

DR. THILO WEICHERT, WAISENHOFSTR. 41, 24103 KIEL

An die Präsidentin des
Niedersächsischen Landtags
- Landtagsverwaltung -
Hannah-Arendt-Platz 1
30159 Hannover

Kiel, den 26.04.2018

**Stellungnahme des
Netzwerks Datenschutzexpertise**
gegenüber dem Niedersächsischen Landtag
zu den **Vorschlägen zur Änderung des Niedersächsischen Datenschutzrechts**

insbesondere zum

1. Entwurf eines Gesetzes zur Neuordnung des niedersächsischen Datenschutzrechts –
Gesetzentwurf der Landesregierung, v. 28.03.2018, Nds. LT-Drs. 18/548
2. Änderungsvorschlag der Fraktionen der SPD und der CDU, Mail vom 03.04.2018
3. Antrag der Fraktion Bündnis 90/Die Grünen „Landesregierung darf nicht die Chance auf
einen besseren Datenschutz verspielen!“ v. 20.02.2018, Nds. LT-Drs. 18/352.

Sehr geehrte Frau Präsidentin,
sehr geehrte Damen und Herren Abgeordnete,

vielen Dank für die Möglichkeit der Stellungnahme zu den o. g. Landtagsanträgen. Deren
Hintergrund ist die Anpassung des niedersächsischen Datenschutzrechts an das
europäische Recht, das vom 25.05.2018 an anwendbar sein wird, insbesondere die
- Europäische Datenschutz-Grundverordnung, Verordnung (EU) 2016/679 v. 27.04.2016,
ABl. L 119 v. 04.05.2016, S. 1 ff. (DSGVO) und die
- Europäische Datenschutzrichtlinie Justiz/Inneres, Richtlinie (EU) 2016/680 v. 27.04.2016,
ABl. L 119 v. 04.05.2016, S. 89 ff. (DSRI-JI).

Wegen der äußerst umfangreichen Anträge beschränkt sich die vorliegende Stellungnahme
auf besonders hervorzuhebende Aspekte.

1 Allgemeines

Es ist zu begrüßen, dass der Regierungsvorschlag zur **Bezeichnung der Datenschutz-
Grundverordnung** deren Namen verwendet und nicht, so wie dies der Bundesgesetzgeber
tut, die bürokratische Bezeichnung „Verordnung (EU) 2016/679“. Dadurch wird der ohnehin
schon komplexe Rechtstext leichter verständlich und auch für Laien eher nachvollziehbar.

Dieser positive Ansatz wird nicht beim „Änderungsvorschlag zum Gesetz zur Neuordnung
des niedersächsischen Datenschutzrechts“ fortgeführt. Der Änderungsvorschlag versäumt
es, für die „Richtlinie (EU) 2016/680“ einen populär verständlichen Begriff zu verwenden. Es
wird angeregt, anstelle dieser formalen Bezeichnung die Worte „**Datenschutzrichtlinie
Justiz/Inneres**“ (DSRI-JI) zu verwenden.

Die Vorschläge zielen darauf ab, den **rechtlichen Anforderungen** der DSGVO und der DSRI-JI zu genügen und haben die Bürgerinnen und Bürger als Adressaten nicht erkennbar im Blick. Es bestehen Defizite bei der Verständlichkeit und der Anwendungsfreundlichkeit. Es ist anzuerkennen, dass der Entwurf an bisher geltende Regelungen anknüpft, soweit diese durch das EU-Recht nicht obsolet wurden. Doch hätte auf Regelungen verzichtet werden können, die auch in der Vergangenheit keine praktische Relevanz hatten.

Es ist zu bedauern, dass die Gesetzesvorschläge, ebenso wie sämtliche sonstigen bekannten Entwürfe zur Anpassung bzw. Umsetzung des europäischen Datenschutzrechts **keinerlei innovative Elemente** enthalten und sich auf für notwendig erachtete Regelungen beschränken. Seit den 70er Jahren war das deutsche Landesdatenschutzrecht international Vorreiter, etwa mit dem weltweit ersten Datenschutzgesetz von Hessen im Jahr 1970 oder mit dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH) aus dem Jahr 2000.

Derartige innovative Elemente wären die Zusammenführung des digitalen Grundrechtsschutzes, der sich nicht nur auf das Grundrecht auf Datenschutz beschränkt, sondern sich auf weitere Grundrechte und deren demokratische Funktion beziehen sollte und damit u. a. auch die Aspekte der Informationsfreiheit oder der Algorithmenkontrolle erfasst. Ein geeigneter Diskussionsansatz besteht unter dem Titel „**Charta der Digitalen Grundrechte** der Europäischen Union“.¹

Scharf kritisiert werden muss, dass die Einfügung eines zweiten Teils des NDSG zur Umsetzung der DSRI-JI in einem **Fraktionsänderungsantrag** erfolgt. Diese Vorgehensweise beeinträchtigt die öffentliche demokratische Diskussion, die bei einer Gesetzgebung von dieser Bedeutung notwendig ist.

Es besteht für die Umsetzung des europäischen Datenschutzrechts **kein zwingender zeitlicher Druck**. Seit zwei Jahren ist bekannt, dass und was wegen der europarechtlichen Vorgaben an mitgliedstaatlichen Änderungen nötig ist. Erfolgt bis Mai 2018 insofern keine gesetzliche Umsetzung, so gelten die bisherigen Regelungen weiter, soweit sie nicht durch höherrangiges europäisches Recht verdrängt werden. Eine kurzfristige Rechtsunsicherheit wegen verzögerter Umsetzung ist einem Zustand vorzuziehen, bei dem wegen europarechtlicher oder verfassungsrechtlicher Verstöße langfristig Rechtsunsicherheit besteht.

2 Zum Vorschlag eines neuen Niedersächsischen Datenschutzgesetzes (NDSG-E), Art. 1, LT-Drs. 18/548

Zu § 1 Abs. 2 NDSG-E: Die **Ausnahme der Staatsanwaltschaften** von der allgemeinen Datenschutzregulierung war bisher in Deutschland nicht üblich und wird durch das EU-Recht nicht gefordert. Die Ausnahme geht davon aus, dass der Staatsanwaltschaft eine den Richtern entsprechende Unabhängigkeit zukäme, was in Deutschland nicht der Fall ist. Vielmehr sind die Staatsanwaltschaften in die allgemeine Justizverwaltung integriert, auch wenn sie im Rahmen von strafrechtlichen Ermittlungen und gerichtlichen Verfahren tätig werden. Durch die Ausnahme wird ein Sonderrecht geschaffen, das dazu führen wird, dass Staatsanwaltschaften den Datenschutz in Zukunft weniger ernst nehmen.

Zu § 6 Abs. 2 NDSG-E: Die **Zweckänderungsregelungen** in den Nrn. 1-5 knüpfen tatbestandlich jeweils nur an der Erforderlichkeit für bestimmte andere Zweck an und verlangen keine zusätzliche Angemessenheitsprüfung in Bezug auf Eingriffstiefe und konkret verfolgtem Zweck. Dieses Defizit lässt sich allenfalls durch eine verfassungskonforme

¹ <https://digitalcharta.eu/>.

Auslegung beheben. Vorzuziehen wäre eine ausdrückliche Klarstellung, dass in jedem Fall eine Verhältnismäßigkeitsprüfung erforderlich ist.

Zu § 7 NDSG-E: Die Regelung zu **automatisierten Verfahren und gemeinsamen Dateien** enthält eine allgemeine Abwägungsregelung ohne Konkretisierungen und ohne Nennung von Garantien und Schutzmaßnahmen. Sie bleibt sogar hinter Art. 26 DSGVO zurück, der eine „Vereinbarung in transparenter Form“ verlangt. Es bestehen in anderen Landesgesetzen erheblich präzisere und rechtsstaatlich vertretbarere Lösungen wie z. B. in § 8 Landesdatenschutzgesetz (LDSG) Schleswig-Holstein (SH), das Aussagen zur Kontrolle, der Funktion zentraler Stellen, die Art der Protokollierung, der Dokumentation und der Vereinbarung enthält.

Zu § 13 NDSG-E insgesamt: Die **Forschungsregelung** beschränkt sich darauf, wissenschaftliche Forschung durch öffentliche Stellen in Niedersachsen zu normieren. Sie setzt nicht die in Art. 5 Abs. 1 lit. b DSGVO vorgesehene Forschungsprivilegierung um. Sie gibt auch keine Antwort darauf, dass Forschung oft gemeinsam von öffentlichen und nicht-öffentlichen Stellen sowie von Stellen in verschiedenen Bundesländer oder EU-Staaten durchgeführt wird. Anstelle der Fortsetzung des Regelungschaoses zur Forschung ist es wünschenswert, über einen Bund-Länder-Staatsvertrag in Deutschland ein einheitliches Forschungsrecht festzuschreiben, das auch der Sensitivität von Daten nach Art. 9 Abs. 1 DSGVO gerecht wird. Die geplante Regelung berücksichtigt nicht, dass etwa im medizinischen Bereich wichtige Forschungsprojekte nur durchgeführt werden können, wenn eine Offenbarungsbefugnis zu Berufsgeheimnissen, also z. B. zur ärztlichen Schweigepflicht, mit entsprechenden Sicherungen vorgesehen ist (vgl. Art. 9 Abs. 3 DSGVO). So behindert die geplante Regelung weiterhin unangemessen die Durchführung medizinischer Forschungsprojekte (Art. 5 Abs. 3 GG, Art. 13 Europäische Grundrechte-Charta - GRCh). Nur über eine einheitliche bundesweite Regulierung können die in Art. 89 DSGVO geforderten praktikablen Garantien realisiert werden. Ein problemadäquater Vorschlag für eine Bund-Länder-Regulierung unter Berücksichtigung von Berufsgeheimnissen zumindest für medizinische Forschungsprojekte liegt seit September 2017 vor und sollte von Bund und Ländern umgehend in Angriff genommen werden.²

Zu § 13 Abs. 4 NDSG-E: Die Verpflichtung zur ausschließlichen **Verarbeitung in einem konkreten Forschungsvorhaben** und der Anzeige bei der Datenschutzbehörde berücksichtigt nicht, dass Forschungsdaten inzwischen oft in Registern für eine Vielzahl unterschiedlicher Forschungsvorhaben bereit gestellt werden und im Interesse des wissenschaftlichen Fortschritts genutzt werden müssen. Die vorgesehene Anzeige jeder Übermittlung (!) hat in der Vergangenheit keinen adäquaten Schutz gewährleistet und stellt eine unverhältnismäßige bürokratische Anforderung an Forschende ohne einen erkennbaren Nutzen dar.

Zu § 13 Abs. 5 NDSG-E: Es ist zwingend eine Norm nötig, die eine Begründungs- und Dokumentationspflicht bei einer **Nichtumsetzung der Betroffenenrechte** im Bereich der Forschung vorsieht. Anderenfalls wird die Regelung zu einer pauschalierten Verweigerung der Betroffenenrechten führen.

Zu § 14 NDSG-E: Es wird vorgeschlagen, über den Bereich der öffentlichen Stellen hinausgehend eine **Meldepflicht von Videoüberwachung** im öffentlichen Raum auf einem Internet-Portal vorzusehen um zu gewährleisten, dass die Kombination von Videoüberwachung verschiedener Stellen nicht zur einer Totalüberwachung des öffentlichen Raums ausartet, und um die öffentliche Transparenz zu stärken. Es bestehen Zweifel, dass die in Abs. 3 vorgesehene Beratung zur Videoüberwachung durch die Datenschutzbehörde mit dem dort vorhandenen Personal wirksam bewerkstelligt werden kann.

² <https://www.netzwerk-datenschutzexpertise.de/dokument/medizinische-forschung-und-datenschutz>.

Zu § 17 NDSG-E: Die in Abs. 1 Nr. 1 und 2 vorgesehenen **Schutzmaßnahmen für sensitive Daten** enthalten teilweise fragwürdige Wiederholungen europäischer Regelungen: Die Protokollierungspflicht (Nr. 1) ist in Art. 5 Abs. 2 DSGVO geregelt und erstreckt sich auf jede Form der personenbezogenen, nicht nur der sensitiven Datenverarbeitung. Die in Nr. 2 vorgesehene Beschränkung und Dokumentation der Zugriffsbefugnisse ergibt sich – auch für jede Art der Verarbeitung – schon aus Art. 5 Abs. 1 lit. c, 32 Abs. 1 lit. b, d DSGVO. Die Regelungen sind inhaltlich unschädlich, können aber den falschen Eindruck erwecken, dass die Anforderungen nur bei sensibler Verarbeitung beachtet werden müssten. Entsprechendes gilt für die in Abs. 2 Nr. 4 erwähnte Verschlüsselung, die schon in Art. 32 Abs. 1 lit. a DSGVO zur Pflicht gemacht wird.

Zu § 18 Abs. 1 NDSG-E: Im Interesse einer europäischen sprachlichen Vereinheitlichung wäre es sinnvoll, „die von der oder dem Landesbeauftragten geleitete Behörde“ wie in der DSGVO (z. B. Art. 51) einfach „Aufsichtsbehörde“ oder „**Datenschutzaufsichtsbehörde**“ zu benennen. Für den unerfahrenen Rechtsanwender würde dadurch erkennbar, dass es sich um das Selbe handelt.

Zu § 18 Abs. 3, 4 NDSG-E: Es ist zu begrüßen, dass für die oder den **Landesbeauftragten** keine Altersgrenze vorgesehen ist. Es fehlt bzgl. der Bestellung eine Regelung, die, wie in Art. 53 Abs. 1 DSGVO gefordert, ein transparentes Verfahren für die Auswahl und Wahl vorsieht. Der Hinweis auf die Wahl durch das Parlament genügt insofern nicht. Trotz der relativ langen Amtszeit mit einmaliger Wiederwahlmöglichkeit sollte auf die Beschränkung der Wiederwahl im Interesse einer höchstmöglichen Qualifikation verzichtet werden.³

Zu § 20 Abs. 2 S. 2, 4 NDSG-E: Die Regelung, wonach die Aufforderung zur Stellungnahme gegenüber einem Verantwortlichen in jedem Fall mit einer **Unterrichtung der Rechts- oder Fachaufsichtsbehörde** verbunden ist, ist nicht sinnvoll. Zum einen kann hierin eine Beeinträchtigung der Unabhängigkeit der Aufsichtsbehörde gesehen werden (vgl. Art. 52 DSGVO). Problematisch ist die Regelung auch wegen des damit verknüpften bürokratischen Aufwands für die Rechts- und Fachaufsicht. Es sollte davon ausgegangen werden, dass verantwortliche öffentliche Stellen auch ohne Fach- und Rechtsaufsicht in der Lage sind, ihren datenschutzrechtlichen Pflichten zu genügen.

3 Zu weiteren Änderungen des Landesrechts, Art. 2, 12 u. 13, LT-Drs. 18/548

Zu § 3a Nr. 1 lit. b NdsArchivG-E: Das Angebot der Archivierung darf nicht zu einer unbeschränkten **Verlängerung der Speicherfrist** führen. Insofern ist die Regelung zu begrüßen. Wegen der prekären Personalsituation im Archivbereich sollte aber eine Regelung aufgenommen werden, wonach auf Bitte des Landesarchivs die Frist von 6 Monaten verlängert werden kann.

Zu § 36 PsychKG-E und § 21c MaßregelvollzugsG: Es ist grundsätzlich nicht zu beanstanden, dass in der Regelung eine **Auskunftsverweigerung zum „Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen“** vorgesehen ist. Es sollte aber im Gesetz klargestellt werden, dass die Auskunft an einen Vertreter oder eine Vertrauensperson des Betroffenen zu erteilen ist, wenn so die Gefahr der Selbst- oder Fremdgefährdung nicht besteht.

4 Zum Änderungsvorschlag der Fraktionen der CDU und der SPD

³ Dazu ausführlich Netzwerk Datenschutzexpertise, Zum Auswahlprozess von Datenschutzbeauftragten als Leitung der Aufsichtsbehörden, 03.02.2017, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_auswahlblfdi6.pdf.

Zu § 26 NDSG-E: Die Regelung zur Unterscheidung verschiedener Kategorien betroffener Personen greift Art. 6 DSRI-JI auf und wiederholt diesen ohne inhaltliche Präzisierungen. Die Regelung leidet unter dem gleichen Defizit wie § 72 BDSG. Die **Unterscheidung von Personenkategorien** macht nur Sinn, wenn sich hieran unterschiedliche Schutzmaßnahmen erstrecken. Die reine Benennung der verschiedenen Kategorien genügt nicht den europarechtlichen Vorgaben. Sollen spezielle Rechtsfolgen in spezifischem Recht geregelt werden, so ist hierauf im Interesse der Rechtsklarheit hinzuweisen. Ein Verweis hierauf in der Begründung genügt nicht.

Zu § 27 NDSG-E: Auch bzgl. der Unterscheidung zwischen **Tatsachen und persönlichen Einschätzungen** wird europarechtswidrig offen gelassen, worin außer der Benennung dieser Kategorien der Unterschied liegen soll. In dem ebenso defizitären § 73 BDSG wird zumindest darauf hingewiesen, dass feststellbar sein muss, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen. Ein Bezug zu § 32 Abs. 1 S. 3 NDSG-E, der den Datenschutz beim Übermittlungsempfängern sichern soll, sollte aufgenommen werden.

Zu § 28 Abs. 4 NDSG-E: Es kann nicht dem Verantwortlichen überlassen werden, wann **regelmäßige Prüfungen der Erforderlichkeit** von Daten zu erfolgen haben. Entgegen der Gesetzesbegründung ist die Regelung keine hinreichende verfahrensrechtliche Vorkehrung zur Sicherstellung der Fristwahrung nach Art. 5 S. 2 DSRI-JI. Es bedarf zumindest landesweit einheitlicher Vorgaben. Sollen diese nicht schon per Gesetz festgelegt werden, so ist eine verbindliche Vorgabe durch die oberste Landesbehörde nötig. Darüber hinaus sind Vorgaben nötig, die die Umsetzung der Prüfpflichten gewährleisten.

Zu § 29 NDSG-E: Die Regelungen in den Absätzen 1 und 2, wonach **automatisierte Entscheidungen** nur auf einer Rechtsvorschrift mit geeigneten Schutzvorkehrungen erlaubt sind, sind überflüssig, da dies schon in Art. 11 DSRI-JI geregelt ist und die Absätze selbst keine Erlaubnisnormen erhalten und wohl auch nicht enthalten sollen. Absatz 3 ist ebenso überflüssig aber unschädlich, da das Diskriminierungsverbot bzgl. besonderer Datenkategorien schon nach Unionsrecht besteht.

Zu § 31 NDSG-E: Die Regelung zum **automatisierten Abrufverfahren**, die sich auf eine Verweisung auf § 7 beschränkt, ist ohne rechtliche Wirkung, da dem § 7 kein materieller oder auch nur wirkungsvoller prozessualer Regelungsgehalt innewohnt (s. o.).

Zu § 32 Abs. 4 S. 2 NDSG-E: Die Regelung, wonach die normativen **Bedingungen für die Datenverarbeitung** (z. B. eine enge Zweckfestlegung oder Nutzungsbeschränkungen) durch einen Hinweis per Kennzeichnung umgesetzt werden können, verstößt gegen den Grundsatz des Privacy by Design (Art. 20 DSRI-JI). Es muss zumindest festgelegt werden, dass, soweit dies möglich ist, die Bedingungen technisch umgesetzt werden. Die allgemeinen Regelungen in § 34 Abs. 2, Abs. 3 NDSG-E genügen insofern nicht.

Zu § 33 NDSG-E: **Einwilligungen** sind im Anwendungsbereich der DSRI-JI nicht vorgesehen, insofern ist die Regelung zumindest befremdlich. Auch wenn diese nicht absolut ausgeschlossen sein sollen, so können diese nur in Ausnahmesituationen wirksam werden, da die Voraussetzungen für freiwillige Einwilligungen im Bereich von Strafverfolgung und Justiz wegen des regelmäßig bestehenden Zwangscharakters der hoheitlichen Maßnahmen nicht vorliegen. Nicht akzeptabel ist die Regelung in Abs. 4 S. 3, wonach nur auf die Verlangen des Betroffenen in jedem Fall eine Belehrung über die Folgen der Verweigerung der Einwilligung erfolgen muss.

Zu § 35 Abs. 1 NDSG-E: Die Regelung enthält eine unsystematische Aneinanderreihung von Maßnahmen des **technischen Datenschutzes** aus dem alten Recht sowie Schutzziele, wie sie z. B. in Art. 32 DSGVO normiert sind. Sie sind teilweise technisch überholt (z. B. Nr.

1 – Zugangskontrolle – hatte Relevanz für Großrechnertechnologie) oder redundant (z. B. die Nrn. 5-7 – Zugriffs-, Übertragungs- und Eingabekontrolle – sind in Abs. 2 – Protokollierung – geregelt). An Stelle dessen sollten die wesentlichen Schutzziele benannt werden: Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Intervenierbarkeit und Nichtverkettbarkeit.

Zu § 43 Abs. 2 S. 2 NDSG-E: Die Regelung kann nur dahingehend verstanden werden, dass das Recht von Beschäftigten einer öffentlichen Stelle, die Datenschutzaufsichtsbehörde einzuschalten grds. nur unter „**Einhaltung des Dienstweges**“ zulässig sein soll. Diese Einschränkung beeinträchtigt unverhältnismäßig das Petitionsrecht und verhindert faktisch oft die Offenlegung von Missständen durch sog. Whistleblower gegenüber der zuständigen Datenschutzaufsicht.

Zu § 52 Abs. 1 S. 2 NDSG-E: Die Regelung, wonach keine Berichtigungsanspruch bei „**Aussagen und Beurteilungen**“ nötig ist, die inhaltlich falsch sind, ist missverständlich. Es bedarf zumindest einer Ergänzung, die dazu verpflichtet auf den Umstand hinzuweisen, dass es sich um eine „Aussage oder Beurteilung“ handelt.

Zu § 55 Abs. 1 S. 3 NDSG-E: Der Verweis auf eine **Vertretungsmöglichkeit** „entsprechend Artikel 80 Datenschutz-Grundverordnung“ führt in die Irre: Art. 80 DSGVO sieht die Vertretung durch Verbraucherschutzverbände oder z. B. Beschäftigtenvertretungen vor. Entsprechende Einrichtungen gibt es im Bereich Justiz/Inneres nach nationalem Recht bisher nicht. Zudem bezieht sich Art. 80 DSGVO auf den Rechtsschutz, § 32 NDSG-E auf die Behördenanrufung. Soll mit der Regelung ein Verbandsbeschwerderecht eingeführt werden, so sollte dies ausdrücklicher geregelt werden. Wenn nicht, so sollte der Satz gestrichen werden, um den Eindruck zu vermeiden, dass sonstige Betroffenenvertretungen, etwa durch eine Vertrauensperson oder einen Rechtsanwalt, unzulässig wären.

Zu § 57 Abs. 3 NDSG-E: Die Regelung, dass eine Datenschutzkontrolle von Strafverfolgungsbehörden **erst nach Abschluss des Strafverfahrens** zulässig ist, ist verfassungs- und europarechtswidrig. Eine derartige Einschränkung ist in Art. 8 Abs. 3 GRCh nicht vorgesehen. Sie widerspricht der Funktion der unabhängigen Datenschutzkontrolle, wie sie vom BVerfG gerade im Strafverfolgungsbereich zugesprochen wird (BVerfG U. v. 24.04.2013 – 1 BvR 1215/07, Rn. 207 ff.). Die strafgerichtliche Rechtskontrolle beginnt erst mit der Eröffnung des Strafverfahrens und bezieht sich nicht auf eine Kontrolle der Rechtmäßigkeit der Datenverarbeitung im Rahmen der Ermittlung, sondern behandelt diese Frage allenfalls als eine prozessuale Vorfrage. Absatz 3 S. 1, wonach die Regelung auch für die Strafvollstreckung gelten soll, macht keinen Sinn, weil im Rahmen des Strafvollstreckung regelmäßig überhaupt keine gerichtliche Kontrolle stattfindet und von einer Unabhängigkeit der Strafvollstreckungsbehörden nicht im Ansatz gesprochen werden kann. Der Absatz ist ersatzlos zu streichen.

Zu § 57 Abs. 5 S. 2 NDSG-E: Die Regelung beschränkt sich darauf, der Aufsichtsbehörde als „**wirksame Abhilfebefugnis**“ i. S. v. Art. 47 Abs. 2 DSRI-JI eine Beanstandungsmöglichkeit einzuräumen. Die von Art. 47 Abs. 2 lit. b und c vorgesehenen Befugnisse zum Erlass von Anweisungen sowie von Verarbeitungseinschränkungen und -verboten sieht der Entwurf nicht vor. Es gibt auch keine sonstigen Maßnahmen, die den vorgesehenen Beanstandungen die erforderliche Wirksamkeit verleihen könnten. Die Rechtfertigung der Kontrollbeschränkung damit, dass „das Bedürfnis nach ständiger Verfügbarkeit von zur Datenverarbeitung genutzten Datenverarbeitungssystemen“ durch eine „Letztentscheidungsbefugnis“ der Datenschutzaufsicht gefährdet würde, ist schlichtweg falsch, da in einem Rechtsstaat wie Deutschland diese „Letztentscheidungsbefugnis“ den Gerichten zusteht. Es ist zudem realitätsfremd, dass die Datenschutzaufsicht erforderliche Verarbeitungen verbieten würde. Es ist aber nötig, dass bei unzulässigen Verarbeitungen Mittel zur Beseitigung des Rechtsverstoßes gegeben werden. Es ist leider Erfahrung und

Praxis, dass die Exekutive Beanstandungen von Aufsichtsbehörden ignoriert, selbst wenn diese z. B. dem Parlament mitgeteilt werden. Die Beschränkung der Abhilfebefugnisse verstößt damit gegen Art. 47 Abs. 2 DSRI-JI und ist europarechtswidrig. Es sind zusätzlich zur Warnungs- und Beanstandungsbefugnis wirksame Abhilfebefugnisse vorzusehen.

4 Zum Entschließungsantrag der Fraktion Bündnis 90/Die Grünen v. 20.02.2018, LT-Drs. 18/352

Der Antrag enthält in Nr. 1 die richtige Forderung, bei den Ausnahmen zu den Betroffenenrechten europarechtskonform vorzugehen und in den Nrn. 2, 3 die Öffnungsklauseln zur Erweiterung der Betroffenenrechte zu nutzen. Diese Forderungen wie auch die weiteren Punkte richten sich an die Landesregierung im Rahmen des Gesetzgebungsverfahrens. Mit der Vorlage des Gesetzentwurfes LT-Drs. 18/548 kam die Landesregierung dem formal nach.

Hinsichtlich der inhaltlichen Bewertung bestehen gegen den Vorschlag der Landesregierung teilweise gravierende verfassungsrechtliche wie europarechtliche Bedenken, die oben dargestellt werden. Diese müssen zu Änderungen im Rahmen des Gesetzgebungsverfahrens führen. Dies gilt z. B. auch für die „klar und deutlich“ geregelten, aber europa- und verfassungsrechtlich unzulässigen Beschränkungen der Befugnisse der Datenschutzaufsicht (Nr. 7 des Antrags). Im Hinblick auf die Anwenderfreundlichkeit und Praxisorientierung (Nr. 6 des Antrags) weisen die vorgelegten Regelungsvorschläge Defizite auf.

Die Themen „Online-Durchsuchung und Quellen-Telekommunikationsüberwachung“ (Nr. 8 des Antrags) werden in dem vorliegenden Entwurfspaket nicht adressiert, wohl aber in einem separat geplanten Paket zur Änderung des Niedersächsischen Sicherheits- und Ordnungsgesetzes bzw. einer Neuregulierung in einem Niedersächsischen Polizeigesetz. Die komplexen verfassungsrechtlichen Anforderungen an die angesprochenen Maßnahmen sind in diesem Kontext zu berücksichtigen.

Für Rückfragen stehe ich zur Verfügung.

Mit freundlichen Grüßen

Dr. Thilo Weichert