der Informationstechnik) gestattet. Der Ausschuss empfiehlt, diesen Zusammenhang zwischen Zweckbindung (Grundsatz) und Übermittlung (Ausnahme) zu verdeutlichen, indem die Regelung in den § 27 verlagert wird (dort als Absatz 0/1 Satz 1).

Zu § 18/1 (Automatisierte Erhebung und Auswertung von Daten eines Verzeichnis- und Berechtigungsdienstes):

Der Ausschuss empfiehlt, die Rechtsgrundlage für den Betrieb eines sog. Advanced Threat Analytics-Systems (ATA-System) aus § 20 Abs. 1 Satz 4 des Entwurfs (vgl. die Begründung, Drs. 18/1598, S. 75) herauszulösen und in die eigenständige Regelung zu verlagern. Technisch handele es sich laut MI und MJ um eine ganz andere Maßnahme als die übrige in § 20 des Entwurfs geregelte Überwachung des Datenverkehrs an Übergabe- und Knotenpunkten. Abweichend vom Entwurf solle hier der Begriff „Verzeichnis- und Berechtigungsdienst“ verwendet werden, weil ein ATA-System sowohl auf den Datenverkehr von Verzeichnisdiensten (die in einem Netzwerk eine zentrale Sammlung von Daten bestimmter Art in einer hierarchischen Datenbank zur Verfügung stellten) als auch von Berechtigungsdiensten (die den Zugriff auf Verzeichnisdienste regelten) zugreife. Abweichend von § 20 des Entwurfs werde nach Mitteilung von MI und MJ von einem ATA-System der Datenverkehr in dem Verzeichnisdienst selbst oder unmittelbar an dessen Netzwerkanschluss erhoben. Ein ATA-System verarbeite dabei keine Inhalte eines Telekommunikationsvorgangs (Inhaltsdaten). Da Verzeichnis- und Berechtigungsdienste nur die Berechtigungen von Konten und Ressourcen abglichen (Kommunikation zwischen Maschine und Maschine), die eine Kommunikation der Nutzerinnen/Nutzer erst ermöglichten, verarbeite ein ATA-System auch keine Verkehrsdaten; der Schutzbereich von Artikel 10 Abs. 1 GG sei infolgedessen nicht eröffnet. Zweck der Maßnahme sei nach Mitteilung von MI und MJ die Suche nach auffälligem Datenverkehr, indem der erhobene Datenverkehr mit dem Normalzustand automatisch abgeglichen werde. Als auffälliger Datenverkehr gälten z. B. ungewöhnlich häufige, direkt aufeinanderfolgende Anmeldeversuche, die nur von einer Kennung ausgehen, ungewöhnliche Bewegungsmuster durch Konten von System-

diensten, gleichzeitige Anmeldeversuche einer Kennung aus unterschiedlichen Subnetzen, die Modifizierung von sensiblen Benutzergruppen oder die Nutzung von identischen (geklonten) Kerberos-Tickets.

Der vom Ausschuss empfohlene Absatz 1 enthält die Ermächtigung zur Datenerhebung und -auswertung, die lediglich durch die Zweckbestimmung und die Erforderlichkeit zu dessen Erfüllung (sowie den allgemeinen Verhältnismäßigkeitsgrundsatz) begrenzt ist. Eine weitergehende (anlassbezogene) Eingriffsschwelle dürfte hier nach den Maßstäben des BVerfG wohl auch nicht erforderlich sein (vgl. nur BVerfG, NJW 2019, 827, 834, Rn. 94). Jeder Behörde soll nach Mitteilung von MI und MJ die Befugnis für die von ihr betriebenen, mit dem Landesdatennetz verbundenen IT-Systeme zustehen. Das Wort „personenbezogener“ soll verdeutlichen, dass die Regelung in das Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG) eingreift. Die Auswertung von Daten, die keinerlei Personenbezug aufweisen, wird dadurch nicht ausgeschlossen, denn dafür bedarf es keiner gesetzlichen Ermächtigung (durch die Verarbeitung solcher Daten wird nicht in Grundrechte eingegriffen; vgl. dazu bereits die Erläuterung zu § 18 Abs. 1 des Entwurfs).

Absatz 2 der Empfehlung enthält eine Löschungsverpflichtung für die nach Absatz 1 erhobenen und ausgewerteten Daten. Eine solche fehlte in § 20 des Entwurfs (§ 20 Abs. 2 Satz 1 bezieht sich nur auf Absatz 1 Satz 3). Die empfohlene Regelung orientiert sich an § 21 Abs. 3 und § 22 Abs. 4.

Zu § 19 (Automatisierte Auswertung von Ereignisdokumentationen und Datenverkehr):

Zur Überschrift:

Da eine Überschrift in möglichst eingängiger Weise den Regelungsgehalt der Vorschrift beschreiben soll, dabei aber notwendigerweise auch vergröbern muss, soll hier zunächst klargestellt werden, dass es in der Vorschrift allein um die automatisierte Auswertung geht. Diese ist zwar teilweise auch mit der vorherigen Erhebung von Daten verbunden (vgl. die Empfehlung zu Absatz 1/1), jedoch steht die Auswertung im Vordergrund. Auch soll hervorgehoben werden, dass es hier um die Auswertung von Ereignisdokumentationen (Absatz 1) und Datenverkehr (Absatz 1/1) geht.

Zu Absatz 1:

Nach Mitteilung des MI ist in Satz 1 mit der „Abwehr von Gefahren für die IT-Sicherheit“ lediglich eine Zweckbestimmung gemeint, keine Eingriffsschwelle (vgl. auch die Begründung, Drs. 18/1598, S. 70). Diese Zweckbestimmung schließt ein, zunächst nach Sicherheitslücken, Schadprogrammen und Angriffen, die Gefahren für die IT-Sicherheit verursachen können, zu forschen. Daraus folgt, dass die Behörde jederzeit die hier geregelte Auswertung durchführen darf, soweit dies zu dem genannten Zweck erforderlich ist (und solange sie dabei nicht unverhältnismäßig vorgeht). Der Ausschuss empfiehlt, dies im Wortlaut zu verdeutlichen (vgl. auch die Empfehlung zu § 18/1 Abs. 1). Nach Mitteilung des MI soll jeder Behörde die Befugnis auf den von ihr betriebenen IT-Systemen, die mit dem Landesdatennetz verbunden sind, zustehen. Auch dies soll im Wortlaut verdeutlicht werden. Durch die empfohlene Satzumstellung wird zudem klargestellt, dass es um die Auswertung von Daten geht, die bereits zuvor auf den betroffenen IT-Systemen „zum Erkennen und Nachverfolgen von Auffälligkeiten“ gespeichert worden sind. Satz 1 enthält also keine Befugnis zu deren Speicherung, sondern setzt die Speicherung aufgrund anderer Rechtsvorschriften voraus (laut MI sind dies § 3 des Niedersächsischen Datenschutzgesetzes [NDSG] und Artikel 6 Abs. 1 DSGVO). Durch die empfohlene Ergänzung des Wortes „personenbezogene“ soll verdeutlicht werden, dass es sich bei Absatz 1 um eine datenschutzrechtliche Befugnis handelt, die in das Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG) eingreift. Soweit die hier auszuwertenden Ereignisdokumentationen im Rahmen eines Telekommunikationsvorgangs gespeichert werden, dürfte es sich zugleich um Verkehrsdaten nach § 3 Nr. 30 TKG handeln, deren Schutz das Fernmeldegeheimnis (Artikel 10 Abs. 1 GG) gewährleistet (daher auch die Nennung von § 19 in § 28). Für Daten, die keinerlei Personenbezug aufweisen, bedarf es hingegen keiner Ermächtigung, weil durch deren Verarbeitung nicht in Grundrechte eingegriffen wird. Dass für die Auswertung der Daten die in den Sätzen 2 und 3 enthaltenen Maßgaben gelten, soll in Satz 1 hervorgehoben werden.

Die zu Satz 2 Nr. 5 empfohlene Änderung beruht auf dem Änderungsvorschlag der Fraktionen von SPD und CDU. Die Änderung wurde wie folgt begründet:

> *„Bei der Auswertung der Ereignisdokumentationen ist es erforderlich, dass neben der Auswertung der bereits in § 19 Absatz 1 Satz 2 aufgelisteten Ereignisdokumentationen auch solche von lokalen Anwendungen auf den Systemen ausgewertet werden. Wenn ein Angreifer in ein Netzwerk eindringt, dann dringt er auch auf die lokalen Systeme ein. Ein solches Eindringen von Angreifern kann dann nur erkannt werden, wenn auch die Ereignisdokumentation der lokal installierten Anwendersoftware ausgewertet wird. Nur auf diese Weise kann umfassend festgestellt werden, welche Lücken der Angreifer ausgenutzt hat, um diese Lücke dann gegen neue Angriffe absichern zu können."*

Das MI hat dazu mitgeteilt, dass z. B. Start und Ende des Programms sowie Fehlerzustände und Abstürze protokolliert werden sollen, grundsätzlich jedoch nicht die tatsächliche Nutzung. Bei Browsern und Proxys werde zwar die URL aufgezeichnet, diese tauche jedoch auch im nach Absatz 1/1 überwachten Datenverkehr auf, werde also bereits erfasst. Daher komme der beabsichtigten Erweiterung keine höhere Persönlichkeitsrelevanz zu.

Zu Satz 3 hat das MI ausgeführt, dass die Vorschrift aus datenschutzrechtlicher Sicht erforderlich sei, weil bisher getrennt verarbeitete Datenbestände zusammengeführt und ausgewertet werden sollen. Der Ausschuss empfiehlt dazu lediglich eine redaktionelle Verbesserung.

Zu Absatz 1/1:

In Absatz 1/1 soll die in § 20 Abs. 1 des Entwurfs enthaltene Befugnis zur automatisierten Erhebung und Auswertung des Datenverkehrs aufgenommen werden, weil diese Maßnahme gemeinsam mit der in Absatz 1 geregelten Auswertung gespeicherter Log-Dateien die erste Stufe der Angriffserkennungssysteme (IDS/SIEM-Systeme) bildet.

Auch hier ist nach Mitteilung des MI mit der „Abwehr von Gefahren für die IT-Sicherheit" in Satz 1 lediglich eine Zweckbestimmung gemeint, keine Eingriffsschwelle, was im Wortlaut verdeutlicht werden sollte (vgl. die Erläuterung zu Absatz 1 Satz 1). Auch hier soll nach Mitteilung des MI jeder Behörde die Befugnis auf den von ihr betriebenen, mit dem Landesdatennetz verbundenen IT-Systemen zustehen, hier allerdings nur an den Übergabe- und Knotenpunkten. Zudem soll hier hervorgehoben werden, dass die Suche nach Maßgabe des Satzes 2 erfolgt.

Satz 2 soll sprachlich gestrafft werden. Dabei soll wie in Absatz 1 Satz 1 hervorgehoben werden, dass die Befugnis nur für die Erhebung personenbezogener Daten erforderlich ist. In Satz 2 soll zudem die Befugnis zur unverzüglichen Auswertung der erhobenen und entschlüsselten Daten aus Satz 3 aufgenommen werden; dadurch wird Satz 3 insgesamt entbehrlich (dazu gleich).

Nach dem Änderungsvorschlag der Fraktionen von SPD und CDU sollte Satz 3 die folgende Fassung erhalten:

> *„[3]Es dürfen insbesondere Kopfdaten, Übertragungsprotokolle und Steuerdaten unverzüglich ausgewertet werden."*

Dieser Vorschlag wurde wie folgt begründet:

> *„Die auszuwertenden Protokolltypen sollten nicht enumerativ und abschließend aufgelistet werden. Stattdessen sollte eine technik-neutrale und zukunftsoffene Formulierung gewählt werden, um zu gewährleisten, dass auch andere im Landesdatennetz zum Einsatz kommende Netzwerkprotokolle auf Anomalien überprüft werden können. Eine technik-neutrale Formulierung ist insbesondere mit Blick auf die rasche Entwicklung neuer Angriffsformen und der Notwendigkeit zur schnellen Anpassung der Detektionssysteme erforderlich, um auch zukünftig Angriffe abwehren zu können."*

Der Ausschuss empfiehlt demgegenüber, Satz 3 ganz zu streichen, weil die Regelung entbehrlich ist. Die Befugnis zur unverzüglichen automatisierten Auswertung des erhobenen und entschlüsselten Datenverkehrs soll - ohne weitere Beschränkung - in Satz 2 aufgenommen werden. Nach Mitteilung des MI liegt dem Gesetzentwurf die Konzeption zugrunde, dass auf der ersten Stufe der Auswertung des Datenverkehrs sowohl Verkehrsdaten (§ 20 Abs. 1 des Entwurfs) als auch Inhalts-

daten (§ 22 Abs. 1 des Entwurfs) automatisiert auf Regelverletzungen durchsucht werden dürfen; unterschiedliche Eingriffsschwellen oder Verfahrensvorschriften sind insoweit nicht vorgesehen. Vor diesem Hintergrund empfiehlt der Ausschuss, die erste Stufe der Auswertung in § 19 Abs. 1 und 1/1 für Verkehrs- und Inhaltsdaten gemeinsam zu regeln und erst auf der zweiten und dritten Stufe zwischen Verkehrs- und Inhaltsdaten zu unterscheiden (vgl. dazu die Erläuterung zu Absatz 1/2). Im Gesetzentwurf ist zwar auf der ersten Stufe vorgesehen, sämtliche (nicht nur die ggf. in den Kopfdaten enthaltenen) Inhaltsdaten automatisiert auszuwerten (vgl. § 22 Abs. 1 des Entwurfs), nicht jedoch auch sämtliche den verschiedenen Protokollschichten (IP, TCP/UDP, HTTP/FTP usw.) zugeordneten Verkehrsdaten (sondern nur die in § 20 Abs. 1 Satz 3 des Entwurfs genannten). Dieses Regelungskonzept hätte mithin zur Folge, dass zwar sämtliche Inhaltsdaten im laufenden Datenverkehr analysiert werden dürften, nicht hingegen sämtliche technischen „Verpackungen“ dieser Inhaltsdaten. Diese - auch vom MI unbeabsichtigte - Einschränkung aufzuheben, war das Ziel des Änderungsvorschlages. Zur Erreichung dieses Regelungsziels ist die zu Satz 3 vorgeschlagene Formulierung allerdings aus mehreren Gründen ungeeignet. Zum einen deutet die Nennung von Regelbeispielen („insbesondere Kopfdaten, Übertragungsprotokolle und Steuerdaten“) darauf hin, dass noch weitere Verkehrsdaten (die keine Kopfdaten, Übertragungsprotokolle oder Steuerdaten sind) unverzüglich ausgewertet werden könnten. Das ist nach Mitteilung des MI aber nicht der Fall; es gebe keine anderen Arten von Verkehrsdaten. Dies entspricht auch der Intention des Änderungsvorschlages, demzufolge gerade keine Verkehrsdaten (d. h. technische „Verpackungen“ von Inhaltsdaten) von der Analyse ausgenommen werden sollen. Zum anderen lässt die Formulierung des Änderungsvorschlages nicht erkennen, dass die Regelung auch zur automatisierten Auswertung der von den verschiedenen Protokoll-Schichten „verpackten“ Inhaltsdaten ermächtigen soll (siehe oben). Die Inhaltsdaten müssten also zur Verdeutlichung des beabsichtigten Regelungsgehalts eigentlich neben den „Kopfdaten, Übertragungsprotokollen und Steuerdaten“ genannt werden. Damit würde der Datenverkehr allerdings nach Mitteilung des MI vollständig erfasst, sodass Satz 3 keine Einschränkung mehr enthalten würde. Dies wäre allerdings nur schwer erkennbar. Vor diesem Hintergrund empfiehlt der Ausschuss, auf die Regelung in Satz 3 insgesamt zu verzichten und Satz 2 um die Befugnis zur unverzüglichen automatisierten Auswertung des Datenverkehrs zu ergänzen (ohne Beschränkung auf bestimmte Verkehrs- oder Inhaltsdaten). Da die Regelung gegenüber dem Gesetzentwurf nur die Auswertung einzelner weiterer Typen von Verkehrsdaten (aus bisher im Landesdatennetz nicht genutzten Protokollen, z. B. FTP oder SFTP) gestattet, dürfte damit keine nennenswerte Vertiefung des Grundrechtseingriffs verbunden sein.

Satz 4 des Entwurfs betrifft die Verzeichnis- und Berechtigungsdienste und soll in den neuen § 18/1 verlagert werden (vgl. die Erläuterung dort).

Zu Absatz 1/2:

Die von Absatz 2 Satz 3 sowie § 20 Abs. 2 Satz 2 des Entwurfs abweichende Empfehlung zu Absatz 1/2 dient zunächst dazu, auf der ersten Stufe der automatisierten Auswertung eine einheitliche Regelung für Verkehrsdaten und Inhaltsdaten zu schaffen (nach dem Entwurf sollte sich die Auswertung von Inhaltsdaten allein nach § 22 richten). Diese Empfehlung trägt dem Umstand Rechnung, dass nach dem Gesetzentwurf die Anforderungen an die Verkehrs- und Inhaltsdatenauswertung sowohl hinsichtlich der Eingriffsschwelle als auch hinsichtlich der Verfahrensanforderungen identisch sind (vgl. § 22 Abs. 1 des Entwurfs). Durch die einheitliche Regelung der ersten Stufe der Auswertung soll die Regelung leichter verständlich werden. Die zweite und dritte Stufe der Auswertung sollen hingegen - insoweit entsprechend dem Gesetzentwurf - wegen der unterschiedlichen Verfahrensanforderungen in verschiedenen Regelungen für Verkehrsdaten (§ 21) und Inhaltsdaten (§ 22) verbleiben.

Die Empfehlung zu Absatz 1/2 soll überdies klarstellen, dass Telekommunikations-Inhaltsdaten, wenn sie nach den Absätzen 1 und 1/1 verarbeitet werden, lediglich hinsichtlich ihrer technischen Bedeutung ausgewertet werden dürfen. Nach Mitteilung des MI sollen die von den Absätzen 1 und 1/1 erfassten Inhaltsdaten allein daraufhin untersucht werden, ob sie Schadcode enthalten. Es solle nicht zulässig sein, die kommunikative Bedeutung der Daten bzw. den semantischen Inhalt der Telekommunikation auszuwerten. Dieses Verbot ergebe sich zwar bereits aus dem Verhältnismäßigkeitsprinzip (die Auswertung der kommunikativen Bedeutung der Daten sei laut MI für die Abwehr der Gefahr für IT-Sicherheit unter keinen Umständen erforderlich). Da diese Beschränkung jedoch für die Bewertung der Eingriffstiefe der Maßnahmen bedeutsam ist (vgl. dazu die Erläute-

rungen zu § 21 Abs. 2), soll sie ausdrücklich in dem empfohlenen Absatz 1/2 hervorgehoben werden (vgl. zur zweiten und dritten Stufe der Auswertung von Inhaltsdaten die entsprechenden Empfehlungen zu § 22 Abs. 2 Satz 1 Halbsatz 2 sowie Abs. 3 Satz 1 Halbsatz 2). Da die Legaldefinition der Inhaltsdaten in § 1 Abs. 1 Nr. 7 gestrichen werden soll (vgl. die Erläuterung dort), bietet sich hier die redaktionelle Klarstellung durch Klammerzusatz an, dass hier und im Folgenden mit den „Inhaltsdaten“ die „Inhalte einer Telekommunikation“ gemeint sind.

Zu Absatz 2:

Satz 1 soll auch für die Auswertung nach Absatz 1/1 gelten; § 20 Abs. 2 Satz 1 des Entwurfs wird dadurch entbehrlich. Zudem soll der Tatbestand der Vorschrift an die Empfehlungen zu den Absätzen 1 und 1/1 angepasst werden. Weiter soll deutlich werden, dass die Löschungsverpflichtung umfassend ist, sich also sowohl auf die zur Auswertung kopierten und zusammengeführten bzw. erhobenen Daten als auch auf die Auswertungsergebnisse erstreckt.

Da Satz 2 nur die Auswertung der bereits auf Grundlage anderer Rechtsvorschriften gespeicherten Daten betrifft (vgl. die Erläuterung zu Absatz 1 Satz 1), soll dies im Wortlaut verdeutlicht werden.

Satz 3 des Entwurfs soll - zusammen mit § 20 Abs. 2 Satz 2 des Entwurfs - in Absatz 1/2 verlagert bzw. durch die dortige Regelung ersetzt werden (vgl. die Erläuterung zu Absatz 1/2).

Satz 4 des Entwurfs betrifft die Auswertung, nicht die in Absatz 2 ansonsten geregelte Löschung. Zur Verbesserung der Rechtssystematik soll die Regelung in den § 27 Abs. 0/1 Satz 2 (Zweckbindungsgrundsatz) verlagert werden, zumal das Verbot nach Mitteilung des MI nicht nur für die Auswertung nach § 19 Abs. 1 des Entwurfs gelten soll, sondern auch für die anderen Auswertungstatbestände (§§ 20 bis 22 des Entwurfs).

Zu § 20 (Erhebung und Auswertung des Datenverkehrs):

Die in Absatz 1 Sätze 1 bis 3 des Entwurfs enthaltene Befugnis soll in § 19 als Absatz 1/1 aufgenommen werden (vgl. die dortige Erläuterung), die in Absatz 1 Satz 4 des Entwurfs enthaltene Regelung über die Auswertung von Verzeichnisdiensten in § 18/1 (vgl. die Erläuterung dort).

Absatz 2 des Entwurfs entspricht § 19 Abs. 2 Sätze 1 und 3 und wird daher von den dortigen Regelungen abgedeckt, sodass auch dieser Absatz hier gestrichen werden soll.

Zu § 21 (Weitere Auswertung ohne Inhaltsdaten in Verdachtsfällen):

Zur Überschrift:

Die Überschrift ist im Entwurf wenig aussagekräftig, da bereits in den §§ 19 und 20 des Entwurfs die „Auswertung“ geregelt wird. Durch die empfohlene Fassung soll deutlich werden, dass die hier geregelte Auswertung Verdachtsfälle betrifft (also die zweite und dritte Stufe der Eskalation, vgl. dazu die Erläuterung zu § 19 Abs. 1/2) und nicht durchgehend automatisiert durchgeführt wird (vgl. Absatz 2).

Zu Absatz 1:

Die in Satz 1 enthaltene Eingriffsschwelle für die weitere automatisierte Auswertung (zweite Stufe) soll mit der Löschungsverpflichtung in § 19 Abs. 2 harmonisiert werden. Nach Mitteilung des MI liegen zureichende tatsächliche Anhaltspunkte dann vor, wenn bei der Auswertung nach § 18/1 oder § 19 eine Regelverletzung festgestellt wird. Dieser werde dann (automatisiert) nach Absatz 1 weiter nachgegangen, indem weitere automatisierte Regeln auf den Datenbestand angewendet werden. Diese Regeln würden zwar manuell ausgelöst, jedoch automatisiert ausgeführt. Personenbezogene Daten würden auf dieser Stufe mithin nicht von Menschen wahrgenommen. Eine nicht automatisierte bzw. manuelle Auswertung der personenbezogenen Daten erfolge erst auf der dritten Stufe (Absatz 2). Anstelle der „bestimmten Daten“ soll klargestellt werden, dass hier die nach § 18/1 Abs. 1 oder § 19 Abs. 1 oder 1/1 erhobenen oder ausgewerteten Daten sowie die Auswertungsergebnisse gemeint sind. Das MI hat mitgeteilt, dass die nach § 18/1 Abs. 1 oder § 19 Abs. 1 oder 1/1 ausgewerteten Daten auf dieser Eskalationsstufe zusammengeführt und gemeinsam aus-

gewertet werden sollen; dies soll im Wortlaut abgebildet werden. Zudem soll die Erforderlichkeit für die Erkennung oder Abwehr der Gefahr für die IT-Sicherheit klarer gefasst werden.

Die für die weitere Auswertung erforderliche Speicherung soll aus Satz 2 des Entwurfs in Satz 1 verschoben werden. Nach Mitteilung des MI beginnt die Speicherfrist mit dem Zeitpunkt der Feststellung der Regelverletzung zu laufen (d. h. mit der Feststellung der zureichenden tatsächlichen Anhaltspunkte). Die Daten dürfen dann zwar mit denen aus anderen Regelverletzungen zusammengeführt werden, wenn sie zur Erkennung und Abwehr derselben Gefahr für die IT-Sicherheit erforderlich sind (Zweckidentität), für die Löschungsfrist ist jedoch die jeweilige Regelverletzung maßgeblich, die zu ihrer Speicherung geführt hat. Die empfohlene Verlängerung der Speicherfrist von 7 auf 30 Tage beruht auf dem Änderungsvorschlag der Fraktionen von SPD und CDU. Diese Änderung wurde wie folgt begründet:

> *„Die in den §§ 21 und 22 des NDIG-E vorgesehene 7-tägige Speicherfrist geht auf ein Rechtsgutachten sowie auf eine Entscheidung des BGH zurück. In dieser Entscheidung hatte der BGH die Speicherung für sieben Tage zum Erkennen, Eingrenzen oder Beseitigen von Störungen einer Telekommunikationsanlage durch den Anbieter nach sachverständige Beratung von als für „auf das zur Erreichung der legitimen Zwecke notwendige Maß begrenzt“ angesehen.*
>
> *Seit diesem Urteil des BGH, das vom 3. Juli 2014 ist, sind Angriffsmethoden und Schadsoftware in erheblichem Umfang weiterentwickelt worden. Nach neuerlicher Auskunft der Experten, insbesondere auch nach der langjährigen Erfahrung des BSI, sind die im derzeitigen NDIG-E vorgesehenen sieben Tage nicht mehr für die Erkennung und Abwehr von Gefahren für die IT-Sicherheit ausreichend. Die steigende Komplexität der verwendeten Schadsoftware und die stetig weiter steigenden hohen Angriffszahlen stellen besondere Herausforderungen dar, die zunehmend mehr Zeit in Anspruch nimmt und nehmen wird.“*

Der GBD hatte insoweit keine durchgreifenden rechtlichen Bedenken. Durch die Verlängerung der Speicherungsfrist auf der zweiten Stufe der Auswertung werde der Grundrechtseingriff zwar (in zeitlicher Hinsicht) vertieft. Allerdings würden die Daten weiterhin auf dieser Stufe ausschließlich automatisiert ausgewertet. Im Hinblick auf die Erforderlichkeit verfüge der Gesetzgeber über einen gewissen Einschätzungsspielraum, der aus Sicht des GBD hier angesichts der Begründung nicht überschritten sein dürfte.

Zu Satz 2 empfiehlt der Ausschuss lediglich redaktionelle Folgeänderungen.

In einem neuen Satz 3 soll die Löschungspflicht als Kehrseite der Speicherung nach Satz 1 ausdrücklich geregelt werden (redaktionell angelehnt an die Empfehlung zu § 19 Abs. 2).

Zu Absatz 2:

Der Ausschuss empfiehlt, die Voraussetzung der weiteren, auch manuellen Auswertung nach Satz 1 (dritte Stufe der Verkehrsdatenauswertung) klarer herauszustellen und sprachlich an Absatz 1 Satz 1 anzulehnen. Zudem soll ausdrücklich bestimmt werden, dass auf dieser Eskalationsstufe die Daten über die Speicherfrist des Absatzes 1 Satz 1 hinaus gespeichert werden dürfen (vgl. die Begründung, Drs. 18/1598, S. 76). Da das MI mitgeteilt hat, dass sich die für die dritte Stufe der Auswertung notwendigen Anhaltspunkte auch bereits aus der ersten Stufe der Auswertung (§§ 18/1 und 19) ergeben könnten (Sprungeskalation), soll diese Variante im Wortlaut von Satz 1 abgebildet werden. Das MI hat zu Satz 1 mitgeteilt, dass durch die manuelle Auswertung von Log-Dateien (§ 19 Abs. 1) in Verbindung mit dem Datenverkehr im Netz (§ 19 Abs. 1/1) und am Verzeichnisdienst (§ 18/1) auch durch Sicherheitslücken verursachte Gefahren für die IT-Sicherheit detektiert werden könnten. Der Ausschuss empfiehlt daher auf Vorschlag des MI, die Regelung auch auf diese Konstellation zu erstrecken.

Satz 2 des Entwurfs verbindet zwei unterschiedliche Regelungsgehalte, die nach der Empfehlung des Ausschusses in zwei getrennten Vorschriften (in den Sätzen 1 und 6) zum Ausdruck gebracht werden sollen. Einerseits bestimmt Satz 2 des Entwurfs, dass die Datenverarbeitung nach Satz 1 nur zulässig ist, soweit und solange sie zur Erfüllung ihres Zwecks (Erkennung und Abwehr der in Satz 1 genannten Gefahr) erforderlich ist. Dieser Regelungsgehalt soll in Satz 1 aufgenommen werden (vgl. auch die Empfehlungen zu Absatz 1 Satz 1, § 18/1 Abs. 1 sowie § 19 Abs. 1 Satz 1

und Abs. 1/1 Satz 1). Andererseits gestattet Satz 2 des Entwurfs auch die Datenverarbeitung „zur Erkennung und Abwehr *anderer* Schadprogramme oder Angriffe“. Diese Datenverarbeitung dient nicht mehr dem in Satz 1 genannten Anlass bzw. Zweck; nach Mitteilung des MI geht es dabei um die Nutzung der Daten zum Umgang mit dem „Beifang“ der Auswertung nach Satz 1, der über die eingesetzte Sensorik und Eskalation vorher noch nicht entdeckt worden ist. Nach den Maßstäben des BVerfG dürfte es sich bei dieser Datenverarbeitung nicht um eine (an strengere Voraussetzungen geknüpfte) Zweckänderung handeln, sondern um eine - vom BVerfG sogenannte - weitere Nutzung im Rahmen der ursprünglichen Zwecke. Deren verfassungsrechtliche Voraussetzungen dürften hier erfüllt sein, da die Daten „seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter“ genutzt werden sollen (vgl. BVerfGE 141, 220, 324 f., Rn. 278 f.). Dieser Regelungsgehalt soll in den neuen Satz 6 aufgenommen werden. Da nach der Rechtsprechung des BVerfG die weitere Nutzung im Rahmen des ursprünglichen Zwecks „als bloßer Spurenansatz“ bzw. „als schlichter Ausgangspunkt für weitere Ermittlungen“ zulässig ist (a. a. O., S. 325 f., Rn. 280 f.), hält es der Ausschuss für ausreichend, die weitere Nutzung an „tatsächliche Anhaltspunkte“ für den Verdacht eines (anderen) Angriffs oder Schadprogramms zu knüpfen. Nach Mitteilung des MI soll die weitere Nutzung aber ebenfalls dem Behördenleitervorbehalt nach den Sätzen 3 und 4 unterliegen. Diesem Vorschlag ist der Ausschuss mit seiner Empfehlung zu Halbsatz 2 gefolgt. Die durch eine Sicherheitslücke verursachte Gefahr für die IT-Sicherheit soll auch in Satz 6 - ebenso wie in Satz 1 - aufgenommen werden.

Da nach Mitteilung des MI die Anordnung der Behördenleitung im Einvernehmen mit der weiteren Person ergehen soll, empfiehlt der Ausschuss, dies im Wortlaut von Satz 3 zu verdeutlichen. Zwar soll die weitere Person im dienstrechtlichen Sinne nicht weisungsunabhängig sein (dies bedürfte einer ausdrücklichen gesetzlichen Regelung), jedoch geht das MI davon aus, dass sich die beabsichtigte Schutzwirkung bereits daraus ergebe, dass die Behördenleitungen von der Möglichkeit, die weitere Person zur Erteilung des Einvernehmens anzuweisen, nur sehr zurückhaltend Gebrauch machen werden. Im Übrigen erhielten weder die Behördenleitung noch die weitere Person bei ihrer Entscheidung Zugang zu entpseudonymisierten personenbezogenen (Verkehrs-)Daten ihrer Mitarbeiterinnen/Mitarbeiter, weil die Daten zu dem Zeitpunkt der Entscheidung noch nicht entpseudonymisiert seien. In Satz 4 soll auf Vorschlag des MI auch die Situation berücksichtigt werden, dass eine geeignete Person mit der Befähigung zum Richteramt zwar bei der Behörde beschäftigt ist, jedoch zum Zeitpunkt der Entscheidung nicht zur Verfügung steht (z. B. wegen Krankheit, Urlaub, Teilzeit, Elternzeit o. ä.). Dass Satz 5 des Entwurfs nur für die in Satz 4 geregelte Ersatzperson gelten soll (so die Mitteilung des MI) soll dadurch verdeutlicht werden, dass der Regelungsgehalt von Satz 5 durch die Worte „und von deren Behördenleitung bestimmte“ (Person) in Satz 4 übernommen und Satz 5 gestrichen wird.

Der Ausschuss war sich bewusst, dass der mit den Sätzen 3 bis 5 des Entwurfs verbundene Verzicht auf den Richtervorbehalt, der sowohl in der Literatur (vgl. *Buchberger*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, Rn. 22 zu § 5 BSIG) als auch von der LfD (vgl. die Begründung, Drs. 18/1598, S. 29 und 77) kritisiert worden ist, im Hinblick auf den Verhältnismäßigkeitsgrundsatz ein verfassungsrechtliches Risiko begründet. Dieses erscheint dem Ausschuss allerdings als überschaubar, wie sich aus den folgenden Überlegungen ergibt:

Die automatisierte Erhebung und Auswertung nach § 19 Abs. 1 und 1/1 (erste Stufe) sowie nach Absatz 1 (zweite Stufe) und insbesondere die in Absatz 2 geregelte nicht automatisierte, entpseudonymisierte Auswertung (dritte Stufe) führt, soweit davon Telekommunikations-Verkehrsdaten erfasst werden, d. h. die näheren Umstände eines Telekommunikationsvorgangs (insbesondere ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versuchen worden ist), zu einem Eingriff in das Fernmeldegeheimnis nach Artikel 10 Abs. 1 GG (vgl. nur BVerfGE 130, 151, 179, Rn. 112). Bei den übrigen auszuwertenden Daten handelt es sich zumindest um einen Eingriff in das Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG (das Fernmeldegeheimnis nach Artikel 10 Abs. 1 GG verdrängt in seinem Anwendungsbereich als speziellere Garantie das Recht auf informationelle Selbstbestimmung; vgl. nur BVerfGE 125, 260, 310, sowie die Erläuterung zu § 18 Abs. 1). Ob der Verhältnismäßigkeitsgrundsatz zur Rechtfertigung dieser Grundrechtseingriffe die vorherige Kontrolle der Maßnahme durch eine unabhängige Stelle, etwa in Form einer richterlichen Anordnung, verlangt (vgl. dazu allgemein BVerfGE 141, 220, 275, Rn. 117),

ergibt sich auch aus dem Eingriffsgewicht der Maßnahme (BVerfG, a. a. O., S. 267, Rn. 98 f.). Nach den Maßstäben des BVerfG bestimmt sich die Eingriffstiefe insbesondere durch die Art der erfassten Informationen, den Anlass und die Umstände der Datenerhebung, den betroffenen Personenkreis und die Art der möglichen Verwertung der Daten (vgl. nur BVerfGE 120, 378, 401 ff.):

- Zur Art der erfassten Informationen: Die Persönlichkeitsrelevanz der Auswertung von Telekommunikations-Verkehrsdaten wird vom BVerfG grundsätzlich als hoch eingeschätzt. Nach der Rechtsprechung des BVerfG lassen sich aus Verkehrsdaten - abhängig von dem jeweiligen Nutzungsverhalten - „tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen“; es könnten „bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse“ gezogen werden (BVerfGE 125, 260, 319, Rn. 211). Hierbei muss allerdings berücksichtigt werden, dass sich die vom BVerfG genannten Gefahren auf die vollständigen Telekommunikations-Verkehrsdaten aus sechs Monaten bezogen. Die Aussagekraft der im Zusammenhang mit einer technischen Regelverletzung (d. h. den zureichenden tatsächlichen Anhaltspunkten für eine Gefahr für die IT-Sicherheit im Sinne des Absatzes 1) gespeicherten Verkehrsdaten dürfte geringer sein, sodass auch die Persönlichkeitsrelevanz der Maßnahme als geringer einzuschätzen sein dürfte.

  Die Persönlichkeitsrelevanz der Maßnahme könnte dadurch weiter verringert sein, dass die auszuwertenden Verkehrsdaten überwiegend nicht durch eine private Nutzung der überwachten IT-Systeme entstehen, sondern durch deren dienstliche Nutzung. Daraus auf eine bloße Betroffenheit der „Sozialsphäre“ zu schließen, dürfte allerdings zu weit gehen. Die Begründung nennt z. B. den - bis in die Intimsphäre hineinreichenden - Austausch mit dem Personalrat oder der/dem Suchtbeauftragten (Drs. 18/1598, S. 79). Hinzu kommt, dass die in den Behörden beschäftigten und von den Maßnahmen betroffenen Personen die Überwachung der - erlaubten oder geduldeten - privaten Nutzung der behördlichen IT-Systeme zwar dadurch vermeiden könnten, dass sie ihre private Kommunikation vorzugsweise über private IT-Systeme abwickeln. Diese Ausweichmöglichkeit wurde in der Anhörung thematisiert (und deren Fehlen wurde vom BVerfG auch schon bei der Bewertung der Eingriffstiefe berücksichtigt; vgl. BVerfGE 125, 260, 319, Rn. 210). Sie besteht jedoch nicht für die Personen, die sich mit ihren Anliegen an die Behörden wenden (müssen) und deren politische und geschäftliche Kommunikation ebenfalls von Artikel 10 Abs. 1 GG geschützt ist (vgl. BVerfGE 100, 313, 358). Auch insofern sind verschiedene Konstellationen denkbar, in denen die betroffenen Daten nicht nur der „Sozialsphäre“ zuzurechnen sein dürften, sondern die Intimsphäre berühren können (z. B. bei der Kommunikation mit Jugendämtern oder Gesundheitsämtern). Die Persönlichkeitsrelevanz der erfassten Daten dürfte mithin trotz des (überwiegenden) dienstlichen Bezugs nicht als wesentlich verringert anzusehen sein.

- Zu den Bereichen Anlass und Umstände der Datenverarbeitung sowie betroffener Personenkreis wird in der Begründung des Gesetzentwurfs (a. a. O., S. 29) auf das komplexe Stufenmodell und die grundsätzlich automatisierte Datenverarbeitung verwiesen. Dass durch das Stufenmodell mit der automatisierten Auswertung auf der ersten und zweiten Stufe die Eingriffstiefe differenziert wird, führt allerdings nicht zwingend dazu, dass auch die Eingriffstiefe auf der dritten Stufe zwingend als so gering einzuschätzen ist, dass auf einen Richtervorbehalt verzichtet werden könnte. Bedeutsamer erscheint der Hinweis in der Begründung, dass die „Zielrichtung … der Maßnahme“ nicht zwingend einen Richtervorbehalt erfordere (a. a. O., S. 29). Zwar dürfte es den betroffenen Personen in erster Linie darauf ankommen, ob überhaupt durch die Verarbeitung ihrer (Verkehrs-)Daten in ihre Privatsphäre eingegriffen wird, und erst in zweiter Linie auf die damit verbundene Zielrichtung. Jedoch könnte die Persönlichkeitsrelevanz der Datenverarbeitung hier dadurch verringert sein, dass es bei der Maßnahme gerade nicht darum geht, Schlüsse auf das Verhalten von Betroffenen zu ziehen, die nach der Rechtsprechung des BVerfG die hohe Persönlichkeitsrelevanz kennzeichnen (vgl. BVerfGE 120, 378, 404). Durch § 18 Abs. 3 und § 19 Abs. 2 Satz 4 des Entwurfs bzw. § 27 Abs. 0/1 des Vorschlags wird ausdrücklich ausgeschlossen, Rückschlüsse auf das Verhalten betroffener Personen zu ziehen (z. B. im Hinblick auf ihre Arbeitsleistung bzw. ihre Arbeitszeiten). Es geht auch nicht darum, die gewonnenen Daten mit weiteren Informationen über die Betroffenen zu verknüpfen (vgl. dazu BVerfG, a. a. O.). Die Maßnahme ist allein darauf gerichtet, technische Vorgänge (d. h. Angriffe und Schadprogramme) ausfindig und unschädlich zu

machen. Diese Zielrichtung unterscheidet sich von der Verkehrsdaten-Auswertung zu strafprozessualen, gefahrenabwehrrechtlichen und nachrichtendienstlichen Zwecken, bei der es in allen genannten Bereichen gerade darum geht, aus den Daten Rückschlüsse auf das Verhalten der Betroffenen zu ziehen. Das Eingriffsgewicht der hier geregelten Maßnahmen dürfte daher geringer sein als bei den genannten verhaltensbezogenen Maßnahmen.

Auf das Eingriffsgewicht dürfte sich zudem der Umstand verringernd auswirken, dass die mit der Maßnahme verbundenen Grundrechtseingriffe zum Schutz derselben Grundrechte derselben Personen (Fernmeldegeheimnis und Recht auf informationelle Selbstbestimmung) vorgenommen werden. Die von den Grundrechtseingriffen betroffenen Personen partizipieren grundsätzlich in demselben Verhältnis an der Schutzwirkung der ergriffenen Maßnahmen (d. h. der Abwehr von Angriffen und Schadprogrammen, die zu einem Datenabfluss aus den kompromittierten IT-Systemen führen können), wie sie durch ihre Grundrechtsbetroffenheit dazu beitragen. Anders gewendet: Je mehr die betroffenen Personen IT-Systeme zur Telekommunikation nutzen, desto stärker wird zwar in ihre Grundrechte eingegriffen, desto stärker profitieren sie jedoch auch von dem mit den Eingriffen bewirkten Schutz ihrer Grundrechte.

Nach der Rechtsprechung des BVerfG sind anlasslose Maßnahmen, d. h. Maßnahmen gegenüber Personen, die den Grundrechtseingriff durch ihr Verhalten nicht veranlasst haben, grundsätzlich von höherer Eingriffstiefe als anlassbezogene Maßnahmen (ständige Rspr., vgl. BVerfGE 120, 378, 402; 125, 260, 317, Rn. 206; 130, 151, 187, Rn. 133; zuletzt Beschl. v. 18.12.2018 - 1 BvR 142/15 -, NJW 2019, 827, 834, Rn. 98). Allerdings ist eine vorsorgliche anlasslose Datenverarbeitung nicht allein schon deswegen ein besonders schwerer Eingriff (BVerfGE 130, 151, 189, Rn. 138) oder generell ausgeschlossen (BVerfG NJW 2019, 827, 834, Rn. 94). Hier muss nach dem Stufenmodell der Maßnahmen differenziert werden: Vollständig anlasslos sind lediglich die Maßnahmen auf der ersten Stufe (vgl. § 19 Abs. 1 und 1/1 der Empfehlung). Bereits auf der zweiten Stufe werden zureichende tatsächliche Anhaltspunkte für eine Gefahr für die IT-Sicherheit verlangt (vgl. Absatz 1), auf der dritten Stufe (nicht automatisierte Auswertung) sogar hinreichende tatsächliche Anhaltspunkte. Anlasslos sind allerdings auch die Maßnahmen der zweiten und dritten Stufe insoweit, als sie sich nicht gegen konkret „verdächtige“ Betroffene richten (z. B. Störerinnen/Störer im Sinne des Gefahrenabwehrrechts). Die erhobenen und ausgewerteten Daten können also einer großen Zahl von Betroffenen zuzuordnen sein, die zu der Maßnahme selbst keinen Anlass gegeben haben. Die Maßnahmen können mithin jede und jeden treffen, die oder der mittels der überwachten IT-Systeme kommuniziert. In solchen Fällen sieht das BVerfG wegen der Streubreite der Maßnahme die Gefahr von allgemeinen Einschüchterungseffekten, die zu Beeinträchtigungen bei der Grundrechtsausübung führen können (vgl. BVerfGE 120, 378, 402; 125, 260, 320, Rn. 212; zuletzt Beschl. v. 18.12.2018 - 1 BvR 142/15 -, NJW 2019, 827, 834, Rn. 98). Durch diese Streubreite wird die Eingriffstiefe erhöht.

Erhöht ist die Eingriffstiefe nach der Rechtsprechung des BVerfG auch dann, wenn es sich um eine heimliche Maßnahme handelt, weil dadurch ein Gefühl des Überwachtwerdens entstehen kann (ständige Rspr., vgl. nur BVerfGE 120, 378, 402 f.; 141, 220, 264 f., Rn. 91 f.; zuletzt Beschl. v. 18.12.2018 - 1 BvR 142/15 -, NJW 2019, 827, 834, Rn. 98). Die hier geregelte Maßnahme wird zwar nicht offen durchgeführt. Ob dadurch die Eingriffstiefe erhöht wird, unterliegt jedoch Zweifeln. Zunächst fehlt es hier wohl schon an dem typischen Kennzeichen der heimlichen Informationsbeschaffung, dass die Behörde die ermittelten Informationen bei offener Ermittlung nicht erhielte oder dass die offene Vorgehensweise die Ermittlung wegen drohender Abschottung oder Flucht insgesamt erschwerte oder unmöglich machte (vgl. *Rachor*, in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, E Rn. 249). Hinzu tritt der Umstand, dass die Zielrichtung der hier geregelten Maßnahme nicht auf eine Verhaltenskontrolle der (zufällig) betroffenen Personen gerichtet ist (siehe oben), deren Grundrechte zudem durch die eingesetzte Maßnahme geschützt werden sollen (siehe oben). Ob in einer solchen Konstellation das BVerfG in demselben Umfang von der möglichen Entstehung eines Gefühls des Überwachtwerdens ausginge wie bei den typischen heimlichen Überwachungsmaßnahmen, steht daher aus Sicht des Ausschusses nicht fest.

- Zur Art der möglichen Verwertung der Daten verweist die Begründung des Gesetzentwurfs (a. a. O., S. 29) auf die strenge Zweckbindung und den verfolgten Grundsatz der Datenminimierung (auf jeder Stufe werden die nicht mehr erforderlichen Daten unverzüglich gelöscht; vgl. 19 Abs. 2 [erste Stufe], § 21 Abs. 1 Satz 3 [zweite Stufe] und Abs. 3 [dritte Stufe]). Für die Bewertung der Persönlichkeitsrelevanz kommt es allerdings darauf an, wie „streng“ die Zweckbindung des § 18 Abs. 3 des Entwurfs bzw. § 27 Abs. 0/1 der Empfehlung ausgestaltet ist (vgl. dazu die dortigen Erläuterungen), und insbesondere, in welchem Umfang Zweckänderungen bzw. Übermittlungen nach § 27 zugelassen werden, durch die den betroffenen Personen nachteilige Folgeeingriffe drohen (vgl. BVerfGE 120, 378, 403). Der Gesetzentwurf sieht zwar in § 27 Abs. 1 die zweckändernde Übermittlung sowohl an Strafverfolgungsbehörden als auch an Gefahrenabwehr- und Verfassungsschutzbehörden vor. Allerdings ist hier zu berücksichtigen, dass die Zielrichtung der Maßnahme nicht unmittelbar auf die Ermittlung von Sachverhalten gerichtet ist, die in den Zuständigkeitsbereich der genannten Behörden fallen, entsprechende Erkenntnisse also nur zufällig entstehen (siehe oben). Hinzu kommt, dass die Übermittlungen durch einen Richtervorbehalt bzw. die diesem entsprechende Beteiligung der G 10-Kommission abgesichert sind. Bei den Übermittlungsvorschriften wird zudem der Grundsatz der hypothetischen Datenneuerhebung eingehalten (vgl. die Empfehlungen zu § 27 Abs. 1). Zweckändernde Nutzungen für dienstrechtliche Maßnahmen, z. B. Disziplinarverfahren, sind ausgeschlossen (zu diesem Zweck sieht § 27 keine Übermittlung vor; die missverständliche Verweisung in § 25 Satz 2 Nr. 1 des Entwurfs soll gestrichen werden). Bei der in § 27 Abs. 2 geregelten Übermittlung an andere Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, geht es nach Mitteilung des MI insbesondere um sogenannte Indicator of Compromise (IoC)-Listen (diese enthalten IP-Adressen, URL und andere technische Informationen) sowie um einzelne IP-Pakete, Byte-Muster usw. Das MI ist der Auffassung, dass die Persönlichkeitsrelevanz dieser Daten gering sei; insbesondere drohten den betroffenen Personen keine durch die Übermittlung veranlassten Folgeeingriffe.

Der Ausschuss ist vor dem Hintergrund der dargelegten Eingriffstiefe der Auffassung des MI gefolgt, dass die mit der Maßnahme verbundenen Grundrechtseingriffe auch ohne einen Richtervorbehalt, wie er bei anderen Regelungen über den Zugriff auf Telekommunikations-Verkehrsdaten vorgesehen ist (vgl. § 100 g i. V. m. § 101 a StPO, § 33 c NPOG und § 20 i. V. m. § 21 des Niedersächsischen Verfassungsschutzgesetzes [NVerfSchG]), verfassungsrechtlich gerechtfertigt werden können, zumal vergleichbare Eingriffsregelungen (z. B. in § 5 BSIG und Artikel 16 BayEGovG) ebenfalls keinen Richtervorbehalt enthalten. Der GBD hat insoweit darauf hingewiesen, dass im Ergebnis zwar in Ermangelung verfassungsgerichtlicher Judikatur zu den hier geregelten speziellen Grundrechtseingriffen ein verfassungsrechtliches Risiko verbleibe, das durch die Einführung eines Richtervorbehalts vermieden werden könne. Angesichts der dargelegten Eingriffstiefe, des im Gesetzentwurf vorgesehenen Behördenleitervorbehalts (der verstärkt wird durch das notwendige Einvernehmen mit einer Juristin/einem Juristen) und des sowohl für zweckändernde Übermittlungen als auch für Nicht-Benachrichtigungen vorgesehenen Richtervorbehalts erscheine dieses Risiko jedoch als überschaubar.

Zu Absatz 2/1:

Für die weitere automatisierte Auswertung nach den Absätzen 1 und 2 soll hier - entsprechend der Überschrift - ausdrücklich klargestellt werden, dass nach § 21 keine Telekommunikations-Inhaltsdaten gespeichert oder ausgewertet werden dürfen (vgl. dazu bereits die Erläuterung zu § 19 Abs. 1/2). Das MI hat zur Ausführbarkeit dieser Regelung mitgeteilt, dass bei der Anwendung der Vorschrift im Einzelfall den Anwenderinnen/Anwendern jeweils bewusst sei, ob sie Inhaltsdaten verarbeiteten oder nicht. Als Beispiel für in den Absätzen 1 und 1/1 enthaltene Inhaltsdaten nennt das MI die URL, die - z. B. bei einer Suchanfrage im Internet - auch Inhaltsdaten enthalten könne. Auch die nach Absatz 1 auszuwertenden Log-Dateien könnten Inhaltsdaten aufweisen (z. B. bei Netzwerkkomponenten und E-Mail-Relais); dies sei aber jeweils anhand der Datenstruktur der Log-Dateien erkennbar.

Zu Absatz 3:

Der Ausschuss empfiehlt, in der Löschungsregelung klarzustellen, dass sie sich auf sämtliche Daten bezieht, die nach Absatz 2 ausgewertet wurden, d. h. auch auf die nach § 19 der Empfehlung erhobenen Daten. Zudem soll die Erforderlichkeit auf die in Absatz 2 genannten Zwecke bezogen werden (dieser Zweck kann auch in der Erkennung und Abwehr einer anderen Gefahr für die IT-Sicherheit nach Absatz 2 Satz 6 der Empfehlung liegen). Aufgenommen werden soll auch die Möglichkeit einer Übermittlung nach § 27, die einer Löschung entgegenstehen kann. Nach Mitteilung des MI werden nur solche Daten nach § 27 übermittelt, die auf der in Absatz 2 geregelten dritten Stufe ausgewertet worden sind, sodass eine entsprechende Ausnahme von der Löschungspflicht nur hier (sowie in § 22 Abs. 4) erforderlich ist (vgl. dazu auch die Empfehlung zu § 27 Abs. 2 Satz 1).

Zu § 22 (Weitere Auswertung von Inhaltsdaten in Verdachtsfällen):

Zu Absatz 1:

Da die in Absatz 1 Satz 1 des Entwurfs geregelte erste Stufe der Auswertung von Inhaltsdaten nach der Empfehlung des Ausschusses von § 19 Abs. 1 und 1/1 erfasst wird (vgl. auch die Empfehlung zu § 19 Abs. 1/2) und die Löschungsregelung in Satz 2 des Entwurfs § 19 Abs. 2 entspricht, ist Absatz 1 des Entwurfs insgesamt entbehrlich und soll gestrichen werden (zumal die hier enthaltene Beschränkung auf Gefahren für die IT-Sicherheit „des Landes“ nach Mitteilung des MI auf einem redaktionellen Versehen beruht). Dass § 22 demnach (nur noch) die zweite und dritte Stufe der Auswertung von Inhaltsdaten regelt, soll in der Überschrift deutlich werden (vgl. die entsprechende Empfehlung zu der Überschrift von § 21).

Zu Absatz 2:

Absatz 2 enthält die Regelungen zu der zweiten Stufe der Auswertung von Telekommunikations-Inhaltsdaten. Die Empfehlung zu Satz 1 soll klarstellen, dass sich die Eingriffsschwelle dadurch von derjenigen in § 21 Abs. 1 Satz 1 unterscheidet, dass sich aus der Auswertung auf der ersten Stufe zureichende Anhaltspunkte dafür ergeben haben müssen, dass die weitere Auswertung der Inhaltsdaten zur Erkennung und Abwehr der Gefahr erforderlich ist. Auf Vorschlag des MI sollen auch hier die durch eine Sicherheitslücke verursachten Gefahren für die IT-Sicherheit aufgenommen werden (vgl. die Empfehlungen zu § 21 Abs. 2 Sätze 1 und 6). Die Empfehlung, auch hier (wie in § 21 Abs. 1 Satz 1 für die Verkehrsdatenauswertung) die Speicherfrist auf der zweiten Stufe von 7 auf 30 Tage zu verlängern, beruht auf dem Änderungsvorschlag der Fraktionen von SPD und CDU. Der GBD hatte auch hier insoweit keine durchgreifenden rechtlichen Bedenken (vgl. die Erläuterung zu § 21 Abs. 1 Satz 1).

Der Ausschuss empfiehlt, das Verbot der Auswertung der kommunikativen Bedeutung der Inhaltsdaten auch hier in dem empfohlenen Halbsatz 2 hervorzuheben (vgl. die Empfehlungen zu Absatz 3 Satz 1 Halbsatz 2 sowie zu § 19 Abs. 1/2).

Satz 2 soll redaktionell berichtigt und an § 21 Abs. 1 Satz 2 angeglichen werden. Der Regelungsgehalt von Satz 3 des Entwurfs soll in Satz 1 aufgenommen werden, sodass Satz 3 gestrichen werden kann.

Die Empfehlungen zu den Regelungen über den Behördenleitervorbehalt (Sätze 4 bis 6) entsprechen denen zu § 21 Abs. 2 Sätze 3 bis 5 des Entwurfs. Anders als dort geht es hier allerdings nicht um eine (vorherige) Anordnung, sondern um eine (nachträgliche) Genehmigung. Nach Mitteilung des MI ist hier technisch keine Anordnung möglich, weil die flüchtigen Daten entweder sofort automatisiert gespeichert werden oder unwiederbringlich verloren sind. In der Praxis ähnele das Verfahren trotzdem einer vorherigen Anordnung, weil mit der Behördenleitung und der Juristin/dem Juristen ein Fallkatalog vereinbart werde, der dann zu einer automatischen Speicherung (und einer anschließenden Genehmigung) führe.

Der Ausschuss empfiehlt, in einem neuen Satz 7 ausdrücklich zu regeln, dass die Inhaltsdaten sowie die darauf bezogenen Auswertungsergebnisse unverzüglich zu löschen sind, wenn die Genehmigung abgelehnt oder nicht unverzüglich erteilt wird.

In einem neuen Satz 8 soll zudem eine - § 21 Abs. 1 Satz 3 der Empfehlung entsprechende - Löschungsregelung aufgenommen werden.

Zu Absatz 3:

Absatz 3 enthält die Regelungen zu der dritten Stufe der Auswertung von Telekommunikationsinhaltsdaten. Der Ausschuss empfiehlt, die Eingriffsschwelle in Satz 1 - ohne inhaltliche Änderung - an die Empfehlungen zu Absatz 2 Satz 1 (zweite Stufe) und § 21 Abs. 2 (dritte Stufe der Verkehrsdatenauswertung) anzupassen (vgl. zu der im Wortlaut ergänzten Möglichkeit der Sprungeskalation von der ersten zur dritten Stufe die Erläuterung zu § 21 Abs. 2 Satz 1). Nach Mitteilung des MI ist mit der „direkt personenbezogenen Auswertung“ dasselbe gemeint wie mit der nicht automatisierten entpseudonymisierten Auswertung nach § 21 Abs. 2 Satz 1. Daher soll hier dieselbe Formulierung gewählt werden. Auf Vorschlag des MI sollen auch hier die durch Sicherheitslücken verursachten Gefahren für die IT-Sicherheit aufgenommen werden (vgl. die Empfehlungen zu Absatz 2 Satz 1 sowie zu § 21 Abs. 2 Sätze 1 und 6). Das Verbot der Auswertung der kommunikativen Bedeutung der Inhaltsdaten soll auch hier in dem empfohlenen Halbsatz 2 hervorgehoben werden (vgl. die Empfehlungen zu Absatz 2 Satz 1 Halbsatz 2 sowie zu § 19 Abs. 1/2).

Satz 2 des Entwurfs verbindet wie § 21 Abs. 2 Satz 2 des Entwurfs zwei unterschiedliche Regelungsgehalte. Die Regelung soll daher teilweise in die Eingriffsschwelle in Satz 1 integriert, teilweise in den neuen Satz 6 ausgegliedert und sodann gestrichen werden (vgl. die Erläuterung zu § 21 Abs. 2 Satz 2 des Entwurfs).

Die Empfehlungen zu dem Behördenleitervorbehalt (Sätze 3 bis 5 des Entwurfs) entsprechen denen zu § 21 Abs. 2 Sätze 3 bis 5 sowie zu Absatz 2 Sätze 4 bis 6 des Entwurfs. Der Ausschuss hat bei seiner Empfehlung in Rechnung gestellt, dass das verfassungsrechtliche Risiko des Verzichts auf den Richtervorbehalt hier größer sein könnte als bei der manuellen Auswertung von Verkehrs- und sonstigen Daten nach § 21 Abs. 2, weil die Persönlichkeitsrelevanz von Telekommunikations-Inhaltsdaten in der Tendenz größer sein dürfte als die von Telekommunikations-Verkehrsdaten. Für das in der Erläuterung zu § 21 Abs. 2 dargelegte Beispiel der (dienstlichen) Kommunikation mit dem Personalrat oder der/dem Suchtbeauftragten liegt es auf der Hand, dass die Persönlichkeitsrelevanz der Information, ob und wann eine Telekommunikation mit diesen Personen stattgefunden hat, von der Persönlichkeitsrelevanz der konkreten Inhalte dieser Kommunikation deutlich übertroffen werden kann. Dieser gesteigerten Eingriffstiefe wird allerdings zum einen schon dadurch begegnet, dass eine gezielte Suche nach Inhalten, aus denen sich z. B. Straftaten ergeben, ausgeschlossen ist (vgl. die Empfehlung zu Satz 1 Halbsatz 2), sodass allenfalls Zufallsfunde an den Kommunikationsinhalt anknüpfende nachteilige Folgen auslösen können. Zum anderen dürfen zufällig entdeckte Daten von besonderer Persönlichkeitsrelevanz (Kernbereich privater Lebensgestaltung, besondere Kategorien personenbezogener Daten i. S. d. DSGVO und Daten, die geeignet sind, die betroffene Person in ihrer beruflichen und persönlichen Stellung zu beeinträchtigen) nach Absatz 5 nicht genutzt oder übermittelt werden; sie sind unverzüglich zu löschen. Die Inhaltsdaten dürfen auch nicht für dienstrechtliche Maßnahmen verwendet werden (z. B. Disziplinarverfahren; vgl. dazu die Empfehlung zu § 25 Satz 2 Nr. 1 des Entwurfs). Da die Eingriffstiefe daher im Ergebnis jedenfalls geringer sein dürfte als bei den klassischen „Abhör-Maßnahmen“ (strafprozessuale, gefahrenabwehrrechtliche oder nachrichtendienstliche Telekommunikationsüberwachung nach § 100 a StPO, § 33 a NPOG oder § 1 Abs. 1 Nr. 1 des Artikel 10-Gesetzes [G 10]), hat auch der GBD das mit dem Verzicht auf den Richtervorbehalt verbundene verfassungsrechtliche Risiko als überschaubar eingeschätzt (vgl. im Übrigen die Erläuterungen zu § 21 Abs. 2).

Zu dem empfohlenen Satz 6 vgl. die Erläuterung zu Satz 2 des Entwurfs sowie zu dem empfohlenen § 21 Abs. 2 Satz 6.

Zu Absatz 4:

Der Ausschuss empfiehlt, die Löschungsregelung redaktionell auf § 21 Abs. 3 abzustimmen (vgl. auch die Erläuterung dort).

Zu Absatz 5:

Der Ausschuss hat bei seiner Empfehlung berücksichtigt, dass der Gesetzgeber nur dort verpflichtet ist, Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung zu schaffen, wo Überwachungsmaßnahmen typischerweise zur Erhebung kernbereichsrelevanter Daten führen können (ständige Rspr., vgl. nur BVerfGE 141, 220, 277, Rn. 123). Er hat sich insoweit der Auffassung des MI angeschlossen, das davon ausgeht, dass ausschließlich bei der manuellen Verarbeitung von Inhaltsdaten eine Kernbereichsrelevanz infrage kommt. Da die Auswertung der kommunikativen Bedeutung der Inhaltsdaten verboten werden soll (vgl. die Empfehlungen zu Absatz 2 Satz 1 Halbsatz 2 und Absatz 3 Satz 1 Halbsatz 2), kann von kernbereichsrelevanten Inhalten sowie von Daten, die geeignet sind, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen, nur zufällig Kenntnis genommen werden. Dies ist allerdings nicht vollständig auszuschließen.

Satz 1 des Entwurfs soll gestrichen werden, denn das MI hat dazu mitgeteilt, dass kernbereichsrelevante Daten bei der automatisierten Erhebung und Auswertung technisch nicht ausgesondert werden können. Die Entwurfsregelung wäre daher nicht ausführbar.

Die Empfehlung zu Satz 2 regelt die oben dargelegte, nach Mitteilung des MI einzig vorstellbare Konstellation, in der Kernbereichsdaten bei einer Auswertung nach Absatz 3 entdeckt werden. Bei den Daten aus besonderen Kategorien personenbezogener Daten, die nach dem Entwurf den Kernbereichsdaten gleichgestellt werden, soll durch den empfohlenen Klammerzusatz die Verweisung auf Artikel 9 DSGVO aufgenommen werden. Dadurch wird die Begriffsbestimmung in § 1 Abs. 1 Nr. 4 des Entwurfs entbehrlich. Da nach Mitteilung des MI die Daten, die geeignet sind, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen, die nach den Sätzen 1 und 3 des Entwurfs den Kernbereichsdaten gleichgestellt werden sollen, in Satz 2 des Entwurfs aufgrund eines redaktionellen Versehens fehlen, sollen sie hier aufgenommen werden. Zudem soll in Satz 2 das in den Satz 2 des Entwurfs enthaltene Verbot, die genannten Daten zu speichern, zu verändern, zu nutzen oder zu übermitteln, und die in Satz 3 des Entwurfs enthaltene Verpflichtung, diese Daten unverzüglich zu löschen, redaktionell an § 33 Abs. 5 Satz 1 NPOG angeglichen werden. Satz 3 des Entwurfs soll infolgedessen gestrichen werden.

Die Empfehlung zu Satz 4 enthält lediglich eine redaktionelle Anpassung der Satzeinleitung.

Die Empfehlungen zu den Sätzen 5 bis 7 sind an § 33 Abs. 5 Sätze 2 bis 4 NPOG angelehnt (allerdings ohne Bezugnahme auf das in § 25 des Entwurfs nicht geregelte endgültige Absehen von der Benachrichtigung; vgl. § 30 Abs. 7 NPOG). Die von dort übernommene längere Aufbewahrung der Dokumentation trägt dem Umstand Rechnung, dass Löschungsvorschriften, wie sie der Gesetzentwurf vorsieht, vom BVerfG in der BKAG-Entscheidung für verfassungswidrig erklärt worden sind (vgl. BVerfGE 141, 220, 323, Rn. 272 f.).

Zu § 22/1 (Ergänzende Auswertung durch das Bundesamt für Sicherheit in der Informationstechnik):

Die Empfehlung, eine Regelung über die ergänzende Auswertung von Daten durch das BSI aufzunehmen, beruht auf einem Änderungsvorschlag der Fraktionen von SPD und CDU, der wie folgt begründet wurde:

> *„Der Gesetzentwurf soll um eine Öffnungsklausel ergänzt werden, die es ermöglicht, die spezielle Technik zur Erkennung von Schadsoftware (sog. Schadprogramm-Erkennungs-System, kurz SES) sowie die langjährige Expertise des BSI bei der Auswertung des Netzwerkverkehrs zu nutzen. Eine Übertragung von Hoheiten auf das BSI ist derzeit mangels verfassungsrechtlicher Grundlage nicht möglich. Daher kann die Auswertung der Daten aus dem Landesdatennetz durch das BSI lediglich im Rahmen einer Auftragsdatenverarbeitung erfolgen. Im Rahmen der Beauftragung des BSI sind die Bestimmungen zur Auftragsdatenverarbeitung gemäß Art. 28 DS-GVO zu beachten. Bei der Nutzung der Technik des BSI werden spezielle SES-Sensoren an Schnittstellen des Landesdatennetzes innerhalb des Landes Niedersachsen angebracht. Die SES-Sensoren werden vom BSI mit speziellen Signaturen zur Erkennung von Schadsoftware ausgestattet und regelmäßig aktualisiert. Die Auswertung der Daten im*

SES-Sensor erfolgt vollkommen automatisch. Nur soweit der SES-Sensor mindestens hinreichende Anhaltspunkte für eine Schadsoftware gefunden hat, werden die für die weitere Auswertung erforderlichen Daten automatisiert an das BSI zur weiteren einzelfallbezogenen Analyse weitergeleitet. Durch die ausschließlich signaturbasierte Auswertung der Daten ist es möglich, das in den §§ 21 ff. vorgegebene Eskalationsmodell auch bei Nutzung der speziellen Technik des BSI zu wahren. Hierzu sind von der Leitung der beauftragenden Behörde sowie einer oder einem Beschäftigten mit Befähigung zum Richteramt im Vorfeld der Auswertung Fallgruppen für die Ausleitung mit dem BSI fortlaufend abzustimmen.

Im Übrigen empfiehlt es sich generell im Rahmen der Auswertung der Daten mit Fallgruppen zu arbeiten, bei denen im Vorfeld die zureichenden und hinreichenden Anhaltspunkte für eine Gefahr für die IT-Sicherheit definiert sind und bei deren Eintreten eine Freigabe gemäß der §§ 21 bzw. 22 erforderlich ist."

Der Ausschuss hat sich mit den - in der Begründung des Änderungsvorschlages angedeuteten - verfassungsrechtlichen Grenzen für die beabsichtigte Beauftragung einer Bundesbehörde befasst. Nach der Rechtsprechung des BVerfG sind die Verwaltung des Bundes und die Verwaltung der Länder als in sich geschlossene Einheiten prinzipiell voneinander getrennt. Die Verwaltungszuständigkeiten sind in den Artikeln 83 ff. GG abschließend geregelt und nicht abdingbar. Bund und Länder können also auch im Einvernehmen (z. B. durch korrespondierende einfache Gesetze) nicht davon abweichen. Daraus ergibt sich das Verbot einer sogenannten Mischverwaltung (sofern diese nicht im Grundgesetz selbst vorgesehen ist; vgl. z. B. Artikel 91 c Abs. 1 GG, der Bund und Länder ermächtigt, bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenzuwirken, über dessen Reichweite allerdings keine Klarheit besteht; vgl. nur *Jarass/Pieroth*, GG, 13. Aufl. 2014, Art. 91c Rn. 2 ff.; *Schliesky*, in: Bonner Kommentar zum GG, Art. 91 c Rn. 24 ff.). Die klare Zuordnung von Verwaltungszuständigkeiten ist insbesondere im Hinblick auf das Demokratieprinzip erforderlich; die Bürgerinnen und Bürger müssen wissen, wen sie wofür verantwortlich machen können (vgl. zum Ganzen BVerfGE 119, 331, 364 ff.). Der Verwaltungsträger, dem durch das Grundgesetz Verwaltungsaufgaben zugewiesen worden sind (hier das Land, das für die Ausführung von Landesgesetzen zuständig ist), hat diese Aufgaben grundsätzlich durch eigene Verwaltungseinrichtungen, also mit eigenem Personal, eigenen Sachmitteln und eigener Organisation wahrzunehmen. Von diesem Grundsatz der eigenverantwortlichen Aufgabenwahrnehmung darf nur in engen Grenzen abgewichen werden: Die Zusammenarbeit muss sich auf eine eng begrenzte Verwaltungsmaterie beziehen und ein sachlicher Grund muss die gemeinsame Aufgabenwahrnehmung rechtfertigen (BVerfGE 119, 331, 367). Zudem muss die Letztverantwortung des zuständigen Verwaltungsträgers für die Aufgabenwahrnehmung gewahrt bleiben (a. a. O., S. 366; vgl. auch *Dittmann/Winkler*, in: Sachs, GG, 8. Aufl. 2018, Art. 83 Rn. 4). In der Literatur werden allerdings vereinzelt - abweichend vom BVerfG - nur ausdrücklich im GG verankerte Ausnahmen für zulässig gehalten (so *Groß*, in: Friauf/Höfling, Berliner Kommentar zum GG, Art. 83 Rn. 31 f.).

Die Kooperation soll hier auf eine ergänzende Auswertung der dem BSI übermittelten Daten und mithin auf eine eng begrenzte Verwaltungsmaterie beschränkt werden, insbesondere wenn die BSI-Sensorik auf den Datenverkehr angewendet wird, bei dem die auf Grundlage der §§ 18/1 ff. eingesetzten IDS/SIEM-Systeme keine zureichenden oder hinreichenden tatsächlichen Anhaltspunkte für das Vorliegen einer Gefahr für die IT-Sicherheit festgestellt haben. Für die Einbindung des BSI liegt nach Auffassung des Ausschusses auch ein sachlicher Grund vor. Das MI hat bestätigt, dass das BSI über Techniken und Analysefähigkeiten verfüge, die die Möglichkeiten und Fähigkeiten der zuständigen Landesbehörden bei der Ermittlung von Gefahren für die IT-Sicherheit überstiegen. Der Einsatz dieser zusätzlichen Techniken und Analysefähigkeiten sei erforderlich, um gegenwärtigen und zukünftigen Bedrohungslagen für die IT-Sicherheit wirkungsvoll zu begegnen, zumal die abzuwehrenden Cyberangriffe ausgefeilter würden und zunehmend schwerer zu detektieren seien. Nach Satz 3 des Änderungsvorschlages sollen die Daten „unter der Hoheit der beauftragenden Behörde" ausgewertet werden. In der Begründung wird dazu ergänzt, dass die „Übertragung von Hoheiten auf das BSI" aus verfassungsrechtlichen Gründen nicht beabsichtigt sei. Daraus wird ersichtlich, dass die Letztverantwortung für die Aufgabenerfüllung bei der beauftragenden Behörde verbleiben soll. Der Ausschuss empfiehlt allerdings, die Letztverantwortung der beauftragenden Behörde im Wortlaut der Vorschrift noch stärker hervorzuheben, um verfassungsrechtliche Risiken zu

vermeiden (vgl. zur Bedeutung der rechtsstaatlichen Grundsätze der Normklarheit und Widerspruchsfreiheit bei der Bestimmung von Verwaltungszuständigkeiten BVerfGE 119, 331, 366 m. w. N.). Insbesondere soll in Satz 2 Nr. 1 klargestellt werden, dass die bei der ergänzenden Auswertung nach Maßgabe der §§ 21 und 22 erforderlichen Anordnungen und Genehmigungen von der beauftragenden Behörde getroffen bzw. erteilt werden müssen. Dadurch soll sichergestellt werden, dass die Letztverantwortung für die weiteren Eskalationsstufen bei der beauftragenden Behörde verbleibt. Zudem soll in Satz 3 verdeutlicht werden, dass ein Weisungsrecht der beauftragenden Behörde gegenüber dem BSI besteht, das ebenfalls die Letztverantwortung der beauftragenden Behörde absichert. Auch der GBD hielt angesichts der Rechtsprechung des BVerfG, deren Maßstäbe hier eingehalten worden sein dürften, das mit der Regelung verbundene verfassungsrechtliche Risiko für überschaubar (auch wenn das BVerfG bisher nicht ausdrücklich über die Ausführung von Landesrecht durch Bundesbehörden entschieden hat).

Der GBD hat allerdings darauf hingewiesen, dass nicht sicher sei, ob das BSI die hier geregelten Aufträge annehmen dürfe oder ob es dafür eine korrespondierende (Bundes-)Regelung benötige. Möglicherweise könne die Zusammenarbeit auf die Aufgabenzuweisung in § 3 Abs. 1 Satz 2 Nr. 13a BSIG (Unterstützung der zuständigen Stellen der Länder auf deren Ersuchen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik) gestützt werden, die im Jahr 2017 eingefügt wurde, um es dem BSI zu ermöglichen, den Landesbehörden technische Expertise bei der Bewältigung ihrer (landes-)gesetzlichen Aufgaben zur Verfügung zu stellen (vgl. BT-Drs. 18/11242, S. 37; *Buchberger*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, Rn. 12 zu § 3 BSIG: „spezialgesetzlich geregelter Fall der Amtshilfe“). Ob es ergänzender Befugnisnormen auf Seiten des Bundes bedürfe, müsste allerdings dort geprüft und entschieden werden.

Die Empfehlungen des Ausschusses werden im Einzelnen wie folgt begründet:

In der Überschrift soll das BSI ausgeschrieben werden (die Abkürzung wird erst in Satz 1 eingeführt).

In Satz 1 soll klargestellt werden, dass die ergänzende Auswertung nur bei Behörden infrage kommen soll, die selbst IT-Systeme nach dem Zweiten Abschnitt (IDS/SIEM-Systeme) betreiben (siehe oben). Zudem soll klargestellt werden, dass es sich laut MI bei der für die Umsetzung des Änderungsvorschlages beabsichtigten technischen Konstruktion (die niedersächsische Behörde leitet die von ihr erhobenen Daten an die sog. SES-Sensoren aus) um eine Übermittlung handelt. Diese Übermittlung kann sich laut MI aufgrund der technischen Einrichtungen beim BSI allein auf den Datenverkehr nach § 19 Abs. 1/1 beziehen, nicht hingegen auf die Ereignisdokumentationen (§ 19 Abs. 1). Nach Mitteilung des MI sei es technisch möglich, die Ausleitung an das BSI auf den Datenverkehr zu beschränken, der bei der automatisierten Auswertung mittels der Sensorik in Niedersachsen nicht auffällig war, also keine Eskalation ausgelöst hat. Daher empfiehlt der Ausschuss, die Vorschrift entsprechend zu begrenzen, weil die Ausleitung der Trefferfälle nicht erforderlich ist (siehe oben).

Der Ausschuss empfiehlt, den Regelungsgehalt von Satz 2 zu verdeutlichen, insbesondere im Hinblick auf die Einhaltung des verfassungsrechtlichen Rahmens (siehe oben). Mit den Worten „dafür Sorge zu tragen“ ist gemeint, dass die Behörde das BSI nur dann beauftragen darf, wenn es die Einhaltung der in den Nummern 1 bis 5 enthaltenen Maßgaben vertraglich zusichert; dies soll aus der Satzeinleitung deutlich werden.

Aus Satz 2 Nr. 1 soll nicht nur hervorgehen, dass die ergänzende Auswertung durch das BSI nach Maßgabe der §§ 21 und 22 mit dem dort differenziert geregelten Eskalationsmodell erfolgen muss. Zur Einhaltung der verfassungsrechtlichen Grenzen (siehe oben) soll ausdrücklich geregelt werden, dass bei Eskalationsschritten, die einer besonderen Anordnung oder Genehmigung bedürfen (vgl. § 21 Abs. 2 Satz 3, § 22 Abs. 2 Satz 4 und Abs. 3 Satz 3), die Behördenleitung der beauftragenden Behörde zu entscheiden hat.

Satz 2 Nr. 2 soll redaktionell verbessert werden.

Satz 2 Nr. 3 soll vereinfacht werden. Nach Mitteilung des MI ist beabsichtigt, dass das BSI lediglich sog. sanitarisierte Daten weiter verwenden darf. Diese enthalten keine personenbezogenen Daten, daher begründet ihre Verwendung keinen (weiteren) Grundrechtseingriff (aus diesem Grund wer-

den in § 27 auch keine Übermittlungen an das BSI geregelt). Es bedarf hier somit nur der Regelung, dass eine weitere Verwendung von personenbezogenen Daten unzulässig ist.

Satz 2 Nr. 4 soll neben der Löschung auch die Einhaltung der in § 23 geregelten Anforderungen an die Datensicherheit und Protokollierung aufnehmen. Nach Einschätzung des MI war dies mit der „ordnungsgemäßen“ Verarbeitung nach Nummer 5 gemeint. Dass § 23 für die ergänzende Auswertung gilt, soll hier (sowie in § 23) verdeutlicht werden.

Zu Satz 2 Nr. 5 empfiehlt der Ausschuss lediglich redaktionelle Verbesserungen.

Aus Satz 3 soll deutlicher hervorgehen, dass hier die Verantwortung im Sinne der Aufgabenwahrnehmung gemeint ist. Zur Einhaltung der verfassungsrechtlichen Maßstäbe (siehe oben) soll hier verdeutlicht werden, dass damit ein Weisungsrecht der beauftragenden Behörde gegenüber dem BSI gemeint ist.

Zu § 22/2 (Speicherung und Auswertung von Daten zur Abwehr einer dringenden Gefahr für die IT-Sicherheit):

Die empfohlene Regelung über die Speicherung von Daten zur Abwehr einer dringenden Gefahr beruht ebenfalls auf einem Änderungsvorschlag der Fraktionen von SPD und CDU. Dieser wurde wie folgt begründet:

> *„Neue Erkenntnisse bei der Bekämpfung von Angriffen auf die IT-Sicherheit haben ergeben, dass für die Erkennung von Schadsoftware und des Ausmaßes einer Beeinträchtigung im Falle einer Infektion in bestimmten Fällen eine retrograde Auswertung zwingend erforderlich ist. Hintergrund sind aktuelle Sicherheitsvorfälle mit der Schadsoftware Emotet. Sobald Schadsoftware wie Emotet in ein System eindringt, lädt sie weitere Schadsoftware nach, die sich sodann lateral im Netzwerk ausbreitet und dort umfassende Informationen über das Netz sammelt und an den Angreifer sendet. Dieses Vorgehen dient in der Regel der Vorbereitung weiterer Angriffe, insbesondere durch sog. Verschlüsselungstrojaner (Ransomware). Schadsoftware wie diese stellt demzufolge eine große Gefahr nicht nur für die Vertraulichkeit der Daten des Landesdatennetzes dar, sondern auch für deren Integrität und Verfügbarkeit. Wie gegenwärtig diese Gefahr ist, haben wiederholt Sicherheitsvorfälle mit sog. Ransomware gezeigt, aktuell beispielsweise beim Krankenhaus-Betreiber DRK Trägergesellschaft Süd-West. Dabei wurden die IT-Systeme von insgesamt 13 Krankenhäusern verschlüsselt und die Arbeit des Klinikpersonals erheblich beeinträchtigt. Aufgrund der hocheffizienten Weiterentwicklung von Schadsoftware kann es vorkommen, dass die Erstinfektion von den IT-Sicherheitssystemen nicht erkannt wird, sodass eine unbemerkte Ausbreitung von Schadsoftware im Netzwerk möglich ist. In derartigen Fällen können das Ausmaß der Beeinträchtigung dann nur durch eine retrograde Auswertung erkannt und die Gefahr abgewehrt bzw. Schäden behoben werden. Die retrograde Auswertung ist ausschließlich als Ultima-Ratio zulässig.“*

Die empfohlene Regelung ermöglicht die anlasslose und flächendeckende Speicherung des gesamten Datenverkehrs (einschließlich sämtlicher von Artikel 10 Abs. 1 GG geschützter Verkehrs- und Inhaltsdaten) der unmittelbaren und mittelbaren Landesverwaltung, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind, für einen Monat (erster Grundrechtseingriff) sowie die Auswertung dieser gespeicherten Daten zur Abwehr dringender Gefahren für die IT-Sicherheit (zweiter Grundrechtseingriff). Sowohl die Speicherung nach Absatz 1 als auch die Auswertung nach Absatz 2 greifen hinsichtlich der erfassten Verkehrs- und Inhaltsdaten in das Fernmeldegeheimnis (Artikel 10 Abs. 1 GG) und im Übrigen in das Recht auf informationelle Selbstbestimmung ein (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG). Die Eingriffsintensität dieser Maßnahmen geht deutlich über die mit der Erhebung und Auswertung des Datenverkehrs verbundenen Eingriffe (vgl. dazu die Erläuterungen zu § 21 Abs. 2 und zu § 22 Abs. 3) hinaus. Zwar wird - anders als dort - nur der Datenverkehr erfasst (vgl. § 19 Abs. 1/1), nicht hingegen die automatisierten Ereignisdokumentationen (vgl. § 19 Abs. 1), jedoch werden nicht nur - wie dort - flüchtige Daten durchgesehen und unverzüglich wieder gelöscht (wenn sie nicht im Falle ihrer Auffälligkeit zur weiteren Auswertung gespeichert werden), sondern zu einer möglichen späteren Auswertung für 30 Tage „auf Vorrat“

gespeichert. Dieser Speicherung liegt denknotwendig kein Stufenmodell zugrunde, sie erfolgt „anlasslos“ (vgl. dazu die Erläuterung zu § 21 Abs. 2).

Der GBD hat darauf hingewiesen, dass eine so umfangreiche Speicherung von Telekommunikations-Inhaltsdaten bislang - soweit dem GBD bekannt - der Rechtsordnung fremd sei. Um mit dem verfassungsrechtlich aus dem Rechtsstaatsprinzip (Artikel 20 Abs. 3 GG) abgeleiteten Grundsatz der Verhältnismäßigkeit vereinbar zu sein, unterliege eine Regelung von solcher Eingriffstiefe ähnlich strengen Voraussetzungen wie die vom BVerfG im Jahr 2009 für verfassungswidrig erklärte Verpflichtung der Telekommunikations-Diensteanbieter, sämtliche Telekommunikations-Verkehrsdaten sechs Monate zu speichern (vgl. BVerfGE 125, 260). Angesichts der Begründung und des insoweit bestehenden Einschätzungsspielraums des Gesetzgebers bestünden zwar an dem legitimen Zweck, der Geeignetheit und der Erforderlichkeit der Eingriffe keine Zweifel. Fraglich sei jedoch, ob die Maßnahmen der Verhältnismäßigkeit im engeren Sinne (Angemessenheit) genügten. Das BVerfG halte eine anlasslose Speicherung für verfassungsrechtlich bedenklich, weil sie geeignet sei, bei der Bevölkerung ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das die unbefangene Grundrechtsausübung beeinträchtigen könne (BVerfGE 125, 260, 320, Rn. 212). Ein solches bedrohliches Gefühl des Beobachtetseins könne auch bei der empfohlenen Speicherung des Telekommunikationsverkehrs mit Behörden entstehen, zumal hier sogar die Inhaltsdaten erfasst würden. Andererseits könne ein bedrohliches Gefühl des Beobachtetseins möglicherweise auch dann entstehen, wenn der Staat die für die digitale Verwaltung unentbehrlichen Telekommunikationsbeziehungen nicht effektiv davor schützte, durch Schadprogramme oder Angriffe kompromittiert zu werden. Ob das BVerfG diese gefühlten Bedrohungen im Falle einer verfassungsrechtlichen Überprüfung saldieren und wo es ggf. die stärkere Bedrohung verorten würde, könne der GBD allerdings nicht vorhersagen. Das BVerfG prüfe des Weiteren, ob eine Maßnahme auf die Totalüberwachung der Kommunikation der Bevölkerung insgesamt angelegt sei (dann wäre sie in jedem Fall unverhältnismäßig) oder ob sie in begrenzter Weise an die besondere Bedeutung der Telekommunikation in der modernen Welt anknüpfe und auf das spezifische Gefahrenpotenzial reagiere, das sich mit dieser verbinde (BVerfG, a. a. O., S. 322, Rn. 216); in diesem Fall wäre sie zumindest rechtfertigungsfähig. Bei den hier empfohlenen Maßnahmen sei in Rechnung zu stellen, dass die in Absatz 1 vorgesehene Speicherung nicht sämtlichen (privaten, beruflichen oder sonstigen) Telekommunikationsverkehr erfasse, sondern lediglich die Kommunikation mit Behörden (der unmittelbaren und mittelbaren Landesverwaltung). Diese Kommunikation werde zwar teilweise auch privater Natur sein, sie stehe jedoch überwiegend in einem dienstlichen Kontext (vgl. die Erläuterung zu § 21 Abs. 2). Zudem solle die empfohlene Regelung laut ihrer Begründung darauf reagieren, dass die zu speichernden Daten flüchtig und unsichtbar sind, mithin auf keinem anderen Weg verfügbar gehalten werden können (vgl. dazu BVerfG, a. a. O., S. 323, Rn. 217). Vor diesem Hintergrund könne das BVerfG auch die empfohlene Regelung noch als hinreichend begrenzte Reaktion auf die spezifischen Gefahren der digitalen Verwaltung ansehen und mithin für rechtfertigungsfähig halten. Das BVerfG habe die damaligen TKG-Regelungen allerdings vor allem deswegen als rechtfertigungsfähig angesehen, weil die Speicherung nicht direkt durch eine staatliche Stelle erfolgte, die Speicherung nicht auch die Kommunikationsinhalte erfasste und zudem die Speicherung aufgerufener Internetseiten untersagt war (BVerfG, a. a. O., S. 324, Rn. 218). Gerade in der Trennung von speichernder (nichtöffentlicher) und zugreifender (öffentlicher) Stelle habe das BVerfG eine wirksame Kontrolle durch die notwendige Filterung der Daten gesehen (a. a. O., S. 338 f., Rn. 250). In allen drei genannten Punkten gehe die empfohlene Regelung über die damalige TKG-Regelung hinaus: Nach der vorgeschlagenen Regelung würden nicht nur Verkehrsdaten, sondern auch Inhaltsdaten erfasst, die speichernde und die auswertende Stelle seien identisch und auch die abgerufenen Internetseiten würden gespeichert. Dieser Umstand begründe aus Sicht des GBD in jedem Fall ein erhebliches verfassungsrechtliches Risiko. Dass das BVerfG die vorgeschlagene Regelung im Falle einer Überprüfung für nicht rechtfertigungsfähig halten werde, lasse sich allerdings nicht sicher prognostizieren. Denn zum einen sei die Speicherung auf höchstens 30 Tage begrenzt (nicht wie damals im TKG auf sechs Monate). Zum anderen dürften die gespeicherten Daten nur hinsichtlich ihrer technischen Bedeutung, in keinem Fall hingegen personenbezogen bzw. verhaltensbezogen ausgewertet werden (vgl. § 27 Abs. 0/1), sodass sich nachteilige Folgen für Betroffene auf Zufallsfunde beschränkten. Dies sei nach Einschätzung des GBD im Hinblick auf die Persönlichkeitsrelevanz der Maßnahme von besonderer Bedeutung (vgl. dazu bereits die Erläuterung zu § 21 Abs. 2).

Der Ausschuss möchte die Regelung trotz des dargelegten verfassungsrechtlichen Risikos im Hinblick auf die Verhältnismäßigkeit in das Gesetz aufnehmen, empfiehlt allerdings, das verfassungsrechtliche Risiko zumindest dadurch zu reduzieren, dass in normenklarer Weise hohe Anforderungen an die Auswertung gestellt werden (vgl. zur Eingriffsschwelle BVerfG, a. a. O., S. 329 f., Rn. 230 f.), diese Anforderungen vor der Auswertung von einer unabhängigen Stelle überprüft werden (vgl. zum Richtervorbehalt BVerfG, a. a. O., S. 337 f., Rn. 247 ff.) und überdies die Anforderungen an die Datensicherheit (vgl. dazu BVerfG, a. a. O., S. 325, Rn. 220 ff.) und den Kernbereichsschutz eingehalten werden. Dazu dienen die vom Änderungsvorschlag abweichenden Empfehlungen, die im Folgenden im Einzelnen begründet werden. Aus der empfohlenen Regelung ergeben sich überdies Folgeänderungen. Insbesondere soll § 22/2 in die Regelung über die Datensicherheit (§ 23) aufgenommen werden (zu der verfassungsrechtlichen Notwendigkeit siehe oben). Auf Vorschlag des MI soll § 22/2 aber auch in die Aufzählungen in den §§ 22/3, 25, 26, 26/1 und 27 aufgenommen werden.

Zu Absatz 1:

In der Regelung über die Speicherung in Satz 1 soll präzisiert werden, dass mit dem „anfallenden Datenverkehr“ der nach § 19 Abs. 1/1 erhobene Datenverkehr gemeint ist. Mit der Formulierung „zu dem Zweck … erforderlich“ ist auch nach dem Verständnis des MI keine konkrete Eingriffsschwelle beabsichtigt (dies wäre wohl auch sinnlos, weil die Speicherung zu diesem Zweck immer erforderlich sein dürfte; vgl. dazu auch *Buchberger*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, Rn. 12 zu § 5 BSIG). Daher soll im Wortlaut verdeutlicht werden, dass es sich um eine Zweckbestimmung handelt. Dabei sollen die Sicherheitslücken gestrichen werden. Denn Sicherheitslücken können nach Mitteilung des MI ohne Angriffe oder Schadprogramme, welche die Sicherheitslücken ausnutzen, die hier abzuwehrenden dringenden Gefahren für die IT-Sicherheit (dazu gleich) nicht verursachen.

Der Ausschuss empfiehlt, die begrifflich § 2 Nr. 4 NPOG entlehnte „dringende Gefahr für die IT-Sicherheit“ in normklarer Weise näher zu bestimmen. Die „dringende Gefahr“ ist hier begrifflich nicht ohne Weiteres geeignet, weil sie nach § 2 Nr. 4 NPOG nur bestimmte Rechtsgüter schützt („Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt“). Der Ausschuss versteht darunter hier eine (konkrete) Gefahr für die IT-Sicherheit, die in zweifacher Weise qualifiziert werden soll, nämlich zum einen hinsichtlich der Höhe des zu erwartenden Schadens und zum anderen hinsichtlich der Eintrittswahrscheinlichkeit des Schadens. Dies soll im Wortlaut ausformuliert werden (redaktionell angelehnt an § 2 Nr. 4 NPOG). Da es hier - anders als sonst im Zweiten Abschnitt - um die IT-Sicherheit „im Landesdatennetz“ geht, soll klargestellt werden, dass damit eine dritte Qualifizierung der Gefahr für die IT-Sicherheit gemeint ist, nämlich dass die Gefahr für das gesamte Landesdatennetz besteht. Der empfohlene Klammerzusatz komplettiert die Legaldefinition des neuen Begriffs der „dringenden Gefahr für die IT-Sicherheit“ als dreifach qualifizierte konkrete Gefahr für die IT-Sicherheit und dient zur Vereinfachung der Überschrift und der Eingriffsschwelle in Absatz 2 Satz 1.

Zu Absatz 1 Satz 2 empfiehlt der Ausschuss zu verdeutlichen, dass die gespeicherten Daten nach einem rollierenden System zu löschen sind, d. h. mit der Speicherung der Daten des 31. Tages sind die Daten des 1. Tages zu löschen.

Zu Absatz 2:

Die Eingriffsschwelle in Absatz 2 Satz 1, die eine Auswertung der nach Absatz 1 gespeicherten Daten ermöglicht, soll begrifflich an Absatz 1 Satz 1 angepasst werden (dringende Gefahr für die IT-Sicherheit, vgl. zur Begriffsbestimmung die dortige Erläuterung). Durch diese angesichts der dreifachen Qualifizierung der konkreten Gefahr für die IT-Sicherheit hohe Eingriffsschwelle soll zugleich klargestellt werden, dass die Regelung allein auf den Schutz der IT-Sicherheit gerichtet ist, nicht hingegen auf die Straftatenverhütung oder gar die Straftatenverfolgung (wodurch die damit verbundenen Probleme hinsichtlich der Gesetzgebungskompetenz vermieden werden). Durch diese Empfehlung wird auch der Straftatenkatalog in Absatz 2 Satz 5 des Änderungsvorschlages entbehrlich. Die Empfehlung zu Satz 1 dient zudem dazu, die Maßnahme als „ultima ratio“ (vgl. die Begründung) deutlicher kenntlich zu machen. Anstelle der Formulierung in Satz 2 („zwingend erforderlich“) soll in Satz 1 wie im NPOG die Steigerung der Erforderlichkeit mit dem Wort „unerlässlich“

gekennzeichnet werden. Absatz 2 Satz 2 des Änderungsvorschlages wird dadurch entbehrlich. In Satz 1 soll überdies klargestellt werden, zu welchen Rechtsfolgen die Befugnis zur retrograden Auswertung führt bzw. führen kann. Ähnlich den Regelungen in § 21 Abs. 2 Satz 1 und § 22 Abs. 3 Satz 1 soll ausdrücklich benannt werden, dass die Vorschrift zur automatisierten und nicht automatisierten Auswertung, zur Entpseudonymisierung sowie zur über 30 Tage hinausreichenden Speicherung der Daten ermächtigt (ohne die Verlängerung der Speicherdauer würden bereits nach dem ersten Tag der Auswertung Teile der auszuwertenden Daten entfallen). Damit soll im Übrigen klargestellt werden, dass bei der retrograden Auswertung keine neuen Daten mehr hinzukommen können (es sei denn durch die Anpassung der Filter auf der ersten Stufe nach den §§ 18/1 und 19 sowie entsprechende Folgemaßnahmen auf der zweiten und dritten Stufe nach den §§ 21 und 22), die Maßnahme also nicht in die Zukunft gerichtet ist. Aus dem Zusammenhang mit den Worten „soweit und solange“ soll außerdem erkennbar werden, dass die Auswertung nach Absatz 2 zunächst begrenzt angeordnet werden muss (z. B. beschränkt auf automatisierte Auswertung und kurzfristige Verlängerung der Speicherung), wenn sich eine weitergehende Maßnahme noch nicht als „unerlässlich“ erweist (z. B. nicht automatisierte Auswertung mit dazu notwendiger längerer Speicherungsdauer).

In einem neuen Satz 1 Halbsatz 2 soll wie in § 19 Abs. 1/2 sowie § 22 Abs. 2 Satz 1 Halbsatz 2 und Abs. 3 Satz 1 Halbsatz 2 ausdrücklich klargestellt werden, dass die Auswertung der kommunikativen Bedeutung von Inhaltsdaten unzulässig ist, da dies für die Persönlichkeitsrelevanz der Maßnahme von besonderer Bedeutung ist (siehe oben).

In Satz 2 soll der insbesondere für die betroffenen Inhaltsdaten relevante Kernbereichsschutz sichergestellt werden. Das Niveau soll hier nicht hinter § 22 Abs. 5 zurückbleiben, sodass eine entsprechende Verweisung empfohlen wird.

Zu Absatz 3:

Der Ausschuss empfiehlt zu Satz 1 aus den oben dargelegten Gründen, den in Absatz 2 Sätze 3 und 4 des Änderungsvorschlages vorgesehenen Behördenleitervorbehalt durch den Richtervorbehalt zu ersetzen. Das Wort „Maßnahmen“ soll dabei zum Ausdruck bringen, dass jede einzelne in Absatz 2 Satz 1 genannte Art der Datenverarbeitung (automatisierte Auswertung, nicht automatisierte Auswertung, Entpseudonymisierung, Verlängerung der Speicherdauer) einer ausdrücklichen richterlichen Anordnung bedarf (die auch zunächst begrenzt und später erweitert werden kann; vgl. dazu die Erläuterung zu Absatz 2 Satz 1). Diese Empfehlung berücksichtigt insbesondere, dass die speichernde Stelle dieselbe ist wie die auswertende Stelle und daher ohne eine dazwischen geschaltete unabhängige Stelle wohl kaum von einer wirksamen Kontrolle ausgegangen werden könnte (siehe oben).

In den Sätzen 2 bis 4 sollen ergänzende Anforderungen an den behördlichen Antrag und die gerichtliche Entscheidung aufgenommen werden, wie sie das BVerfG für erforderlich gehalten hat (BVerfGE 125, 260, 338, Rn. 249; vgl. auch die entsprechenden Regelungen im NPOG, z. B. in § 33 a Abs. 5 Sätze 1 bis 4 und 8).

Die zu Satz 5 empfohlene Verweisung entspricht den Empfehlungen zu § 25 Abs. 2 Satz 2 Halbsatz 2 und § 27 Abs. 1 Satz 2 Halbsatz 2.

Eine Befristung bzw. Verlängerung der Anordnung soll hier (anders als z. B. in § 33 a Abs. 5 Sätze 5 bis 7 NPOG) nicht vorgesehen werden, weil die Auswertung ausschließlich retrograd erfolgt, d. h. nicht auf zukünftig zu erhebende Daten gerichtet ist (siehe oben). Dies schließt allerdings nicht aus, ggf. eine begrenzte Anordnung zu treffen, die später (bei neuen Erkenntnissen) durch eine neu beantragte Anordnung nach Satz 3 erweitert wird (vgl. dazu die Erläuterung zu Absatz 2 Satz 1).

Mit den Sätzen 6 bis 9 empfiehlt der Ausschuss auf Vorschlag des MI eine Eilbefugnis bei Gefahr im Verzug. Die Empfehlungen sind insoweit an § 33 a Abs. 6 Sätze 1, 2 und 5 bis 7 NPOG angelehnt. Insbesondere soll in Satz 6 Halbsatz 2 bestimmt werden, dass die Anordnung auch eine Begründung der Gefahr im Verzug enthalten muss (wie in § 33 a Abs. 6 Satz 2 NPOG). Für den Fall einer abgelehnten richterlichen Bestätigung der Anordnung soll bei der Löschungspflicht in Satz 9 Halbsatz 2 klargestellt werden, dass die rollierende Speicherung als solche (Absatz 1) davon unbe-

einträchtigt bleibt; für weitere Anwendungsfälle des Absatzes 2 sollen die Daten weiter zur Verfügung stehen.

Zu Absatz 4:

Die empfohlene Regelung enthält die in Absatz 2 Satz 6 des Änderungsvorschlages vorgesehene Löschungspflicht und präzisiert diese, indem sie Übermittlungen ermöglicht (wie auch § 21 Abs. 3 und § 22 Abs. 4) sowie in einem neuen Halbsatz 2 dieselbe Unberührtheitsklausel aufnimmt wie in Absatz 3 Satz 9 Halbsatz 2 (siehe oben).

Zu § 22/3 (Beseitigung von Schadprogrammen):

Die empfohlene Regelung greift in Satz 1 den Regelungsgehalt des § 18 Abs. 2 des Entwurfs an rechtssystematisch passender Stelle auf und ergänzt in Satz 2 die Ermächtigung zur Löschung untrennbar mit dem Schadprogramm verbundener Daten (vgl. die Erläuterung zu § 18 Abs. 2 des Entwurfs).

Zu § 23 (Datensicherheit, Protokollierung):

Zur Überschrift:

Die Überschrift soll auch den Regelungsgehalt des Absatzes 3 aufnehmen und gestrafft werden.

Zu Absatz 1:

Die Empfehlung enthält Folgeänderungen zu den vorgeschlagenen §§ 18/1, 22/1 und 22/2. Im Übrigen sollen hier auch die - nach Mitteilung des MI gleichermaßen zu schützenden - Auswertungsergebnisse genannt werden (vgl. die Empfehlungen zu § 18/1 Abs. 2, § 19 Abs. 2 Satz 1, § 21 Abs. 1 Satz 3 und Abs. 3, § 22 Abs. 2 Satz 6 und Absatz 4).

Zu Absatz 2:

In der empfohlenen Nummer 0/1 soll Nummer 6 des Entwurfs aufgenommen werden, weil auf die hier genannten Personen in den Nummern 1 und 7 verwiesen wird.

In Nummer 1 soll durch Verweisung auf Nummer 0/1 präzisiert werden, wer „die dafür bestimmten Personen“ sind (vgl. im Übrigen die Erläuterung zu Absatz 1).

Nummer 2 soll sprachlich verbessert werden (zur Verweisung auf die §§ 18/1, 22/1 und 22/2 vgl. die Erläuterung zu Absatz 1).

Nummer 4 ist angesichts der Regelungen in § 21 Abs. 1 Satz 2 und § 22 Abs. 2 Satz 2 auch nach Auffassung des MI redundant und soll daher gestrichen werden.

Nummer 6 des Entwurfs soll in die neue Nummer 0/1 verlagert werden.

Nach Mitteilung des MI sind in Nummer 7 mit den dort genannten Personen die nach Nummer 6 des Entwurfs von der Behördenleitung ermächtigten Personen gemeint. Dies soll im Wortlaut durch Verweisung auf Nummer 0/1 klargestellt werden.

Zu Absatz 2/1:

Da die Regelung des Sicherheitskonzepts in § 24 des Entwurfs ebenfalls die Datensicherheit betrifft und überdies unmittelbar an die hier in den Absätzen 1 und 2 geregelten organisatorischen und technischen Maßnahmen anknüpft, soll die Regelung hier als Absatz 2/1 eingefügt werden. Dass sich das Sicherheitskonzept auf das „von der Behörde verwendete System zur Datenverarbeitung nach den §§ 19 bis 22“ beziehen soll (Begründung, Drs. 18/1598, S. 80), soll im Wortlaut von Satz 1 verdeutlicht werden (zur Verweisung auf die §§ 18/1, 22/1 und 22/2 vgl. die Erläuterung zu Absatz 1).

Durch die Empfehlungen zu den Sätzen 2 und 3 soll ebenfalls der beabsichtigte Regelungsgehalt verdeutlicht werden.

Zu Absatz 3:

In Satz 1 soll der Zweck (Datenschutzkontrolle) nicht genannt werden, weil er zugleich durch Satz 3 festgelegt wird. Die Regelung soll im Übrigen sprachlich gestrafft werden. Auf Vorschlag des MI soll hier auch die Übermittlung aufgenommen werden, um deren Rechtmäßigkeit nachvollziehen zu können. Ebenfalls auf Vorschlag des MI soll auch die Verarbeitung der Auswertungsergebnisse erfasst werden. Vgl. im Übrigen die Erläuterung zu Absatz 1.

Satz 2 soll sprachlich gestrafft werden.

In Satz 3 soll ebenso wie in Satz 1 (und § 22 Abs. 5 Satz 6) auf die „Datenschutzkontrolle“ abgestellt werden. Dieser Begriff entspricht inhaltlich der in § 35 Abs. 4 Satz 1 Nr. 3 NDSG genannten „Überprüfung der Rechtmäßigkeit der Datenverarbeitung“ und wird z. B. auch in § 17 c Abs. 2 Satz 9, § 31 a Abs. 1 Satz 4, § 33 Abs. 5 Satz 3, § 39 Abs. 2 Satz 1, § 40 Abs. 1 Satz 5 und § 42 Abs. 2 Satz 1 NPOG verwendet.

Der Ausschuss empfiehlt, die Löschungsfrist in Satz 4 zu verlängern (vgl. die Empfehlung zu § 22 Abs. 5 Satz 7), zumal Absatz 4 des Entwurfs bzw. § 26/1 der Empfehlung eine jährliche Unterrichtung der/des LfD vorsieht, die/der bei einer früheren Löschung des Protokolls die Datenverarbeitung teilweise nicht mehr nachvollziehen könnte.

Zu Absatz 4:

Die Regelung soll wegen ihres eigenständigen Gehalts („Beteiligung der oder des Landesbeauftragten für den Datenschutz“) und der Bezüge zu den §§ 25 und 26 hinter diese Regelungen verlagert werden (vgl. die Empfehlung zu § 26/1), zumal es sich bei der vorzulegenden „Aufstellung“ nach Mitteilung des MI nicht um das nach Absatz 3 anzufertigende „Protokoll“ handeln soll.

Zu § 24 (Sicherheitskonzept):

Die Regelung soll zur Verbesserung der Rechtssystematik in § 23 („Datensicherheit“) als Absatz 2/1 aufgenommen werden.

Zu § 25 (Benachrichtigung der betroffenen Personen):

Die Regelung soll zur besseren Verständlichkeit untergliedert werden in einen Absatz 1 (Benachrichtigungspflicht) und einen Absatz 2 (Unterbleiben der Benachrichtigung); vgl. dazu auch § 30 Abs. 4 und 5 NPOG.

Zu Absatz 1:

Die Bezugnahme in Satz 1 auf „Maßnahmen nach diesem Gesetz“ ist zu weit und soll daher beschränkt werden. Nach Mitteilung des MI sind hier nur die Maßnahmen nach den §§ 19 bis 22 des Entwurfs, die auf dem Änderungsvorschlag der Fraktionen von SPD und CDU beruhenden Empfehlungen zu den §§ 22/1 und 22/2 sowie die Übermittlung nach § 27 gemeint. Gestrichen werden soll auch die Benachrichtigung von Behörden. Behörden können nach Mitteilung des MI von den Maßnahmen nicht betroffen sein, denn die Betroffenheit ergibt sich aus der Verarbeitung personenbezogener (nicht behördenbezogener) Daten. Der im Entwurf bestimmte Zeitpunkt der Benachrichtigung der Betroffenen („spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen“) würde voraussetzen, dass der Zweck der Maßnahmen durch eine frühere Benachrichtigung vereitelt würde (vgl. BVerfGE 125, 260, 335 f., Rn. 243). Der Ausschuss empfiehlt vor diesem Hintergrund und auf Vorschlag des MI, die betroffenen Personen unverzüglich zu benachrichtigen, allerdings spätestens nach der Abwehr der durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr für die IT-Sicherheit. Die im Gesetzentwurf enthaltene Begrenzung auf Schadprogramme soll gestrichen werden, weil eine Gefahr für die IT-Sicherheit auch durch Sicherheitslücken und Angriff verursacht werden kann. Zu der in Satz 1 des Entwurfs enthaltenen Variante der „überwiegenden schutzwürdigen Belange Dritter“ (die aus § 5 Abs. 4 Satz 1 BSIG übernommen wurde und sich wohl an § 101 Abs. 4 Satz 3 StPO anlehnt; vgl. *Buchberger*, in Schenke/Graulich/Ruthig, Sicher-

heitsrecht des Bundes, 2. Aufl. 2019, Rn. 24 zu § 5 BSIG) hat das MI mitgeteilt, dass keine entsprechenden Fallkonstellationen vorstellbar seien. Die Variante soll daher gestrichen werden.

Von den Maßnahmen betroffen sind sämtliche Personen, deren Daten verarbeitet worden sind (Begründung, Drs. 18/1598, S. 80). Anders als bei den auf bestimmte Zielpersonen gerichteten Maßnahmen nach dem Strafprozess-, Polizei- und Verfassungsschutzrecht gibt es hier keine Differenzierung zwischen Betroffenen im engeren Sinne („Zielpersonen“) und unvermeidbar mitbetroffenen Personen (deren Daten nur zufällig miterfasst wurden, die aber selbst nicht im Fokus behördlichen Handelns standen), für die das BVerfG unterschiedliche Maßstäbe entwickelt hat (vgl. BVerfGE 125, 260, 334 ff., Rn. 240 ff.; BVerfGE 141, 220, 282 f., Rn. 136). Verfassungsrechtlich zulässig ist jedenfalls eine Ausnahme von der Benachrichtigungspflicht in Fällen, in denen durch die Benachrichtigung bzw. die dazu notwendigen Ermittlungen der Grundrechtseingriff noch vertieft würde (BVerfGE 125, 260, 336, Rn. 244). Diese in Satz 1 des Entwurfs angelegte Ausnahme („wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen“) soll in einen neuen Satz 2 ausgegliedert und an die entsprechende Regelung in § 30 Abs. 4 Satz 4 NPOG angeglichen werden. Nach Mitteilung des MI wird in der Praxis aus diesem Grund die Benachrichtigung über die automatisiert ablaufenden Maßnahmen nach § 18/1, § 19 Abs. 1 und 1/1, § 21 Abs. 1 und § 22 Abs. 2 regelmäßig ausscheiden.

Zu Absatz 2:

Der Ausschuss empfiehlt, die in Satz 2 Nr. 1 des Entwurfs enthaltene Regelung in Satz 1 Nrn. 1 und 1/1 zu untergliedern. Soweit die Benachrichtigung unterbleiben soll, um ein Strafverfahren nicht zu gefährden, soll die Regelung in Satz 1 Nr. 1 aufgenommen und auf § 27 Abs. 1 Nr. 1 abgestimmt werden. Da eine Nutzung oder Übermittlung zum Zweck eines Disziplinarverfahrens nach § 27 generell nicht gestattet ist, soll diese Möglichkeit hier gestrichen werden. Der Ausschuss empfiehlt auf Vorschlag des MI, in Satz 1 Nr. 1 auch das Unterbleiben der Benachrichtigung zur Absicherung der Übermittlungszwecke in § 27 Abs. 1 Satz 1 Nrn. 2 und 3 (Gefahrenabwehr, Verfassungsschutz) aufzunehmen, das nach Mitteilung des MI im Gesetzentwurf übersehen worden ist.

Der nach Mitteilung des MI einzige denkbare Fall, in dem eine Benachrichtigung die IT-Sicherheit gefährden könnte (vgl. Satz 2 Nr. 1 des Entwurfs), besteht in dem mit einer detaillierten Benachrichtigung möglicherweise verbundenen Bekanntwerden einer Sicherheitslücke, das zu weiteren Angriffen führen könnte. Diese Fallkonstellation soll ausdrücklich benannt und wegen ihrer eigenständigen Zielrichtung in Satz 1 Nr. 1/1 ausgegliedert werden.

Der Ausschuss empfiehlt, in Satz 2 den in Satz 3 des Entwurfs enthaltenen Behördenleitervorbehalt für die Fälle des Satzes 1 Nrn. 1 und 1/1 zu einem Richtervorbehalt aufzuwerten. Bei den nur zufällig miterfassten Personen, die selbst nicht im Fokus behördlichen Handelns standen und bei denen anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben (Satz 1 Nr. 2), bedarf es nach der Rechtsprechung des BVerfG keiner richterlichen Bestätigung dieser Abwägungsentscheidung (vgl. BVerfGE 125, 260, 337, Rn. 245). Anders ist dies bei der heimlichen Verwendung der Daten z. B. zu Zwecken eines Strafverfahrens nach Satz 1 Nr. 1 (vgl. BVerfGE 125, 260, 336 f., Rn. 244). Um zu vermeiden, dass die verfahrensmäßige Absicherung der Nichtbenachrichtigung hier hinter § 5 Abs. 4 Sätze 3 bis 5 BSIG zurückbleibt (dort ist zumindest die Zustimmung des insoweit ausdrücklich weisungsfreien behördlichen Datenschutzbeauftragten erforderlich; eine Begründung für diese erst in der Ausschussberatung eingefügte Regelung hat der Bundesgesetzgeber allerdings nicht abgegeben [vgl. BT-Drs. 16/13259, S. 6 f.]), hat sich auch das MI dafür ausgesprochen, die Fälle des Satzes 1 Nrn. 1 und 1/1 von einer richterlichen Zustimmung abhängig zu machen, dann aber auf eine parallele Regelung eines Behördenleitervorbehalts zu verzichten. Dem ist der Ausschuss mit seiner Empfehlung gefolgt.

Zu dem - für die verbleibenden Fälle des Satzes 1 Nr. 2 vorgesehenen - Behördenleitervorbehalt in den Sätzen 3 bis 5 des Entwurfs vgl. die Empfehlungen zu § 21 Abs. 2 Sätze 3 bis 5 des Entwurfs.

Zu § 26 (Dokumentation):

Der Ausschuss empfiehlt zu Satz 1 als Folgeänderung zu § 25, sowohl die behördlichen Anordnungen (§ 25 Abs. 2 Satz 3) als auch die (teilweise an deren Stelle tretenden) gerichtlichen Zustimmungen (§ 25 Abs. 2 Satz 2) zu dokumentieren. Auf Vorschlag des MI sollen überdies auch die Übermittlungen nach § 27 aufgenommen werden, soweit sie der Zustimmung des Amtsgerichts oder der G 10-Kommission bedürfen (§ 27 Abs. 1 Sätze 2 bis 6). Zudem sollen auf Vorschlag des MI auch die Anordnungen und Bestätigungen nach dem neuen § 22/2 dokumentiert werden (§ 22/2 Abs. 3 Sätze 1, 6 und 7).

Die Sätze 2 und 3 sollen an die Empfehlungen zu § 22 Abs. 5 Sätze 6 und 7 angelehnt werden, zumal die Löschungsfrist in Satz 3 zu knapp bemessen sein dürfte (vgl. die Erläuterung zu § 22 Abs. 5 Sätze 6 und 7).

Zu § 26/1 (Beteiligung der oder des Landesbeauftragten für den Datenschutz):

Die Regelung über die jährliche Unterrichtung der/des Landesbeauftragten für den Datenschutz (§ 23 Abs. 4 des Entwurfs) soll wegen ihrer Eigenständigkeit und wegen der Bezüge zu den §§ 25 und 26 in den neuen § 26/1 verlagert werden. In Satz 1 soll zudem klargestellt werden, dass die Verpflichtung nur die Behörden trifft, die ihre Befugnisse nach diesem Abschnitt auch tatsächlich wahrnehmen. Die in der Begründung (Drs. 18/1598, S. 80) genannte Möglichkeit, die Aufstellung „gebündelt von einer Stelle“ vorlegen zu lassen, wird dadurch nicht ausgeschlossen. Sie setzt allerdings voraus, dass die Aufstellung keine personenbezogenen Daten enthält, denn deren Übermittlung zu einem solchen Zweck ist im Gesetz nicht vorgesehen (dies wäre aber wegen der damit verbundenen Vertiefung des Grundrechtseingriffs notwendig). Das MI hat dazu mitgeteilt, dass sich die Aufstellung an der statistischen Aufstellung im Sinne des § 5 Abs. 9 BSIG orientieren wird, also ohne personenbezogene Daten auskommt. Auf Vorschlag des MI sollen in Satz 1 auch die Übermittlungen nach § 27 Abs. 1 (an Strafverfolgungs-, Polizei- und Verfassungsschutzbehörden), die für die Betroffenen nachteilige Folgemaßnahmen auslösen können, in die Aufstellung aufgenommen werden (vgl. auch § 5 Abs. 9 Nr. 1 BSIG sowie die Empfehlung zu § 26 Satz 1). Dasselbe empfiehlt der Ausschuss auf Vorschlag des MI für die neuen §§ 22/1 und 22/2. Da keine andere „zuständige Aufsichtsbehörde für den Datenschutz“ infrage kommen dürfte als die/der LfD, soll diese/dieser in Satz 1 genannt werden. Zwar spricht sich die Begründung (a. a. O.) wegen der Ausnahme der Gerichte für eine offenere Formulierung aus. Jedoch dürfte die Wahrnehmung der Befugnisse nach dem Zweiten Abschnitt durch die vom MJ bestimmte Stelle (vgl. § 17 Abs. 2/2) als Verwaltungsaufgabe im Sinne von § 1 Abs. 2 NDSG anzusehen sein, sodass auch insoweit die/der LfD zuständig ist.

Der GBD hat darauf hingewiesen, dass im Gesetzentwurf - anders als in § 5 Abs. 10 BSIG (der allerdings erst in der Ausschussberatung und ohne nähere Begründung eingefügt worden ist; vgl. BT-Drs. 16/13259, S. 7) - keine parlamentarische Kontrolle in Form einer Unterrichtung des zuständigen Landtagsausschusses vorgesehen worden ist. Das BVerfG hat jedenfalls bei heimlichen Überwachungsmaßnahmen nach dem Bundeskriminalamtgesetz (BKAG) die gesetzliche Sicherstellung regelmäßiger Berichte gegenüber dem Parlament und der Öffentlichkeit verlangt (BVerfGE 141, 220, 285, Rn. 143). Wie oben zu § 21 Abs. 2 dargelegt, dürften die im Zweiten Abschnitt geregelten Befugnisse jedoch von geringerer Persönlichkeitsrelevanz sein als die heimlichen Überwachungsmaßnahmen nach dem BKAG. Der Ausschuss ist daher dem MI gefolgt, das sich vor diesem Hintergrund gegen die Regelung entsprechender Berichtspflichten ausgesprochen hat.

Zu § 27 (Zweckbindung, Übermittlung personenbezogener Daten):

Zu Absatz 0/1:

Die grundsätzlich einer Übermittlung im Wege stehende Zweckbindung der nach diesem Abschnitt verarbeiteten Daten soll aus § 18 Abs. 3 des Entwurfs in den neuen Satz 1 verlagert und an den beabsichtigten Regelungsgehalt angepasst werden (vgl. die Erläuterung zu § 18 Abs. 3 des Entwurfs). Auf Vorschlag des MI soll sich die Zweckbindung auch auf die neuen §§ 22/1 und 22/2 erstrecken.

Der Ausschuss empfiehlt, in Satz 2 das - nach Mitteilung des MI auch für die §§ 20 bis 22 des Entwurfs sowie die neuen §§ 22/1 und 22/2 gewollte - Verbot der Erstellung von Nutzerprofilen aufzunehmen (vgl. die Erläuterung zu § 19 Abs. 2 Satz 4 des Entwurfs). Dabei soll durch das Wort „insbesondere“ hervorgehoben werden, dass es sich um eine deklaratorische Verstärkung des in Satz 1 enthaltenen Zweckbindungsgrundsatzes handelt.

Zu Absatz 1:

Die Satzeinleitung von Satz 1 soll die in der Übermittlung liegende Abweichung von der in Absatz 0/1 geregelten Zweckbindung als solche kennzeichnen. Nach Mitteilung des MI sind mit „den Daten nach den §§ 21 und 22“ nur die Daten gemeint, die auf der dritten Stufe ausgewertet wurden. Darunter fallen die nach § 21 Abs. 2 ausgewerteten Verkehrsdaten und die nach § 22 Abs. 3 ausgewerteten Inhaltsdaten (jeweils auch in Verbindung mit § 22/1 Satz 2 Nr. 1, wenn bei der ergänzenden Auswertung durch das BSI die dritte Stufe erreicht worden ist und die dabei ausgewerteten Daten der beauftragenden Behörde zur Verfügung gestellt wurden) sowie die Auswertung nach dem neuen § 22/2 Abs. 2, aber auch die jeweils zugehörigen Auswertungsergebnisse. Der Ausschuss empfiehlt, dies in der Satzeinleitung zu verdeutlichen. Die im Entwurf enthaltene Soll-Regelung soll beibehalten werden, d. h. jede Behörde wird zur Übermittlung verpflichtet, es sei denn, es liegt ein atypischer Fall vor, der eine Ausnahme von der grundsätzlichen Übermittlungspflicht begründet. Das MI versteht darunter einerseits Massenfälle und andererseits Fälle, in denen eine Ermittlung offensichtlich chancenlos ist.

Der in Satz 1 Nr. 1 (zweckändernde Nutzung zur Strafverfolgung) verwendete Begriff „Straftat von auch im Einzelfall erheblicher Bedeutung“ entspricht § 5 Abs. 6 Satz 1 Nr. 1 BSIG und ist dort wohl auf § 100 g Abs. 1 Satz 1 Nr. 1 StPO zurückzuführen (vgl. *Buchberger*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, Rn. 36 zu § 5 BSIG). Der Ausschuss empfiehlt, die Entwurfsregelung entsprechend der Begründung (Drs. 18/1598, S. 82) anzupassen, um das vom BVerfG aufgestellte Kriterium der hypothetischen Datenneuerhebung (BVerfGE 141, 220, 327 ff., Rn. 286 ff.) zu erfüllen. Der GBD hat dazu allerdings mitgeteilt, dass vor dem Hintergrund der Rechtsprechung des BVerfG zu dem sog. Doppeltürenmodell nicht eindeutig beurteilt werden könne, ob der Landesgesetzgeber mit der von ihm zu regelnden „ersten Tür“ eigene Anforderungen an die - dem für das Strafprozessrecht zuständigen (Bundes-)Gesetzgeber obliegende - strafverfolgungsrechtliche Nutzung der Daten („zweite Tür“) stellen dürfe (BVerfG, a. a. O., S. 337 f., Rn. 316; NJW 2019, 827, 833, Rn. 80 m. w. N.; vgl. zu dieser Problematik auch den Schriftlichen Bericht zu § 39 Abs. 2 Satz 1 Nr. 1 und Satz 2/1 NPOG-Entwurf, Drs. 18/3723, S. 65 f.); der Bundesgesetzgeber habe hingegen bei der Regelung des § 5 Abs. 6 BSIG keiner entsprechenden Einschränkung der Gesetzgebungskompetenz unterlegen. Der Ausschuss empfiehlt vor diesem Hintergrund, anstelle der im Entwurf vorgesehenen konkreten Straftatenschwelle eine davon unabhängige, dem Kriterium der hypothetischen Datenneuerhebung entsprechende Voraussetzung der Übermittlung zu Strafverfolgungszwecken in Satz 1 Nr. 1 zu formulieren. Infrage kommt hier die hypothetische Datenneuerhebung sowohl nach § 100 a StPO (Telekommunikationsüberwachung zur Erhebung von Inhaltsdaten) als auch nach § 100 g StPO (Verkehrsdatenerhebung). Da nach Mitteilung des MI nur solche Daten übermittelt werden sollen, die zur Erfüllung der in Nummer 1 genannten Aufgabe erforderlich sind, empfiehlt der Ausschuss, dies im Wortlaut von Satz 1 Nr. 1 klarzustellen.

In Satz 1 Nr. 2 soll präzisiert werden, dass hier nach Mitteilung des MI sowohl niedersächsische Polizeibehörden als auch solche des Bundes oder eines anderen Landes als Empfänger in Frage kommen. Zudem sollen nach Mitteilung des MI auch hier nur Daten übermittelt werden, die zur Abwehr der genannten Gefahr erforderlich sind.

In Satz 1 Nr. 3 soll präzisiert werden, welche Verfassungsschutzbehörde gemeint ist. Nach Mitteilung des MI ist dies (allein) die des Landes (vgl. § 2 Abs. 1 Satz 1 NVerfSchG). Dies sei ausreichend, weil zwischen den Verfassungsschutzbehörden ohnehin die Pflicht zur Zusammenarbeit bestehe. Dem ist der Ausschuss mit seiner Empfehlung gefolgt. Entsprechend der Begründung (Drs. 18/1598, S. 82) soll auch hier das Kriterium der hypothetischen Datenneuerhebung umgesetzt werden. Infrage kommen hier Verkehrsdatenabfragen nach § 20 NVerfSchG sowie TKÜ-Maßnahmen nach § 3 G 10.

Um die verfahrensmäßigen Sicherungen insoweit nicht hinter § 5 Abs. 7 Satz 9 BSIG zurückbleiben zu lassen, empfiehlt der Ausschuss auf Vorschlag des MI, in Satz 1/1 eine Regelung zum Schutz

der zeugnisverweigerungsberechtigten Berufsgeheimnisträgerinnen/-träger im Sinne der §§ 53 und 53 a StPO aufzunehmen.

In Satz 2 soll - wie auch in § 5 Abs. 6 Satz 4 BSIG - geregelt werden, welches Gericht zuständig ist (vgl. z. B. auch § 33 a Abs. 5 Satz 1 und § 35 a Abs. 3 Satz 1 NPOG sowie die Empfehlung zu § 25 Abs. 2 Satz 4). Zudem soll - wie in Satz 4 und in § 25 Abs. 2 Satz 2 - die Verweisung auf die Verfahrensordnung aus Satz 3 des Entwurfs in einen neuen Satz 2 Halbsatz 2 verlagert werden. Wie auch in § 25 Abs. 2 Satz 2 Halbsatz 2 soll die Verweisung auf das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) durch die empfohlene Verweisung auf § 19 Abs. 4 NPOG präzisiert werden (auf diese Vorschrift verweisen auch verschiedene Vorschriften im NPOG). Satz 3 des Entwurfs soll infolgedessen gestrichen werden.

In Satz 4 soll die - wohl aus § 5 Abs. 6 Satz 5 BSIG stammende - für das Landesrecht unpassende Verweisung auf die §§ 9 bis 16 G 10 nicht übernommen werden (vgl. z. B. § 15 G 10, der nur für die Nachrichtendienste des Bundes gilt und die G 10-Kommission des Bundes meint). Für G 10-Maßnahmen der niedersächsischen Verfassungsschutzbehörde gilt das Niedersächsische Gesetz zur Ausführung des Artikel 10-Gesetzes (Nds. AG G 10). Da mit Satz 4 nach Mitteilung des MI lediglich beabsichtigt wird, dass die G 10-Kommission (des Landes) einer Übermittlung nach Satz 1 Nr. 3 vorher zustimmen muss, soll Satz 4 dies ausdrücklich bestimmen (vgl. auch § 21 Abs. 6 NVerfSchG).

Aufgrund des Änderungsvorschlages der Fraktionen von SPD und CDU empfiehlt der Ausschuss, in den neuen Sätzen 5 bis 7 eine Eilbefugnis bei Gefahr im Verzug aufzunehmen. Diese Änderung wurde wie folgt begründet:

> *„Die Ergänzung des § 27 dient der Effektivität der Gefahrenabwehr. Nach dem derzeitigen Gesetzentwurf ist für die Übermittlung an die in § 27 Absatz 1 Satz 1 genannten Behörden in allen Fällen die Einholung einer vorherigen gerichtlichen Zustimmung bzw. die vorherige Zustimmung der G10-Kommission erforderlich. Für den Fall von Gefahr im Verzuge sieht § 27 derzeit keine Eilkompetenz vor. Es ist aber durchaus denkbar, dass bei der Auswertung des Datenverkehrs auch solche Informationen erlangt werden, die eine unverzügliche Übermittlung erforderlich machen, um die Gefahr effektiv abwehren zu können. § 27 soll daher um eine Eilkompetenz für die unverzügliche Übermittlung der für die Abwehr der Gefahr im Verzuge erforderlichen Daten ergänzt werden."*

Der Ausschuss empfiehlt, die vorgeschlagenen Regelungen sprachlich zu überarbeiten und an die entsprechenden Regelungen im NPOG und NVerfSchG anzupassen. In Satz 5 soll auf Vorschlag des MI nicht „die Ministerin oder der Minister des für die zentrale IT-Steuerung zuständigen Ministeriums" zuständig sein, weil dies für Übermittlungen der vom MJ bestimmten Stelle (vgl. § 17 Abs. 2/2) oder der Behörden der mittelbaren Landesverwaltung (Kommunen usw.) unpassend wäre. Die Anordnungsbefugnis soll der Behördenleitung übertragen werden. Für den Fall einer Ablehnung der nachträglichen Zustimmung soll die Anordnung außer Kraft treten (Satz 7). Das Verwendungsverbot und die Löschungspflicht soll in einem eigenständigen Satz geregelt werden (Satz 8 Halbsatz 1) und durch eine Unterrichtungspflicht gegenüber der empfangenden Stelle ergänzt werden (Halbsatz 2). Der GBD hat in diesem Zusammenhang darauf hingewiesen, dass vor dem Hintergrund der Rechtsprechung des BVerfG zu dem sog. Doppeltürenmodell (siehe oben die Erläuterung zu Satz 1 Nr. 1) nicht eindeutig beurteilt werden könne, ob es in der Gesetzgebungskompetenz des Landes liege, in diesen Fällen die Verwendung der bereits übermittelten Daten auch zu strafprozessualen Zwecken zu verbieten. Das Verwendungsverbot der „ersten Tür" und damit der Gesetzgebungskompetenz des Landes zuzuordnen, liege allerdings nicht fern, weil der (Landes-) Gesetzgeber sonst keine Möglichkeit hätte, die Übermittlung (d. h. die von ihm zu regelnde „erste Tür") durch einen Richtervorbehalt abzusichern, wenn dieser einer Ausnahmeregelung bei Gefahr im Verzug bedarf.

Zu Absatz 2:

Nach Mitteilung des MI geht es bei der Übermittlung nach Absatz 2 um Fälle, in denen eine Sicherheitslücke, ein Schadprogramm oder ein Angriff sicher festgestellt wurde. Um anderen Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind, die Abwehr der sich daraus ergebenden

Gefahren zu ermöglichen (dies schließt die Beseitigung von Störungen, d. h. realisierten Gefahren, ein), sollen die Behörden ermächtigt werden, die dazu notwendigen Auswertungsergebnisse zu übermitteln. Laut MI geht es dabei insbesondere um sogenannte Indicator of Compromise (IoC)-Listen (diese enthalten IP-Adressen, URL und andere technische Informationen) sowie um einzelne IP-Pakete, Byte-Muster usw. Die Persönlichkeitsrelevanz dieser Daten sei, soweit überhaupt vorhanden, gering. Der dargelegte Regelungsgehalt soll durch die Empfehlung zu Satz 1 verdeutlicht werden. Insbesondere soll durch die Satzumstellung hervorgehoben werden, dass in den übermittelten Auswertungsergebnissen personenbezogene Daten nur in dem Umfang enthalten sein dürfen, wie es zur Gefahrenabwehr erforderlich ist (vgl. die Begründung, Drs. 18/1598, S. 82). Die unklare Formulierung der „für den Betrieb der Informationstechnik der Behörden zuständigen Stellen oder damit beauftragte Betriebe“ soll ersetzt werden durch die Übermittlung an die Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind (dieser Oberbegriff erfasst sowohl die Mitglieder des Sicherheitsverbundes gemäß § 12/1 Abs. 1 als auch die angeschlossenen Stellen gemäß § 12/1 Abs. 2; vgl. in diesem Sinne auch § 12/2 Abs. 2, § 13 Abs. 2 Nr. 2 und Abs. 3 sowie § 14 Satz 1). Der Ausschuss empfiehlt auf Vorschlag des MI, die Variante der „beauftragten Betriebe“ zu streichen (zumal sich die Übermittlung von personenbezogenen Daten innerhalb von Auftragsverarbeitungsverhältnissen nach Artikel 28 DSGVO richtet).

Die zu Satz 1 vorgeschlagene Fassung enthält auch die Befugnis für die in Satz 2 genannten Stellen, Auswertungsergebnisse einschließlich darin enthaltener personenbezogener Daten zur Wahrnehmung der Aufgaben nach § 13 Abs. 2 und 3 zu übermitteln. Satz 2 ist daher entbehrlich und soll gestrichen werden.

Zu § 28 (Einschränkung von Grundrechten):

Die Empfehlung, die in den §§ 22/1 und 22/2 geregelten Befugnisse aufzunehmen, beruht auf dem Änderungsvorschlag der Fraktionen von SPD und CDU. Da es nach Mitteilung des MI auch durch § 18 Abs. 2 des Entwurfs bzw. § 22/3 der Empfehlung zu einem Eingriff in das Fernmeldegeheimnis (Artikel 10 Abs. 1 GG) kommen kann, soll auch § 22/3 in die nach Artikel 19 Abs. 1 Satz 2 GG notwendige Zitierung aufgenommen werden.

Zu Artikel 2 (Änderung des Niedersächsischen Beamtengesetzes):

Zu § 92 a (Verarbeitung von Personalaktendaten im Auftrag):

Zu Absatz 1:

Die Empfehlung zu Satz 1 soll durch das Wort „bei“ klarstellen, dass hier keine Zuständigkeitsübertragung beabsichtigt ist (vgl. die Begründung, Drs. 18/1598, S. 83). Die Entwurfsregelung betrifft allein die Ebene der Datenverarbeitungsbefugnisse, nicht hingegen die vorgelagerte verwaltungsorganisationsrechtliche Frage der Zuständigkeitsverteilung (vgl. zur Trennung dieser Ebenen bereits Drs. 16/1088, S. 38, zu § 92 Abs. 2 des Niedersächsischen Beamtengesetzes [NBG]). Das bedeutet, dass die Kommunen auch nach der Einführung der Entwurfsregelung an die Grenzen des § 107 Abs. 6 NKomVG gebunden sein werden, also Aufgaben der Personalverwaltung nur an juristische Personen des öffentlichen Rechts, die der Aufsicht des Landes unterstehen, übertragen dürfen (§ 107 Abs. 6 Satz 2 NKomVG) bzw. nur diese mit der Wahrnehmung solcher Aufgaben beauftragen dürfen (§ 107 Abs. 6 Satz 4 NKomVG). In diesem Zusammenhang hat das MI allerdings darauf hingewiesen, dass § 107 Abs. 6 NKomVG der Inanspruchnahme von Privaten als Verwaltungshelfer nicht entgegenstehe, soweit es lediglich um Hilfstätigkeiten gehe, die wegen ihres vorbereitenden Charakters nicht als Aufgabe der Personalverwaltung im Sinne des § 107 Abs. 6 NKomVG anzusehen seien (z. B. Aktenvernichtung oder vorbereitendes Einscannen von Papierakten).

Satz 2 des Entwurfs soll zur Verbesserung der Rechtssystematik in den Absatz 2/1 verlagert werden.

Ebenfalls zur Verbesserung der Rechtssystematik empfiehlt der Ausschuss in Satz 3 die Regelung aus Absatz 3 des Entwurfs aufzunehmen. Die Absätze sollen dadurch eine sinnvolle Struktur erhalten: Absatz 1 enthält die materiellen Voraussetzungen, Absatz 2 das einzuhaltende Verfahren bei

der Einführung der Auftragsdatenverarbeitung (und der Unterauftragserteilung), Absatz 2/1 enthält die anschließenden Pflichten der personalverwaltenden Behörde. In Satz 3 wird durch die Verschiebung die im Entwurf unklare Bezugnahme auf die „Erfüllung von Aufgaben nach Absatz 1 Satz 1“ entbehrlich. Anstelle des „Verantwortlichen“ soll - wie in Satz 1 - die personalverwaltende Behörde genannt werden. Um auch in Satz 3 klarzustellen, dass die Aufgaben nicht übertragen werden (siehe oben), soll der Wortlaut an Artikel 28 Abs. 3 Satz 2 Buchst. g DSGVO („Erbringung von Verarbeitungsleistungen“) angelehnt werden. Nach Mitteilung des MI soll die Regelung nur bei der erstmaligen Beauftragung einer nicht öffentlichen Stelle Anwendung finden. Bei einer weiteren (Unter-)Auftragsverarbeitung durch den Auftragsverarbeiter (vgl. Artikel 28 Abs. 4 DSGVO) bedürfe es dieser Einschränkung nicht, zumal die Unterauftragsverarbeitung der Genehmigung der personalverwaltenden Behörde bedürfe (und nach Absatz 2 der Genehmigung der obersten Dienstbehörde).

Zu Absatz 2/1:

Die Empfehlung enthält die Regelung aus Absatz 1 Satz 2 des Entwurfs. Im Wortlaut soll klargestellt werden, dass der personalverwaltenden Behörde im Falle einer Unterauftragserteilung die Kontrolle auch gegenüber dem weiteren Auftragsverarbeiter i. S. d. Artikels 28 Abs. 4 DSGVO obliegt.

Zu Absatz 3:

Die Entwurfsregelung soll in Absatz 1 Satz 3 verlagert und hier gestrichen werden (vgl. im Übrigen die dortige Erläuterung).

(Verteilt am 22.10.2019)