Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/508

Alle Abg

LDI NRW, Postfach 20 04 44, 40102 Düsseldorf
Der Präsident
des Landtags Nordrhein-Westfalen
Platz des Landtags 1
40221 Düsseldorf

per E-Mail an: anhoerung@landtag.nrw.de

Aktenzeichen
bei Antwort bitte angeben
L2

Telefon 0211 38424-
Fax 0211 38424-10

Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU - NRWDSAnpUG-EU), Gesetzentwurf der Landesregierung, Drucksache 17/11981

Anhörung des Hauptausschusses am 19. April 2018

Ihr Schreiben vom 19. März 2018, Ihr Zeichen: I.1 / A 05

Sehr geehrter Herr Präsident,
sehr geehrte Damen und Herren Abgeordnete,

für die Gelegenheit zur Stellungnahme danke ich. Das große Rechtsreformprojekt, bei dem die Landesgesetze an das neue EU-Recht anzupassen sind, begleite ich gerne. Die Anpassung stellt eine besondere Herausforderung dar, weil das Datenschutzrecht Querschnittscharakter hat und die Regelungsspielräume im Rahmen der der europarechtlichen Vorgaben nicht immer klar umgrenzt sind.

Als Ergebnis der vorherigen Beteiligung wurden meine Änderungsvorschläge bereits im Vorfeld an einigen Stellen des Gesetzentwurfs berücksichtigt. Dennoch verbleiben noch zahlreiche, zum Teil sehr bedeutsame Punkte, an denen aus meiner Sicht Änderungsbedarf besteht.

Dienstgebäude und Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle Poststraße

A Allgemeine Vorbemerkungen

Mit der grundsätzlichen Zielrichtung des Entwurfs stimme ich überein, für den Anwendungsbereich der Verordnung und der Richtlinie einen möglichst einheitlichen Rechtsrahmen zu schaffen, sowie dort, wo die Verordnung (EU) 2016/679 (im Folgenden: DSGVO) Regelungsspielräume lässt, das bisherige Datenschutzniveau des Landes aufrechtzuerhalten (s. die Ausführungen unter „B Lösung“ auf Satz 2 des Vorblatts). Ich begrüße auch ausdrücklich, dass die Geltung der Vorschriften der DSGVO grundsätzlich auch auf öffentliche Stellen (mit Ausnahme der Verfassungsschutzbehörde) und Verarbeitungsformen erstreckt werden soll, die nicht unter den Anwendungsbereich nach Art. 2 DSGVO zu fassen sind, soweit sie bisher unter das DSG NRW fallen. Ferner bestätige ich, dass, wie unter dem Abschnitt „D Kosten“ erwähnt wird, durch verschiedene Neuregelungen der DSGVO ein Aufgabenzuwachs für die LDI entsteht, der weiteren Personalbedarf zur Folge haben kann.

Soweit das in der Entwurfsbegründung postulierte Ziel der Aufrechterhaltung des bisherigen Datenschutzniveaus aus meiner Sicht nicht hinreichend konsequent verfolgt wird, nehme ich dazu mit Anmerkungen zu den jeweiligen Vorschriften Stellung. Wegen ihrer besonderen Bedeutung weise ich vorab auf folgende Regelungen des Entwurfs hin:

1. Die vorgesehene Regelung der Videoüberwachung (§ 20 d. E.) würde zu einer erheblichen Absenkung des bisherigen Datenschutzstandards führen. Sie wird den verfassungsrechtlichen Anforderungen nicht gerecht und bedarf daher einer grundsätzlichen Überarbeitung. Nach der Verbändeanhörung sind substanzielle Erweiterungen des Tatbestandes vorgenommen worden, die zu einer fast unbegrenzten Ausweitung möglicher Einsatzszenarien führen würden. Die neu aufgenommenen Zwecke sind zu weit und zu unbestimmt, um eine verfassungsgemäße Grundlage für diesen erheblichen Eingriff darstellen zu können. Daher würde es mit § 20 d. E. an einer gesetzlichen Grundlage fehlen, „aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht“ (vgl. BVerfGE 65, 1 ff, 44).

Die Ausweitung der Befugnisse würde in der Praxis zu mehr Videoüberwachung führen. Dies hätte relevante Auswirkungen auf das gesellschaftliche Klima: Freiheitsgefühl und Unbefangenheit im öffentlichen Raum würden beeinträchtigt. Von einer Videoüberwachung mit großer Streubreite wären zahlreiche Personen betroffen, die in keiner Beziehung zu einem etwaigen Fehlverhalten Einzelner stehen, so dass damit eine unverhältnismäßig große Eingriffsintensität verbunden wäre. Der ausufernden und flächendeckenden Ausweitung der Installation von Videokameras gilt es im Übrigen auch deshalb nachdrücklich entgegenzuwirken, damit keine Überwachungsinfrastruktur geschaffen werden kann, die auch eine Verarbeitung der Daten zu weiteren Zwecken ermöglichen würde. Angesichts der rasanten technischen Fortentwicklung sind hier vielfältige Szenarien vorstellbar, wie z. B. der Einsatz von Gesichtserkennungssoftware und die Erstellung von Bewegungsprofilen. Auch wenn dies derzeit noch nicht beabsichtigt ist, würden mit der stark ausgeweiteten Installation von Kameras jedenfalls die Voraussetzungen dafür bereits geschaffen. Auch deshalb muss die Videoüberwachung auf konkret abgegrenzte Zwecke beschränkt bleiben.

2. Eine gravierende Verschlechterung des bisherigen Datenschutzniveaus droht, wenn die ebenfalls nach der Verbändeanhörung neu eingefügte Beschränkung meiner Untersuchungsbefugnisse gegenüber Berufsgeheimnisträgern oder deren Auftragsverarbeitern Eingang in das Gesetz findet (§ 27 Absatz 3 d. E.). Gerade im Bereich der Tätigkeit von Berufsgeheimnisträgern werden häufig besonders schützenswerte Daten, wie zum Beispiel Gesundheitsdaten, verarbeitet. Eine gesonderte Regelung für Beschränkungen der Aufsicht bei Berufsgeheimnisträgern ist weder notwendig noch verhältnismäßig, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Der Gesetzgeber sollte daher keine derartige Regelung treffen.

3. Eine deutliche Minderung des bisherigen Schutzniveaus droht auch durch die im Entwurf (§ 17) vorgeschlagene Regelung zur Datenverarbeitung im Rahmen von Forschungsvorhaben: Soweit sie die Forschung mit besonderen Kategorien personenbezogener Daten – also z. B. Gesundheitsdaten, biometrische Daten etc. – einschließt, ist die vorgesehene Regelung unzulänglich und verfassungsrechtlich bedenklich. Die Einbeziehung dieser besonders schützenswerten Da-

ten in die allgemeine Rechtsgrundlage für Forschungsvorhaben lässt eine Abwägung der betroffenen Grundrechte vermissen. Das bisherige Schutzniveau, wie es zum Beispiel in den Garantien des geltenden § 6 GDSG NRW zum Ausdruck kommt, muss aufrechterhalten werden.

Teilweise verstehe ich die Regelungsspielräume oder auch Regelungsaufträge, die die DSGVO dem nationalen Gesetzgeber lässt, anders, als die Landesregierung: Allgemeine Regelungen, unter welchen Voraussetzungen die Rechte der betroffenen Personen beschränkt werden dürfen (s. Satz 2 zweiter Spiegelstrich des Vorblatts, s. §§ 11ff.) sind nach meiner Auffassung der DSGVO vorbehalten. Der nationale Gesetzgeber darf nur die nach der DSGVO gegebenen Beschränkungsmöglichkeiten ausfüllen. Ähnlich verhält es sich mit den Voraussetzungen legitimer Zweckänderungen (Artikel 6 Absatz 4 DSGVO) und den Ausnahmeerlaubnissen zur Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9 Absatz 2 DSGVO). An Stelle der im Entwurf vorgesehenen allgemeinen Rahmenvorschriften sind hier spezifische nationale Gesetzgebungsmaßnahmen von Nöten (s. u. zu § 9 und zu §§ 15 ff. d. E.). Auch die neu aufgenommene Regelung zur literarischen und künstlerischen Betätigung entspricht aus meiner Sicht weder dem Regelungsauftrag noch dem Regelungsspielraum in Artikel 85 DSGVO (s. u. zu § 19 d. E.).

Ferner lässt der Entwurf Maßnahmen vermissen, die dem Ziel einer effektiven Umsetzung des europäischen Rechtsrahmens in den Mitgliedsstaaten zum Erfolg verhelfen. Vielmehr ist die Tendenz zu verzeichnen, die Aufsichtsbefugnisse gegenüber dem von der DSGVO grundsätzlich gewünschten Niveau im öffentlichen Bereich zu beschränken: So soll die Möglichkeit zur Verhängung von Geldbußen gegenüber öffentlichen Stellen gemäß Art. 83 Absatz 7 DSGVO ausgeschlossen werden, es sollen offenbar weder Vollstreckungsmöglichkeiten für Anordnungen und Verbote noch eine Aktivlegitimation i. S. d. Art. 58 Absatz 5 DSGVO vorgesehen werden, sondern die Möglichkeit, als Beklagte am Prozess beteiligt zu sein, soll genügen. Fraglich ist diesbezüglich, inwieweit es zu Klagen gegen die Maßnahmen der LDI NRW kommen wird, da offen ist, welche Rechtswirkung den Maßnahmen nach dem nationalen Verfahrensrecht zukommt. Das Fehlen derartiger Neuregelungen würde die effektive Umsetzung des europarechtlichen Rechtsrahmens im öffentlichen Bereich stark beeinträchtigen, wenn nicht sogar verhindern, und

das Ziel der DSGVO und der JI-RL, ein europaweit möglichst einheitliches Datenschutzniveau zu garantieren, konterkarieren (s. u. C 3). Auf die europarechtliche Pflicht zur wirksamen Durchsetzung der Ziele des EU-Gesetzgebers (Effizienzgrundsatz, vgl Ehman/ Selmayr, Datenschutz-Grundverordnung, 2017, Art. 58 Rn. 4) wird hingewiesen.

B Zu den einzelnen Vorschriften

Teil 1
Allgemeine Bestimmungen

Zu § 3 d. E.

1. § 3 Absatz 1 d. E. sollte nicht für Datenverarbeitungen nach Teil 3 d. E. gelten.

   Die Vorschrift gilt als „vor die Klammer gezogener" Allgemeiner Teil sowohl für Datenverarbeitungen nach der DSGVO als auch für Datenverarbeitungen, die unter die JI-Richtlinie (JI-RL) und Teil 3 des Entwurfs fallen. Für Datenverarbeitungen im Anwendungsbereich des Teils 3 des Entwurfs ist eine solche generalklauselartige Ermächtigungsgrundlage jedoch deutlich zu weit. Aufgrund der Vielzahl unterschiedlicher Formen der Datenverarbeitung mit je stark divergierenden, aber teils besonders hohen Eingriffsintensitäten in verschiedene Grundrechte enthält die JI-RL eine dezidierte Kasuistik von Anforderungen, die im Einzelfall zu erfüllen sind. Nach Art. 8 Absatz 2 JI-RL müssen die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung in jeder Ermächtigungsgrundlage angegeben werden. Diesen Anforderungen wird die Generalklausel des § 3 Absatz 1 d. E. keineswegs gerecht. Art. 8 Absatz 2 JI-RL sollte daher ausschließlich unmittelbar in den bereichsspezifischen Regelungen umgesetzt werden.

2. In § 3 sollte ein zusätzlicher Absatz aufgenommen werden, in dem der bisherige Regelungsgehalt des § 14 Absatz 4 DSG NRW zur informationellen Gewaltenteilung weitergeführt wird. Danach gelten für Datenübermittlungen innerhalb einer öffentlichen Stelle die gleichen Voraussetzungen wie für Datenübermittlungen zwischen öffentlichen

Stellen.

Nach dem Grundsatz der informationellen Gewaltenteilung ist zu gewährleisten, dass Datenflüsse innerhalb einer öffentlichen Stelle zwischen Stellen mit unterschiedlichen Aufgaben und Zuständigkeiten datenschutzrechtlichen Bedingungen unterliegen. Letztlich soll jeder Bedienstete innerhalb einer öffentlichen Stelle nur diejenigen personenbezogenen Daten zur Kenntnis erhalten, welche er zur Erfüllung seiner Aufgaben auch tatsächlich benötigt. Ein Beispiel für einen relevanten Datenaustausch ist die Weitergabe von Daten des Meldeamtes an das Sozialamt innerhalb einer Gemeinde.

Dem Grundsatz der informationellen Gewaltenteilung kommt nach der Rechtsprechung des Bundesverfassungsgerichts eine hohe verfassungsrechtliche Bedeutung zu. Selbst wenn die Regelung nur klarstellende Funktion besitzen sollte, ist sie erforderlich, da die DSGVO hier nicht deutlich genug erscheint. Die Erwähnung des Grundsatzes allein in der Begründung genügt daher nicht.

Zu § 4 d. E.

Die Anonymität von personenbezogenen Daten sollte allein in Abgrenzung zur Definition der personenbezogenen Daten gemäß Artikel 4 Nr. 1 DSGVO bestimmt werden, da diese zugleich das Hauptkriterium für den sachlichen Anwendungsbereich der DSGVO darstellt. Eine Öffnungsklausel für eine solche Begriffsbestimmung ist entgegen der Entwurfsbegründung nicht ersichtlich.

Im Erwägungsgrund 26 heißt es hierzu:

> „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.
> Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichti-

gen sind.
Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann."

Es ist grundsätzlich problematisch, Daten als anonymisiert zu betrachten, deren Personenbezug an sich herstellbar ist, bei denen aber die Herstellung des Personenbezugs wegen eines unverhältnismäßigen Aufwands gegenwärtig faktisch ausgeschlossen wird. Angesichts der rasanten technologischen Entwicklung in diesem Bereich kann der zunächst unverhältnismäßig erscheinende Aufwand zur „De-Anonymisierung" sich bereits nach kurzer Zeit erheblich verringern.

Es wird sich zeigen, wie die einzelnen DSGVO-Kriterien der wahrscheinlichen Nutzung zur Identifizierung und der zum Zeitpunkt der Verarbeitung verfügbaren Technologie vor diesem Hintergrund in der Zukunft auszulegen sind. Eine parallele, aber nicht vollständig komplementäre Definition der Anonymisierung im nationalen Recht würde angesichts dieser Kriterien in der Praxis zu Verwirrung und Unsicherheiten führen und wäre auch deshalb europarechtlich bedenklich.

Diese Begriffsbestimmung sollte daher nicht in das DSG aufgenommen werden.

Zu § 5 d. E.

1. Es sollte die Gelegenheit genutzt werden, den Anwendungsbereich für privatrechtlich organisierte Vereinigungen öffentlicher Stellen zu präzisieren (Absatz 1 Satz 1). Jedenfalls sollten die Ausnahmen mit Verweisung auf die Vorschriften für nicht-öffentliche Stellen (Absatz 4) nicht abschließend gestaltet werden.

   Nach geltendem Recht gibt es entweder Abgrenzungsprobleme im Verhältnis zum Bundesdatenschutzgesetz (BDSG) oder Wertungswidersprüche in Anwendung der Regelung zu wirtschaftlich tätigen Stellen. Wertungswidersprüche treten auf, wenn etwa eine GmbH als öffentliche Stelle definiert wird, aber nicht in den abschließenden

Ausnahmekatalog bei wirtschaftlichen Zwecken fällt. Nach neuem Recht ist insoweit weder in der am 25. Mai 2018 in Kraft tretenden Fassung des BDSG[1] eine Änderung vorgesehen (Begriffsbestimmungen in § 2 BDSG (2018)), noch im Entwurf des DSG NRW. Derzeit behilft sich die LDI NRW mit einem ungeschriebenen Tatbestandsmerkmal („Aufgaben der Verwaltung"), um Lücken bzw. unangemessene Zuordnungen zu vermeiden. Das Merkmal „deren" Vereinigungen wird derzeit zudem so verstanden, dass die Vereinigung durch öffentliche Stellen „beherrscht" werden muss, um einen zu weiten Anwendungsbereich entgegen der angenommenen Regelungsabsicht auszuschließen. Die Problematik tritt bisher in manchen anderen Landesdatenschutzgesetzen nicht auf, da sie verschiedene andere Definitionen für den Anwendungsbereich gewählt haben oder die Verweisung in das BDSG nicht an eine abschließende Aufzählung knüpfen (Beispiel Hessisches Datenschutzgesetz § 3 Absatz 4 („Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen…"; hier erfolgt im Unterschied zum DSG NRW keine abschließende Aufzählung).

Bleibt die Regelung unverändert, kann der Fall auftreten, dass eine privatrechtlich organisierte öffentliche Stelle am Wettbewerb teilnimmt, so dass eine Verweisung in das BDSG sachlich gerechtfertigt wäre, aber nicht greift, weil die Stelle nicht in § 5 Absatz 4 aufgezählt ist. Dies würde auch die Regelung zu Geldbußen betreffen, die nur für die aufgezählten Stellen vorgesehen sind.

2. Absatz 3 ist im Hinblick auf Landesrechnungshof und Staatliche Rechnungsprüfungsämter ergänzungsbedürftig. Es fehlt eine Regelung, nach welchen Datenschutzvorschriften sie sich außerhalb der Verwaltungsangelegenheiten zu richten haben. In diesem Bereich fehlt es daher auch an der nach Artikel 6 Absatz 3 Satz 1 lit. b) DSGVO notwendigen nationalen Rechtsgrundlage für die Datenverarbeitung.

   Entgegen der Entwurfsbegründung stellt die Vorschrift keine Beibehaltung der bisherigen Rechtslage dar. Bisher war die Tätigkeit des

[1] Bundesdatenschutzgesetz in der Fassung des Artikel 1des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30. Juni 2017, BGBl 2017, S. 2097 ff., in Kraft ab 25. Mai 2018, im Folgenden: BDSG (2018)

Landesrechnungshofs, die außerhalb der Verwaltungsangelegenheiten erfolgt, dem DSG unterworfen mit Ausnahme meiner Aufsichtszuständigkeit sowie einzelner weiterer Vorschriften (vgl. § 2 Absatz 1 Satz 3 DSG NRW).

Teil 2
Durchführungsbestimmungen zur Verordnung (EU) 2016/679

Zu § 7 d. E.

In Satz 1 sollten das Wort „Erhebungszweck“ durch das Wort „Verarbeitungszweck“ ersetzt werden.

Damit würde eine Angleichung an die Formulierung der Informationspflichten nach der DSGVO erreicht (vgl. Artikel 13 Absatz 1 lit. c und 14 Absatz 1 lit. c DSGVO). Auch sollte, entsprechend der bisherigen Rechtslage, jedenfalls eine Information über den Verwendungszweck erfolgen. Dieser würde vom Begriff „Verarbeitungszweck“ umfasst. Die Interessen der betroffenen Person, dass keine für sie nachteiligen Datenübermittlungen stattfinden, dürften durch den letzten Halbsatz des Satz 1 gewährleistet sein.

Zu § 8 d. E.

Es muss klarer gefasst werden, wie die einzelnen Verantwortlichkeiten, auch im Hinblick auf die Nachweispflichten, verteilt sind.

Die Verantwortlichkeitsübertragung ist – gemessen an der DSGVO – unklar. § 8 entspricht in etwa § 14 Absatz 2 DSG NRW. Allerdings ist die ausdrückliche Regelung neu, dass bei Ersuchen durch eine öffentliche Stelle diese die Verantwortung für die Übermittlung (und nicht für die Erhebung bzw. die Rechtmäßigkeit des Ersuchens) trägt. Diese Verantwortlichkeitsübertragung könnte formal wohl nach Art. 4 Nr. 7 Satz 2 DSGVO vorgenommen werden. Allerdings wäre es ungewöhnlich, der Stelle, die die Herrschaft über die Daten hat, die Verantwortung für den Datenumgang ganz zu nehmen. Dies ist offenbar auch nicht gewollt, wie die Folgesätze zeigen, nach denen die übermittelnde Stelle doch einige Prüfpflichten hat, auch bezüglich der Rechtmäßigkeit des Ersuchens.

Dies macht nur Sinn, wenn sie auch verantwortlich dafür bleibt, zu entscheiden, gegebenenfalls die Übermittlung nicht vorzunehmen.

Nach der Begründung soll die Verantwortlichkeitsübertragung insoweit auch die Nachweispflichten betreffen. Mit Blick auf die Betroffenenrechte, insbesondere zur Auskunft, wäre es allerdings geboten, die entsprechende Nachweispflicht auch der übermittelnden Stelle aufzuerlegen. Es ist unklar, ob weitere Pflichten mit der Verantwortlichkeitsübertragung verlagert werden (insbesondere Informations- und Auskunftspflichten) und wofür welche Stelle der richtige Adressat seitens betroffener Personen und Aufsichtsbehörden ist (z.B. Schadenersatz, Meldepflicht bei Datenpannen).

Zu § 9 d. E.

1. Die allgemeine Aufzählung zulässiger Zweckänderungen in Absatz 2 und 4 erfüllt nicht die Anforderungen von Art. 6 Absatz 4 DSGVO.

   Die bisherige allgemeine Abwägung, wann Zweckänderungen erlaubt sein können, nimmt bereits die DSGVO selbst in Art. 23 Absatz 1 vor. Nach der DSGVO ist kein zusätzlicher nationaler Zweckänderungskatalog vorgesehen, sondern es wird lediglich auf verhältnismäßige nationale Regelungen zu den in Art. 23 Absatz 1 DSGVO genannten Zielen verwiesen. Art. 6 Absatz 4 Fall 2 DSGVO stellt damit – anders als in der Entwurfsbegründung ausgeführt – keine eigene Öffnungsklausel für den Erlass von Rechtsvorschriften, die Zweckänderungen erlauben, dar. Nach Art. 6 Absatz 4 DSGVO ist für die Prüfung, ob eine zweckändernde Verarbeitung zulässig ist, grundsätzlich eine Kompatibilitätsprüfung erforderlich. Regelungsgehalt des Art. 6 Absatz 4 Fall 2 ist vielmehr, dass er bestimmt, bei welchen Rechtsgrundlagen (v.a. nach Art. 6 Absatz 1 lit. e i. V. m. Absatz 3 DSGVO) eine Kompatibilitätsprüfung nach Art. 6 Absatz 4 lit. a-e unterbleiben kann. Diese Rechtsgrundlagen sind an den Zwecken des Art. 23 Absatz 1 DSGVO zu messen. Eine solche Rechtsgrundlage stellen § 9 Absatz 2 und 4 des Entwurfs nicht dar.

2. Die nach diesen Maßstäben und vorbehaltlich der genannten Kritik geprüften einzelnen Tatbestände erscheinen gegenüber den nach Art. 23 Absatz 1 DSGVO erlaubten Zwecken teilweise als zu weit

gefasst:

- Absatz 2 Nr. 1 lässt jegliche Gefahr genügen und fordert nicht, wie es noch in einem früheren Entwurf der Fall war, eine „unmittelbar drohende Gefahr“. Damit würde die Regelung eine Absenkung gegenüber dem bisherigen Datenschutzniveau bedeuten. Da sie die Verhältnismäßigkeit nicht wahrt, genügt sie nicht den Anforderungen des Art. 6 Absatz 4 DSGVO i. V. m. Art 23 Absatz 1 DSGVO.

- Absatz 2 Nr. 4 ist nicht unter Art. 23 Absatz 1 lit. e DSGVO zu subsumieren. Es kommt auch kein anderer Tatbestand des Art. 23 Absatz 1 in Frage.

- Absatz 2 Nr. 6 ist im Vergleich zu Art. 23 Absatz 1 lit. e DSGVO zu weit formuliert:

    - Die Formulierung „öffentliches Interesse“ ist zu allgemein, es müssten die wichtigen Ziele des öffentlichen Interesses benannt werden, sonst wäre auch die Aufzählung der wichtigen öffentlichen Interessen in Art. 23 Absatz1 lit. a, b, c, d, f, g, überflüssig.

    - Für die berechtigten Interessen eines Dritten ist kein Tatbestand des Art. 23 Absatz 1 DSGVO ersichtlich.

- Absatz 4 Nr. 1 ist im Verhältnis zu dem herangezogenen Tatbestand des Art. 23 Absatz 1 lit. i 1. Alt. DSGVO zu weit formuliert.

- Absatz 4 Nr. 2: Mit der Berufung auf Art. 23 Absatz 1 lit. i Alt. 2 DSGVO wird deren Wortlaut überdehnt. Bei Anträgen betroffener Personen kann bei Bedarf deren Einwilligung eingeholt werden.

- Absatz 4 Nr. 3 entspricht zwar etwa dem bisherigen § 13 Absatz 2 Satz 3 DSG NRW, aber ein legitimierender Tatbestand in Art. 23 Absatz 1 DSGVO ist nicht ersichtlich.

Zu § 10 d. E.

§ 10 Absatz 2 sollte gestrichen werden, da keine passende Öffnungsklausel der DSGVO ersichtlich ist.

Zu § 11 ff. d. E.

Zunächst ist fraglich, ob die Aufzählung von Voraussetzungen, unter denen die Rechte der Betroffenen auf Information (§ 11 Absatz 1), Auskunft (§ 12 Absatz 2) und Benachrichtigung (§ 13) beschränkt werden können, die europarechtlichen Anforderungen an spezifische Gesetzgebungsmaßnahmen zur Beschränkungen der Betroffenenrechte gemäß Art. 23 Absatz 1 und 2 erfüllen (s. o. u. A, S. 4).

Vorbehaltlich dessen fehlt im Tatbestand des § 11 Absatz 1 Satz 1 Nr. 3 die Ergänzung, dass es sich um zivilrechtliche Ansprüche des Verantwortlichen handeln muss. Die Beschränkung der Informationspflicht gemäß Absatz 1 Satz 1 Nr. 3 entspricht dem erlaubten Zweck des Art. 23 Absatz 1 lit. j nämlich nur, sofern sie sich auf die Durchsetzung von Ansprüchen der verantwortlichen Stelle bezieht. Dies sollte im Gesetzestext klargestellt werden.

Zu § 12 d. E.

1. Absatz 3: Es sollte sichergestellt werden, dass auch in diesen Fällen eine Auskunft erfolgt, sobald ein Ablehnungsgrund im Sinne des Absatzes 2 entfällt.

2. Es sollte noch entsprechend § 18 Absatz 6 DSG NRW ein Hinweis auf die Möglichkeit, sich an die LDI NRW zu wenden, aufgenommen werden.

Zu Kapitel 3 (Struktur)

1. Das Kapitel 3 sollte neu strukturiert werden. Die Vorschriften zur Verarbeitung besonderer Kategorien personenbezogener Daten soll-

ten von den Vorschriften zu besonderen Verarbeitungssituationen systematisch getrennt werden.

Die Systematik dieses Kapitels ist unklar, weil sie Vorschriften zum Umgang mit besonderen Kategorien personenbezogener Daten einerseits und Vorschriften zu besonderen Verarbeitungssituationen vermengt. Es handelt sich dabei aber um unterschiedliche Bereiche, die sich lediglich überschneiden können. Besondere Verarbeitungssituationen sind nach der DSGVO die in ihrem Kapitel IX beschriebenen besonderen Situationen wie Verarbeitung zur Ausübung von Meinungsfreiheit einschließlich journalistischer Zwecke, Verarbeitung durch Kirchen, etc. Der Umgang mit besonderen Kategorien personenbezogener Daten unterliegt dagegen den besonderen Anforderungen gemäß Art. 9 DSGVO unabhängig davon, ob er im Rahmen dieser besonderen Verarbeitungssituationen geschieht.

2. Wird der unter 1. genannte Vorschlag nicht umgesetzt, muss zumindest die Überschrift des Kapitels 3 und die des Kapitels 3 Abschnitt 1 um die Verarbeitung besonderer Kategorien personenbezogener Daten erweitert werden.

   Durch die insoweit lückenhaften Überschriften von Kapitel 3 und Abschnitt 1 kann ein Missverständnis bezüglich des Anwendungsbereichs der §§ 15 und 16 erzeugt werden, da ihr Regelungsgegenstand unabhängig vom Vorliegen besonderer Verarbeitungssituationen ist.

3. Die Überschrift des § 15 sollte unter Beschränkung auf besondere Kategorien personenbezogener Daten umformuliert werden.

   Die Beschränkung entspricht dem Regelungsgehalt der Vorschrift.

4. Die Verwendung des Begriffs „besondere Verarbeitungssituationen“ in den Überschriften von Kapitel 3 und Kapitel 3 Abschnitt 1 sollte überdacht werden, da die Videoüberwachung in § 20 d. E. keine besondere Verarbeitungssituation im Sinne des Kapitels IX DSGVO darstellt.

Zu § 15 d. E.

1. Die Anforderungen an die gesetzgeberische Gestaltung von Ausnahmeerlaubnissen für die Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Absatz 2 lit. b, g, h, i und j DSGVO werden durch § 15, auch i. V. m. §§ 16 – 17 d. E. nicht erfüllt.

   Artikel 9 Absatz 2 lit. b, d, g, h, i und j DSGVO fordern „geeignete Garantien“ bzw. „spezifische Maßnahmen“ für die Verarbeitung von besonderen Kategorien personenbezogener Daten. Zu jeder dieser Ausnahmemöglichkeiten – abgesehen von Artikel 9 Absatz 2 lit. d DSGVO – hat der Gesetzgeber notwendig die auf die jeweils betroffenen personenbezogenen Daten nach Art. 9 Absatz 1 DSGVO und die konkrete Verarbeitungssituation zugeschnittenen Garantiemaßnahmen unter Abwägung der jeweils betroffenen Grundrechte und Interessen zu konkretisieren. Eine allgemeine Aufzählung der Maßnahmen wie in § 15 genügt diesen Anforderungen nicht. Auch ist es nicht zulässig, die Auswahl der Maßnahmen je nach konkreten Umständen dem Verantwortlichen anheimzustellen und damit die dem Gesetzgeber auferlegte Pflicht auf die Verantwortlichen zu übertragen (vgl. § 15 Absatz 1 Satz 1 und 2 d. E.).

   In der Entwurfsbegründung zu § 15 wird zwar darauf verwiesen, dass zusätzliche Garantien im bereichsspezifischen Datenschutzrecht festzulegen sind. Es ist aber unklar, welche bereichsspezifischen Regelungen ab dem 25. Mai 2018 gelten werden. Außerdem ist fraglich, welcher Anwendungsbereich danach überhaupt für die nach der Entwurfsbegründung „im Bereich des allgemeinen Datenschutzes“ zu treffenden Schutzmaßnahmen des § 15 verbleibt. Die Dualität „allgemeines Datenschutzrecht“ und „bereichsspezifisches Recht“ besteht im Hinblick auf die abschließenden spezifischen Ausnahmeerlaubnisse des Art. 9 Absatz 2 DSGVO nicht. Sollte sich der Anwendungsbereich des § 15 im Bereich der DSGVO nur auf bestimmte Tatbestände des Artikel 9 Absatz 2 DSGVO beziehen, wären diese in der Vorschrift zu nennen.

2. Dies vorausgeschickt, ist auch die Verknüpfung der verschiedenen Maßnahmen, die nach § 15 Satz 2 geeignete Garantien darstellen, mit „oder“ (vgl. Ziffer 8) ist missverständlich. Da alle aufgeführten

Maßnahmen dazugehören und nicht als Alternativen zu verstehen sind, ist das Wort „oder“ durch „und“ zu ersetzen.

Zu § 16 d. E.

Die Aussage des § 16, die Verarbeitung besonderer Kategorien personenbezogener Daten sei zu den dort genannten Zwecken zulässig, ist nicht mit den Vorgaben der DSGVO vereinbar, weil die DSGVO in Artikel 9 Absatz 2 selbst die Ausnahmefälle festlegt, in denen die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist. Eine Einschränkung dieses Katalogs ist ebenso wenig europarechtskonform, wie eine Wiederholung der dort aufgeführten Tatbestände – zumal, wenn sie unvollständig ist, weil nur die Zwecke genannt werden und auf die Maßgabe bereichsspezifischer Regelungen mit spezifischen Maßnahmen oder Garantien im Sinne der Artikel 9 Absatz 2 lit. b, g, h, und i DSGVO verzichtet wird.

Zu § 17 d. E.

Soweit die Vorschrift zugleich die Forschung mit besonderen Kategorien personenbezogener Daten nach Art. 9 Absatz 1 der DSGVO regeln will, wird sie den daran zu stellenden Anforderungen nicht gerecht. Für die Forschung mit besonderen Kategorien personenbezogener Daten sind auch nach den ausdrücklichen Vorgaben der DSGVO besondere bereichsspezifische Anforderungen zu regeln, die dem erhöhten Schutzbedürfnis dieser Daten gerecht werden (s. u. 1. und 2.).
Auch für den Bereich der Statistik ist die vorgesehene Regelung nicht angemessen (s. u. 4.).

1. Absatz 1 und 2 stellen keine hinreichende Rechtsgrundlage für die Forschung mit besonderen Kategorien personenbezogener Daten dar. Die Einbeziehung der besonderen Kategorien personenbezogener Daten in § 17 d. E. ist zu streichen.

   Insgesamt bestehen grundlegende Bedenken dagegen, die Forschung mit besonderen Kategorien personenbezogener Daten nach Art. 9 Absatz 1 DSGVO im Rahmen der allgemeinen Forschungsklausel im DSG NRW zu regeln. Diesbezüglich sind – wie bisher –

spezifische Forschungsklauseln in den jeweiligen Regelungszusammenhängen bereichsspezifischer Gesetze erforderlich; nur so kann sichergestellt werden, dass dem besonderen Schutzbedarf der jeweiligen Daten hinreichend Rechnung getragen wird (vgl. Stähler/Pohler, Datenschutzgesetz Nordrhein-Westfalen, 3. Auflage, § 28. Rn 3). Die derzeit geregelten bereichsspezifisch erhöhten Anforderungen, wie sie zum Beispiel derzeit etwa in § 6 GDSG NRW festgelegt sind, müssen erhalten bleiben.

Im Entwurf fehlt die Verankerung strengerer Anforderungen, die dem erhöhten Schutzbedarf, wie er im grundsätzlichen Verarbeitungsverbot des Art. 9 Absatz 1 der DSGVO zum Ausdruck kommt, gerecht werden. Art. 9 Absatz 2 lit. j DSGVO erlaubt die Verarbeitung zu Forschungszwecken ausnahmsweise nur, wenn die gesetzliche Erlaubnis in angemessenem Verhältnis zum verfolgten Ziel steht und spezifische und angemessene Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Diese sind bisher zum Beispiel für Gesundheitsdaten in § 6 GDSG NRW für die Forschung mit Patientendaten in Krankenhäusern festgelegt: Eine Forschung mit personenbezogenen Daten ist nach dessen Absatz 2 Satz 2 ohne Einwilligung des Patienten nur dann möglich, wenn die Einholung der Einwilligung des Patienten entweder unmöglich ist oder sie dem Patienten aufgrund seines gegenwärtigen Gesundheitszustands nicht zugemutet werden kann. Kumulativ fordert das GDSG NRW, dass der Zweck eines bestimmten Forschungsvorhabens nicht auf andere Weise erreicht werden kann und das Interesse an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegen muss. Ferner legt § 6 GDSG NRW in Absatz 2 – 6 weitere unerlässliche Bedingungen fest, von denen nur Absatz 4 eine Entsprechung in § 17 Absatz 2 d. E. findet.

2. Unabhängig von dem unter 1 dargestellten Änderungsbedarf sind in § 17 Absatz 2 die Worte „zu wissenschaftlichen oder historischen Forschungszwecken“ durch „für ein bestimmtes wissenschaftliches oder historisches Forschungsvorhaben“ und in der Nr. 1 das Wort „oder“ durch „und „ zu ersetzen.

Wie bisher (§ 28 DSG NRW) sollte die Erlaubnis zur Verarbeitung ohne Einwilligung mit einem bestimmten Forschungsvorhaben verknüpft sein.

3. Auch die Erlaubnis zur Veröffentlichung in Absatz 4 ist, soweit sie besondere Kategorien personenbezogener Daten umfassen soll, zu weitgehend und würde eine Absenkung des bisherigen Datenschutzniveaus bedeuten.

   Bisher ist zum Beispiel eine Veröffentlichung von Gesundheitsdaten, die einen Rückschluss auf die Person des Patienten zulassen, nach § 6 Absatz 5 GDSG nur zulässig, wenn der Patient in die Veröffentlichung ausdrücklich eingewilligt hat. Dieses Erfordernis muss zur Wahrung des Rechts der Patientinnen und Patienten auf informationelle Selbstbestimmung unbedingt beibehalten werden. Für andere besondere Kategorien personenbezogener Daten müssen entsprechende Anforderungen an eine personenbeziehbare Veröffentlichung geregelt werden.

4. Die Beschränkung der Betroffenenrechte in Absatz 5 ist insgesamt zu streichen. Dies gilt insbesondere auch für den Bereich der Verarbeitung zu statistischen Zwecken.

   Absatz 5 normiert Einschränkungen der Betroffenenrechte gestützt auf Art. 89 Absatz 2 DSGVO. Zu beachten ist, dass alle auf Art. 89 Absatz 2 DSGVO gestützten Ausnahmen unter dem Vorbehalt des Art. 89 Absatz 1 DSGVO stehen. Absatz 5 d. E. wiederholt zum Teil Art. 89 Absatz 2 DSGVO ohne eigenen Regelungsinhalt. Insbesondere der Erwägungsgrund (EG) 156 macht deutlich, dass diese Vorgehensweise nicht geeignet ist, die Öffnungsklausel des Art. 89 Absatz 2 DSGVO auszufüllen, d. h. den Anforderungen der DSGVO gerecht zu werden. Art. 89 Absatz 2 DSGVO ermächtigt nicht zur Schaffung einer allgemeinen Regelung, sondern die Ausnahmen müssen unter bestimmte Bedingungen gestellt werden. Spezialgesetzliche Regelungen bieten sich hier an. Grundsätzlich sollten die Betroffenenrechte nicht eingeschränkt werden.

   Im Hinblick auf die Verarbeitung zu Statistikzwecken ist insbesondere Folgendes zu bemerken: Durch die DSGVO entsteht keine Notwendigkeit, auf Landesebene statistikgesetzliche Regelungen. Es

sollte daher von der Öffnungsklausel des Art. 89 Absatz 2 DSGVO, die Ausnahmen von den Rechten der Betroffenen gemäß der Artikel 15, 16, 18 und 21 DSGVO zulässt, kein Gebrauch gemacht werden. Die Anforderungen an derartige Ausnahmen sind sehr hoch. Das Auskunftsrecht der Betroffenen (Art. 15 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO) und auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie das Widerspruchsrecht (Art. 21 DSGVO) zählen nach dem bisherigen Datenschutzstandard und nach der Rechtsprechung zu den zentralen Datenschutzrechten, deren Geltendmachung oftmals erst zur Durchsetzung des Rechts auf informationelle Selbstbestimmung verhilft. Insofern bestehen gegen die in Absatz 5 vorgesehenen Einschränkungen der Betroffenenrechte erhebliche Bedenken.

Bisher sind in der aufsichtsbehördlichen Praxis keine Fälle bekannt geworden, die diesem Maßstab genügende Ausnahmeregelungen rechtfertigen könnten. Nicht ersichtlich ist, inwiefern diese Betroffenenrechte voraussichtlich eine Verwirklichung der spezifischen (= mit der Statistik verfolgten) Zwecke unmöglich machen oder diese ernsthaft beeinträchtigen könnten. Auch ist nicht nachvollziehbar, weshalb ein Ausschluss der Betroffenenrechte für die Erfüllung statistischer Zwecke notwendig sein sollte. Vielmehr wird durch die Gewährung von Auskunftsrechten auch im Vollzug der amtlichen Statistik Transparenz gewährleistet, wodurch die Akzeptanz von statistischen Erhebungen erhöht wird und darüber hinaus die Korrektur unrichtiger Daten durch von Auskunftspflichtigen selbst korrigierte Erhebungsmerkmale ermöglicht wird (vgl. Art. 16 Satz 2 DSGVO).

Zu § 18 d. E.

1. Zu Absatz 1

Die Gesetzesbegründung zu Absatz 1 ist stellenweise missverständlich. Zunächst ist festzuhalten, dass das in der Begründung angeführte Urteil des Bundesarbeitsgerichts vom 11.12.2014 - 8 AZR 1010/13 - nicht unumstritten ist und eine besondere Konstellation einer Datenverarbeitung behandelt hat. Es wird weiterhin durchaus kontrovers diskutiert, in welchen Fällen eine Einwilligung in die Verarbeitung von Beschäftigtendaten zulässig sein kann. Das strukturelle Ungleichgewicht zwischen Dienstherrn und Beschäftigten lässt es nur in begrenzten Einzelfällen

zu, eine solche Freiwilligkeit einer Einwilligung anzunehmen. Dabei ist jeder Einzelfall zu beurteilen.

Die Generalisierung der Aussage in der Begründung zu Absatz 1 ist daher kontraproduktiv. Die bestehende Formulierung verleitet zu dem Missverständnis, dass generell in jeder entsprechenden Fallgestaltung eine Einwilligung möglich ist. Gerade weil im Weiteren die Begründung zu Absatz 2 differenzierter ist, hindert eine solche pauschalisierende Aussage zu Absatz 1 die Rechtsanwender an einer rechtskonformen Auslegung des Gesetzes.

2. Zu Absatz 2

a) Es bestehen grundsätzliche Einwände gegen die Beispiele für das Vorliegen einer Freiwilligkeit der Einwilligung. Eine Einwilligung ist zwar nicht grundsätzlich ausgeschlossen; es gelten jedoch strenge Anforderungen, insbesondere hinsichtlich der Beurteilung der Freiwilligkeit. Diese ist stets anhand der jeweiligen Einzelfallumstände zu prüfen. Bei den genannten Beispielen „rechtlicher oder wirtschaftlicher Vorteil“ besteht die Gefahr, dass z. B. leistungsbezogene „Vorteile“ mit einer Einwilligung in eine bestimmte Datenverarbeitung dennoch nicht in Zusammenhang stehen.
Soweit eine Verknüpfung gleichgerichteter Interessen für die Freiwilligkeit der Einwilligung sprechen soll, darf nicht übersehen werden, dass dies aus der subjektiven Sicht der Beteiligten durchaus unterschiedlich gesehen werden kann. Die Beurteilung, wann gleichgelagerte Interessen vorliegen, dürfte demnach schwierig sein.

b) In der Begründung wird als ein Anwendungsfall einer wirksamen Einwilligung – gestützt auf das Beispiel der „gleichgerichteten Interessen“ – die Aufnahme von Beschäftigten in eine DNA-Referenzdatei zum Ausschluss von Trugspuren genannt.

Es wird empfohlen, insoweit eine gesonderte gesetzliche Regelung zu vorzusehen, die mit Einwilligung der betroffenen Beschäftigten eine Erhebung und Speicherung ihrer DNA-Daten in einer Referenzdatei zum Ausschluss von Trugspuren erlaubt.

Die Schaffung einer gesetzlichen Grundlage für diese Datenverarbeitung ist zum Schutz des Rechts auf informationelle Selbstbestimmung notwendig. Die Entscheidung für eine Erhebung und Speicherung von

DNA-Daten der Betroffenen zu dem genannten Zweck und die Festlegung der hierfür maßgeblichen Voraussetzungen bleibt wegen der erheblichen Eingriffstiefe dieser Maßnahme in die Grundrechte einer gesetzlichen Normierung vorbehalten. Es ist nicht ausreichend, einen solchen intensiven Eingriff allein in einer Gesetzesbegründung zu erwähnen.

Dabei sollten außerdem die weiteren Voraussetzungen für eine solche Erhebung und Speicherung von DNA-Daten (u.a. umfassende Unterrichtung, Benachteiligungsverbot für den Fall des Absehens von der Einwilligung, Löschungsverpflichtung) ebenfalls gesetzlich geregelt werden. Eine solche landesgesetzliche Regelung sollte sich an die durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 01.06.2017 (BGBl. I 2017, S. 1354) neu eingeführte Vorschrift des § 24 BKAG anlehnen.

3. Zu Absatz 7

Die gesetzliche Regelung der Zwangslöschung gebietet, jegliche Information über eine erfolglos gebliebene Bewerbung zu vernichten. Eine Klarstellung dahingehend, dass zu den „vor der Eingehung eines Beschäftigungsverhältnisses“ erhobenen Daten jegliche Daten der Betroffenen, also auch die Tatsache der Bewerbung als solche, gehören, würde unrechtmäßige Auslegungen des Gesetzes vermeiden. Empfohlen wird daher, in Satz 1 nach dem Wort „erhoben“ die Wörter „oder gespeichert“ einzufügen.

Zu § 19 d. E.

§ 19 stellt eine für den öffentlichen Bereich völlig neuartige Ausnahmeregelung dar, die so nicht in das Gesetz aufgenommen werden sollte. Ihr Regelungsanlass ist unbekannt und der Anwendungsbereich klärungsbedürftig. Ob ein zulässiger Anwendungsbereich für diese Ausnahmevorschrift besteht, bedarf eingehender verfassungs- und europarechtlicher Prüfung (s. u. 1.). § 19 überschreitet in der inhaltlichen Reichweite den Rahmen der Ausnahmeerlaubnis des Artikel 85 Absatz 2 DSGVO, indem er die Ausnahmevorschriften des Medienprivilegs in der derzeit geplanten Änderungsfassung von Rundfunkstaatsvertrag, Landesmedien- und Landespressegesetz übernimmt (vgl. Entwurf zum 16. Rundfunkänderungsgesetz, Drucksache 17/1565 und meine Stel-

lungnahme hierzu vom 1. März 2018, Stellungnahme 17/400), dazu (s. u. 2.). Dabei wird auch nicht berücksichtigt, dass der dort gegebene rundfunk- oder presserechtliche Regelungskontext hier fehlt (s. u. 3.).

1. Der praktische Anwendungsbereich ist unklar und wohl nicht von der Ausnahmemöglichkeit des Artikels 85 DSGVO erfasst:

Der Abwägungsauftrag des Artikel 85 DSGVO gilt nur zwischen dem Recht auf Schutz der personenbezogenen Daten einerseits und dem Recht auf freie Meinungsäußerung (und Informationsfreiheit) andererseits. Auch die Möglichkeit nach Artikel 85 Absatz 2 DSGV, Abweichungen und Ausnahmen von bestimmten Vorschriften der DSGVO vorzusehen, besteht nur,

> „wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen."

Zu beachten ist, dass § 19 DSG-E ausschließlich für öffentliche Stellen gilt, die Grundrechte auf öffentliche Stellen nach deutschem Verfassungsrecht aber grundsätzlich nicht anwendbar sind. Ausnahmen hiervon, die das Grundrecht auf Meinungsfreiheit betreffen, sind mir nicht bekannt. Auch in der Gesetzesbegründung fehlt eine Auseinandersetzung damit, ob und – wenn ja – welche öffentlichen Stellen sich unter welchen Bedingungen ausnahmsweise bei Erfüllung ihrer öffentlichen Aufgaben auf das Grundrecht der Meinungsfreiheit berufen könnten. Falls derartige Konstellationen festzustellen wären, müssten sie auch im Gesetzestext selbst in Bezug genommen werden. In der Regel werden künstlerische oder literarische Werke und die zugehörigen Datenverarbeitungen allerdings natürlichen Personen zuzuordnen sein und nicht einer öffentlichen Stelle.

Konfliktlagen, die ausweislich der Gesetzesbegründung mit dieser Vorschrift geregelt werden sollen, werden nicht beschrieben. Aus der Aufsichtspraxis sind mir derartige Konflikte nicht bekannt geworden.

Insgesamt ist daher davon auszugehen, dass weder ein echter Regelungsbedarf noch ein zulässiger Anwendungsbereich, mithin auch keine europarechtliche Regelungsbefugnis für diese Norm erkennbar ist.

2. Dies vorausgeschickt, würde die Vorschrift aber auch im Regelungsumfang weit über das europarechtlich Erlaubte hinausgehen:

Die Vorschrift nimmt fast alle Vorschriften der Kapitel II-VII und IX DSGVO von der Anwendbarkeit aus, wenn personenbezogene Daten zu künstlerischen oder literarischen Zwecken verarbeitet werden. Art. 85 Absatz 2 DSGVO gestattet Abweichungen wie oben erwähnt jedoch nur als Ergebnis einer Abwägung der beteiligten Grundrechte,

> „wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen

Dies steht einer pauschalen Nichtanwendbarkeit fast aller Vorschriften der DSGVO entgegen. Die notwendige Abwägung des Gesetzgebers, wann, warum und in welchem Maße das Recht auf informationelle Selbstbestimmung hinter dem durch allgemeine Gesetze beschränkbaren Recht auf freie Meinungsäußerung zurücktreten muss, um einen angemessenen Ausgleich der betroffenen Rechte zu schaffen, ist nicht erkennbar. Abweichungen und Ausnahmen von der DSGVO sind damit nicht auf das erforderliche Maß beschränkt worden, sondern das Datenschutzrecht wird in verfassungsrechtlich bedenklichem Umfang nahezu pauschal ausgeschlossen.

Auch die Gesetzesbegründung trägt den Regelungsgehalt in keiner Weise. Zur Begründung wird dort lediglich angeführt, die literarische Arbeit sei mit den Anforderungen der DSGVO „nicht vollends in Einklang zu bringen“ und die Verpflichtung zum Schutz des Rechts auf freie Meinungsäußerung erfordere es, Abweichungen zu regeln. Es liegt auf der Hand, dass eine derart vage Begründung keine weitreichende Nichtanwendung der DSGVO rechtfertigen kann. Die Formulierung „nicht vollends in Einklang zu bringen“ spricht vielmehr dafür, dass nur marginale Anpassungen erforderlich wären.

Ein besonderes Hindernis für das Recht auf freie Meinungsäußerung sieht die Entwurfsbegründung im Bereich der künstlerischen und literarischen Arbeit in den Berichtigungs- und Löschungsansprüchen. Hinsichtlich des Löschungsanspruchs sieht aber bereits Artikel 17 Absatz 3 lit. a DSGVO vor, dass dieser Anspruch nicht gilt, soweit die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information er-

forderlich ist. Mangels Erforderlichkeit ist die geregelte Nichtanwendbarkeit des Artikels 17 DSGVO damit unzulässig.

Ferner ist § 19 Absatz 1 Satz 3 schon formal nicht von der Ausnahmemöglichkeit gedeckt, da er Abweichungen von einer Norm aus Kapitel VIII DSGVO vorsieht, die Artikel 85 Absatz 2 DSGVO nicht zulässt.

3. Die Vorschrift stellt außerdem keine konsistente Regelung dar.

So wird in Absatz 2 von der Möglichkeit von Gegendarstellungen ausgegangen, wobei unklar bleibt, wann ein entsprechender Anspruch vorliegt, da weder der Anwendungsbereich des Rundfunkstaatsvertrags noch des Landespressegesetzes gegeben sein dürfte.

Ferner werden durch § 19 nur Vorschriften der DSGVO vom Anwendungsbereich ausgeschlossen, so dass Teil 1 und 2 des DSG auch auf Datenverarbeitungen zu künstlerischen oder literarischen Zwecken anwendbar sind (vgl. § 5 d. E.). Dies ist jedoch widersprüchlich, soweit das DSG der Durchführung der durch § 19 gerade ausgeschlossenen Regelungen der DSGVO dient (vgl. § 1 Absatz 1 d. E.).

Unklar bleibt schließlich das Verhältnis zu spezialgesetzlichen Betroffenenrechten (z. B. §§ 37 ff. KUG), da § 5 Absatz 5 d. E. zwar vorsieht, dass spezialgesetzliche Regelungen den Vorschriften des Teils 2 vorgehen, § 19 Absatz 1 Satz 1 aber ausdrücklich formuliert, dass Betroffene nur die in § 19 Absatz 2 DSG-E genannten Rechte haben sollen.

Insgesamt ist festzustellen, dass, soweit ein zulässiger Anwendungsbereich der Vorschrift bestehen sollte, eventuelle Abweichungen von der DSGVO auf punktuelle Änderungen beschränkt bleiben müssen.

Zu § 20 d. E

1. Nach der derzeitigen Rechtslage (§ 29b DSG NRW) ist der einzige zulässige Zweck der Videoüberwachung die „ Wahrnehmung des Hausrechts“.
   In einem Vorentwurf wurde die Zweckbestimmung „zur Wahrnehmung des Hausrechts“ ersetzt durch „zur Aufrechterhaltung der

Funktionsfähigkeit der öffentlichen Stelle“. Diese Änderung hätte das bisherige Datenschutzniveau in etwa gehalten, weil sie den zulässigen Zweck aufgrund der Formulierung „zur Aufrechthaltung der Funktionsfähigkeit“ hinreichend eingegrenzt hätte.

Der vorliegende Entwurf enthält nun gleich vier Zweckbestimmungen, die die Videoüberwachung öffentlich zugänglicher Bereiche ermöglichen:

Zu Nr. 1 („zur Erfüllung der Aufgaben öffentlicher Stellen“):

Diese neu aufgenommene Zweckbestimmung ist viel zu weit. Sie hat kaum eingrenzende Wirkung und dürfte als Auffangtatbestand für alle nicht durch die Tatbestände der Nr. 2 - 4 zu begründenden Einsatzzwecke dienen.

So könnte mit Hinweis auf die Aufgabe öffentlicher Stellen, die Verunreinigung etwa von Parkanlagen, Badeseen, Straßen und Plätzen zu verhindern und ggf. zu ahnden, die flächendeckende Überwachung dieser Orte begründet werden. Ebenso ließe sich die Überwachung von Parkplätzen und des gesamten Straßenverkehrs zur Verhinderung und Ahndung von Verkehrsverstößen herleiten.

Mit Hinweis auf eine vorgeblich überwiegende, besondere Bedeutung der Verkehrssicherheit und des Umweltschutzes für die Allgemeinheit könnte so eine umfassende Videoüberwachung des öffentlichen Raums hergeleitet werden – wie etwa in Singapur, wo mithilfe flächendeckender Videoüberwachung Personen ermittelt werden, die falsch parken oder öffentliche Flächen mit Zigarettenkippen und Kaugummis verunreinigen.

Dies wäre eine deutliche Absenkung des bisherigen Datenschutzniveaus – und ein erheblicher Eingriff in das Grundrecht der nordrhein-westfälischen Bürgerinnen und Bürger, sich in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden.

Da die Videoüberwachung jedoch eine besondere Eingriffstiefe besitzt, muss sie nach dem Verhältnismäßigkeitsgrundsatz auch unter

besondere Voraussetzungen gestellt werden (s. o. unter A Seite 2 f.). Dieser Anforderung genügt Absatz 1 Nr. 1 nicht, da die Zweckdefinition keine über die Generalklausel des § 3 Absatz 1 hinausgehenden Kriterien enthält. Soweit in der Gesetzesbegründung ausgeführt wird, in diesen Fällen solle mit Hilfe der Videoüberwachung die Funktionsfähigkeit der öffentlichen Stelle gewährleistet werden, sollte die Zweckbestimmung auch so formuliert werden. Absatz 1 Nr. 1 sollte daher durch die Zweckbestimmung *„zur Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Stelle“* ersetzt werden.

Zu Nr. 2 („zur Wahrnehmung des Hausrechts“):

Dieser Zweck entspricht der bisherigen Regelung in § 29b DSG NRW, die sich aus Sicht der LDI bewährt hat.

Zu Nr. 3 („zum Schutz von Eigentum und Besitz“):

Der in Nr. 3 neu aufgenommene Zweck ist zu weit und unbestimmt und birgt daher wie Nr. 1 das hohe Risiko einer umfassenden Videoüberwachung öffentlicher Orte und Flächen.

Zunächst stellt sich wegen des insoweit unklaren Wortlauts die Frage, ob tatsächlich der Schutz jeglichen Eigentums und Besitzes oder aber ausschließlich der Schutz von Eigentum und Besitz der öffentlichen Stelle gemeint ist. Sollte auch der Schutz von privatem Eigentum und Besitz als Voraussetzung für eine Videoüberwachung öffentlicher Stellen ausreichen, wäre der Tatbestand bereits aus diesem Grund von uferloser Weite.

Selbst wenn eine ergänzende Klarstellung den Tatbestand auf den Schutz von „öffentlichem“ Eigentum und Besitz beschränkte, würde er – aus vergleichbaren Erwägungen wie zu Nr. 1 – einer flächendeckenden Videoüberwachung Tür und Tor öffnen. Denn im Eigentum öffentlicher Stellen können nicht nur Gebäude, Fahrzeuge und Sachen von erheblichem Wert, sondern etwa auch Straßen, Spiel- und Marktplätze, Promenaden, Parkbänke, Fußgängerzonen, Freibäder und Fahrradwege stehen. Die öffentlichen Eigentümer könnten dann wie oben dargelegt vortragen, die Videoüberwachung dieser Orte sei eine erforderliche Maßnahme zum Schutz ihres Eigentums etwa vor Beschädigungen oder Verunreinigungen.

Mit einem an den Freiheitsrechten ausgerichteten Verfassungsverständnis, das die einzelnen Bürgerinnen und Bürgern bei ihrem Aufenthalt in öffentlich zugänglichen Räumen vor einer staatlichen Überwachung schützt, wäre eine solch allgegenwärtige Videoüberwachung nicht vereinbar. Das gegenwärtige Datenschutzniveau würde deutlich herabgesetzt.

Daher sollte der Tatbestand der Nr. 3 – wie unter den Anmerkungen zu Nr. 1 erläutert – durch die Tatbestände „zur Wahrnehmung des Hausrechts“ (Nr. 2) und „zur Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Stelle“ ersetzt werden.

Falls der Gesetzgeber abweichend davon eine eigene Zweckbestimmung „zum Schutz von Eigentum und Besitz“ aufnehmen möchte, sollte die Regelung neu gefasst und um einen Satz 2 in Absatz 1 ergänzt werden, um die erläuterten erheblichen datenschutzrechtlichen Bedenken auszuräumen:

- Nr. 3 neu könnte dann lauten: *„zum Schutz von Eigentum und Besitz der öffentlichen Stelle vor erheblichen Beeinträchtigungen“*
- Neuer Satz 2 in Absatz 1: *„In Fällen der Nr. 3 darf die Videoüberwachung keine Bereiche erfassen, in denen sich regelmäßig Personen rechtmäßig aufhalten“.*

Mit diesen Einschränkungen könnten Eigentum und Besitz der öffentlichen Stelle, die nicht dem Hausrecht unterfallen in einem begrenzten Umfang (keine Bagatellfälle) und in einer Weise geschützt werden, die eine dauerhafte Beobachtung von Personen nicht erlaubt.

Zu Nr. 4 („zur Kontrolle von Zugangsberechtigungen“):

Der ebenfalls im Entwurf neu aufgenommene Tatbestand erfasst sowohl Kontrollen an Gebäudeeingängen als auch Kontrollen von Zugängen innerhalb öffentlicher Gebäude zu besonders gesicherten Bereichen.

Für beide Arten der Zugangskontrolle sind regelmäßig weniger eingriffsintensive Maßnahmen im Einsatz: etwa eine Kontrolle durch Personal an der Eingangspforte und elektronische Schließ- und Zutrittskontrollsysteme für besonders gesicherte Gebäudebereiche.

Sollte ausnahmsweise eine Videoüberwachung für die Zutrittskontrolle erforderlich sein, kommt dafür – wie nach bisheriger Rechtslage – auch der Tatbestand „Wahrnehmung des Hausrechts“ in Betracht (jetzt in § 20 Absatz1 Nr. 2).

Eines eigenständigen Tatbestands bedarf es daher nicht. Ein speziell dafür geschaffener Tatbestand könnte vielmehr das Missverständnis hervorrufen, der Gesetzgeber halte die Videoüberwachung nicht nur im Ausnahme-, sondern im Regelfall für das angemessene Mittel der Zugangskontrolle.

§ 20 Absatz 1 sollte demnach wie folgt neu gefasst werden:

„Die Verarbeitung personenbezogener Daten in öffentlich zugänglichen Bereichen mittels optisch-elektronischer Einrichtungen (Videoüberwachung) durch öffentliche Stellen ist zulässig, wenn dies
1. *zur Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Stelle oder*
2. *zur Wahrnehmung des Hausrechts*

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.“

Alternative (hilfsweise; siehe zu Nr. 3.):

„Die Verarbeitung personenbezogener Daten in öffentlich zugänglichen Bereichen mittels optisch-elektronischer Einrichtungen (Videoüberwachung) durch öffentliche Stellen ist zulässig, wenn dies
1. *zur Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Stelle,*
2. *zur Wahrnehmung des Hausrechts oder*
3. *zum Schutz von Eigentum und Besitz der öffentlichen Stelle vor erheblichen Beeinträchtigungen*

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. In Fällen der Nr. 3 darf die Videoüberwachung keine Bereiche erfassen, in denen sich regelmäßig Personen rechtmäßig aufhalten.“

2. Die Ausgestaltung der Informationspflichten in Absatz 2 ist an die Anforderungen der Art. 12 ff. DSGVO anzupassen.

   Durch die DSGVO sind die Anforderungen an die Transparenz der Datenverarbeitung stark verschärft worden. Dementsprechend bestehen auch stark ausgeweitete Informationspflichten. Da die Videoüberwachung eine Datenerhebung beim Betroffenen darstellt, ergeben sich die erforderlichen Informationen aus Art. 13 DSGVO. Wie in der Gesetzesbegründung ausgeführt, sind die nicht direkt auf den Hinweisschildern befindlichen weiteren Pflichtinformationen am Ort der Videoüberwachung an einer für die betroffene Person zugänglichen Stelle zur Verfügung zu stellen, beispielsweise als vollständiges Informationsblatt (Aushang). Dies muss auch in der Gesetzesfassung zum Ausdruck gebracht werden, damit nicht der Eindruck entsteht, der Betroffene müsse die Informationen beim Verantwortlichen einholen.

3. Die Löschungsregelung in Absatz 4 sollte wie folgt gefasst werden:

   „Soweit nach Absatz 1 eine Speicherung der erhobenen Daten erfolgt, sind diese unverzüglich zu löschen, wenn sie zum Erreichen des verfolgten Zwecks nicht mehr erforderlich sind.“

   Die Formulierung in Absatz 1 S. 1 erweckt den Anschein, als ob alle Daten, die nach Absatz 1 erhoben werden, auch gespeichert werden. Dieser Automatismus ist jedoch nicht gegeben, da eine reine Beobachtung nach wie vor möglich und in vielen Fällen auch ausreichend ist.

   Im Normalfall dürfte bereits innerhalb weniger Tage geklärt werden können, ob eine Sicherung des Materials erforderlich ist. Wenn kein entsprechender Sicherungsgrund besteht, sind die Daten daher in der Regel bereits nach 1 – 2 Tagen, bei Wochenenden und Feiertagen gegebenenfalls etwas länger, zu löschen. Die Regelung einer Höchstfrist von 4 Wochen birgt die Gefahr, dass die Geschäftsprozesse, auf die die Entwurfsbegründung Bezug nimmt, von vorneherein so organisiert werden, dass erst zum Ende dieser Frist überprüft wird, ob eine Speicherung noch erforderlich ist. Die Aufbewahrung über den an sich erforderlichen Zeitraum hinaus würde daher prak-

tisch zu einer Datenvorratshaltung führen, die aus rechtsstaatlichen Gründen abzulehnen ist.

Zu § 22 d. E.

Die nach Absatz 4 für anwendbar erklärten Vorschriften sollten erweitert werden.

Die Verweisung auf die ausgewählten Regelungen in Absatz 4 erscheint zu eng. Zum Beispiel gäbe es dann wohl kein Recht auf Löschung (da Kapitel III DSGVO nicht für anwendbar erklärt wird); für die Ausnahme der Artikel 33 und 34 gibt es keinen Anlass. Möglicherweise bietet sich hier insgesamt eine spezialgesetzliche Regelung an.

Zu § 23 d. E.

Die Einführung von im Vergleich zum bisherigen DSG neuen Datenschutzregelungen ist zu begrüßen, da so eine Lücke geschlossen wird. Der Verweis auf die DSGVO ist grundsätzlich wie bei § 22 angemerkt zu erweitern (s.o.).

Der Ausschluss des Begnadigungsverfahrens von der Kontrolle durch den Landesbeauftragten entspricht im Ergebnis der bisherigen Rechtslage. Gleichwohl ist fraglich, warum hier weiterhin auf die Kontrolle durch den Landesbeauftragten und in der Konsequenz auch auf die Meldepflicht bei Schutzverletzungen verzichtet wird. Gerade im Begnadigungsverfahren können Schutzverletzungen erhebliche Folgen für die Betroffenen haben, so dass zumindest Art. 34 (Benachrichtigung der betroffenen Person bei Schutzverletzungen) gelten sollte.

Zu § 24 d. E.

Absatz 1 und Absatz 3 sollten gestrichen oder im Sinne der folgenden Ausführungen angepasst werden:

Der Landesgesetzgeber hat von seinem Ermessen nach Art. 35 Absatz 1 Satz 2 DSGVO Gebrauch gemacht und sog. kumulierte Datenschutz-

Folgenabschätzungen (DSFA) für den in Absatz 1 beschriebenen Fall zugelassen. Die Voraussetzung „im Wesentlichen unverändert“ lässt dabei nicht definierte Spielräume für Änderungen durch nachgeordnete Behörden bei der betreffenden Verarbeitung zu. Der Verordnungsgeber geht aber von dem Fall aus, dass entweder mehrere Verantwortliche gemeinsam eine DSFA durchführen oder ein Verantwortlicher für mehrere Einsatzbereiche einer Anwendung in seinem Verantwortungsbereich eine kumulierte DSFA durchführt (vgl. auch Working Paper 248 der Art.-29-Gruppe, Seite 8). Auch die in der Gesetzesbegründung vorgenommene Einschränkung genügt dem nicht: Eine vollständige Beurteilung der technischen Begebenheiten sowie eine realistische Einschätzung der potenziellen Risiken, die durch die Verarbeitung des Verantwortlichen im Einzelfall entstehen, sind regelmäßig nicht möglich, wenn die DSFA ohne Beteiligung der das Verfahren tatsächlich einsetzenden Stellen lediglich von der fachlich zuständigen obersten Landesbehörde oder von einer durch diese ermächtigten öffentlichen Stelle durchgeführt wurde.

Nachgeordnete Stellen, die ein vorgegebenes Verfahren einsetzen, aber an der DSFA der obersten Landesbehörde nicht beteiligt waren, müssen eine eigene DSFA durchführen. Dabei können sie Inhalte der DSFA der obersten Landesbehörde übernehmen, soweit die Übereinstimmungen reichen. Es sind bei einem Verfahren sowohl der Prozess als auch die Implementierung zu betrachten. Idealerweise wird bereits in der DSFA der obersten Landesbehörde vorgegeben, welche Freiheiten bei der Implementierung bestehen (Beispiel: Parametrisierung des Behördennamens, Referenzierung semantisch identischer, aber unterschiedlich benannter Rollen im Berechtigungskonzept), so dass die DSFA-Inhalte im Übrigen übertragbar sind und die Prüfung wesentlich erleichtert wird (vgl. § 24 Absatz 2 d. E.). Es verbleibt aber stets im Verantwortungsbereich jeder öffentlichen Stelle, zu überprüfen, ob jegliche besonderen Belange durch den konkreten Einsatz einer Anwendung vor Ort Berücksichtigung finden.

Hierzu hält EG 92 der DSGVO fest: „Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig sein, eine Datenschutz-Folgenabschätzung nicht lediglich auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen – beispielsweise wenn Behörden oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder

wenn mehrere Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten."

Beispiele hierfür enthalten die Leitlinien zur DSFA, Working Paper 248 der Art.-29-Gruppe, S. 8: „Verschiedene Gemeindebehörden, die alle eine ähnliche Videoüberwachungsanlage einrichten, könnten eine einzelne DSFA durchführen, mit der dann die Verarbeitung durch die einzelnen Verantwortlichen in allen diesen Behörden abgedeckt ist; oder ein Bahnbetreiber (ein einziger für die Verarbeitung Verantwortlicher) könnte für die Videoüberwachung all seiner Bahnhöfe eine einzige DSFA durchführen. Dies gilt unter Umständen auch für ähnliche Verarbeitungsvorgänge, die von verschiedenen für die Datenverarbeitung Verantwortlichen durchgeführt werden. In diesen Fällen ist es ratsam, eine Referenz-DSFA gemeinsam zu nutzen bzw. öffentlich zugänglich zu machen; zudem müssen die in der DSFA beschriebenen Maßnahmen umgesetzt und eine Begründung vorgelegt werden, warum eine einzige DSFA ausreichend ist."

Zu § 25 d. E.

1. Der LDI NRW sollte in Absatz 2 der Status einer obersten Landesbehörde zuerkannt werden.

   Da die LDI oberste Landesbehörden kontrolliert und diesen nun auch Anordnungen erteilen kann, sollte sie oberste Landesbehörde sein (vgl. § 8 BDSG (2018) zu der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, sowie die Stellung des Landesrechnungshofs in NRW).

2. Angesichts der bisher unbegrenzten Möglichkeit der Wiederwahl wäre die Möglichkeit einer zweimaligen Wiederwahl in Absatz 3 Satz 1 nicht unangemessen.

3. Zu Absatz 5 Satz 2:
   Art. 53 Absatz 3 DSGVO regelt, dass das Amt eines Mitglieds unter anderem mit seinem Rücktritt endet. § 23 Absatz 5 Satz 2 d. E. weist lediglich darauf hin, dass das Amtsverhältnis, neben den in Artikel 53

Absatz 3 DSGVO genannten Gründen, mit dem Rücktritt endet. Damit wird ein schon in der DSGVO geregelter Beendigungstatbestand wiederholt. Eine gegebenenfalls national regelbare Ausgestaltung dieses Beendigungstatbestandes ist nicht ersichtlich und wohl auch nicht erforderlich.

4. Die Zuständigkeit der Richterdienstgerichte zur Entscheidung über die in Absatz 5 Satz 3 genannte Amtsenthebungsvoraussetzung sollte ergänzt werden.

   Art. 53 Absatz 4 DSGVO sieht neben der in Absatz 5 Satz 3 Amtsenthebungsvoraussetzung eine Amtsenthebung auch vor, wenn die „Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt“ sind. Das DSG NRW enthält bisher keine Regelung dazu, wer in diesem Fall über eine Amtsenthebung entscheidet. Der entsprechende Wortlaut sollte daher in Absatz 5 Satz 3 aufgenommen werden.

Zu § 27 d. E.

1. Zu Absatz 3:
   Die Regelung würde zu einer substanziellen Absenkung des jetzigen Datenschutzniveaus in einem besonders sensiblen Bereich führen.

   Nach geltender Rechtslage bezieht sich die Kontrollbefugnis auch auf die Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen. Nunmehr sollen die Daten, die dem Steuergeheimnis oder der anwaltlichen oder ärztlichen Schweigepflicht und darüber hinaus vielen möglichen anderen Geheimhaltungspflichten unterliegen, der Zuständigkeit der LDI NRW entzogen werden. Welche sachlichen Argumente zu dem Plan geführt haben, gerade diese für die Betroffenen besonders wichtigen Bereiche von der Datenschutzkontrolle völlig auszunehmen, ist nicht erkennbar. Die Vorschrift verletzt damit auch die Vorgaben der DSGVO. Art. 90 Absatz 1 DSGVO gestattet nur notwendige und verhältnismäßige Beschränkungen der Aufsicht gegenüber Personen, die aufgrund einer Rechtsvorschrift einem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen. Die datenschutzrechtliche Aufsicht dient gerade

der Kontrolle des Umgangs des Berufsgeheimnisträgers mit personenbezogenen Daten und damit auch dem Schutz der Betroffenen auf Vertraulichkeit ihrer Daten. Die Befugnis, Datenschutzüberprüfungen durchzuführen, und alle sonstigen Kontrollbefugnisse der Aufsichtsbehörden müssen daher nach der DSGVO unangetastet bleiben.

Es ist im Übrigen auch vor dem Hintergrund der praktischen Erfahrungen in der Vergangenheit nicht nachvollziehbar, warum in einem so weiten und datenschutzrechtlich sensiblen Bereich die Kontrolle beschränkt sein soll. Seit Jahrzehnten haben die Aufsichtsbehörden auch Kontrollbefugnisse gegenüber strafrechtlichen Ermittlungsbehörden, ja sogar gegenüber Verfassungsschutzbehörden. In diesem Zusammenhang sind ebenfalls Geheimhaltungsinteressen zu beachten und zu wahren, die mindestens so bedeutsam sind wie die bestimmter Berufsgeheimnisträger. Dennoch ist die Kontrollkompetenz gerade in diesen für Betroffene auch sehr sensiblen und für den Datenschutzstandard im Land bedeutenden Bereichen unangefochten.

Weder die Betroffenenrechte noch die unterstützende Kontrollkompetenz der Datenschutzbeauftragten dürfen daher bei Berufsgeheimnisträgern beschnitten werden. Vielmehr ist eine wirksame datenschutzrechtliche Kontrolle, auch von Amts wegen, besonders vonnöten. Nach der geplanten Vorschrift wäre in Fällen, in denen standesrechtliche Verstöße auf der Nichteinhaltung der Verschwiegenheitspflicht beruhen – bisher ein typischer datenschutzrechtlicher Prüffall bezogen auf Ärzte – eine aufsichtsrechtliche Tätigkeit unmöglich, wenn sich der Berufsgeheimnisträger auch gegenüber der Aufsichtsbehörde auf die Verschwiegenheit berufen könnte. Hierdurch würden die zur Geheimhaltung von (Gesundheits-) Daten Verpflichteten unangemessen gegenüber den Betroffenen bevorzugt, indem sie von datenschutzaufsichtlichen Prüfungen verschont bleiben sollen. Die Schweigepflicht würde nach dieser Regelung zudem zu einem Instrument des verminderten Schutzes der Betroffenen führen. Abgesehen von Fällen erforderlicher Prüfung von Amts wegen, bei denen keine Schweigepflichtentbindung eingeholt werden kann, weil die Betroffenen namentlich noch nicht bekannt sind, gibt es auch Fälle mit Drittbetroffenheit, in denen die Einhaltung des Datenschutzes aufgrund der Verweigerung der Einwilligung des Patienten

nicht kontrolliert werden könnte.

In der Begründung wird die Einfügung auch mit der Bezugnahme auf § 29 Absatz 3 BDSG (2018) begründet. Für diese Vorschrift wiederum wurden die Grundsätze angeführt, die das BVerfG in seinem Urteil vom 12.04.2005 (BVerfG, Beschluss vom 12.04.2005 – 2 BvR 1027/02 – s. Entwurfsbegründung) hervorgehoben hat. In dem vom BVerfG entschiedenen Fall ging es jedoch um den Schutz der Verschwiegenheit im anwaltlichen Mandatsverhältnis gegenüber der Beschlagnahme durch staatliche Ermittlungsbehörden. Die Argumentation ist daher nicht auf die Kontrolle durch unabhängige Aufsichtsbehörden übertragbar. Die Aufgabe der unabhängigen Aufsichtsbehörden besteht gerade in der Überprüfung der Geheimhaltung und der Einhaltung der datenschutzrechtlichen Anforderungen und nicht in der Verfolgung sonstiger Straftaten.

Die Regelung des Absatzes 3 sollte daher ersatzlos entfallen.

2. Zu Absatz 4 Satz 3:

Eine Beschränkung der Befugnisse der oder des Landesbeauftragten bei besonderer Zusicherung der Vertraulichkeit gegenüber betroffenen Personen gemäß § 22 Absatz 2 Satz 5 DSG NRW ist in der DSGVO nicht vorgesehen und daher durch den nationalen Gesetzgeber nicht mehr regelbar. Die Regelung sollte daher entfallen.

Zu § 31 d. E.

Es besteht praktischer Bedarf nach einer Regelung zur organisatorischen Umsetzung der Meldepflicht der Kontaktdaten der Datenschutzbeauftragten (Art. 37 Absatz 7 DSGVO). Aus dieser folgt, dass die Aufsichtsbehörden ein Register über die gemeldeten Kontaktdaten im öffentlichen und nicht-öffentlichen Bereich führen müssen, das wegen des enormen Umfangs sinnvoll nur in elektronischer Form geführt werden kann. Für die erforderliche Mitteilung der Kontaktdaten in elektronischer Form plant die LDI NWR eine Online-Lösung, bei der jeder Verantwortliche die Kontaktdaten auf der Webseite der LDI NRW selbst eingibt und pflegt. Die Verantwortlichen sollten dazu angehalten werden, dieses Online-Mitteilungssystem zu nutzen und von anderen Kommunikationswe-

gen abzusehen, um den sonst entstehenden erheblichen Verwaltungsaufwand für die Registrierung und Pflege der Meldungen zu vermeiden. Jedenfalls für öffentliche Stellen sollte dazu eine gesetzliche Verpflichtung geschaffen werden.

Zu § 32 d. E.

Die Regelung schließt Geldbußen nach der DSGVO für andere öffentliche Stellen aus. Für die Möglichkeit von Geldbußen gegen alle öffentlichen Stellen spricht dagegen die flächendeckende und einheitliche Gewährleistung der Durchsetzung der DSGVO. Das deutsche Ordnungswidrigkeitenrecht schließt die Verhängung von Geldbußen gegen juristische Personen des öffentlichen Rechts nicht aus. Von der Regelung sollte daher Abstand genommen werden.

Zu § 33 d. E.

1. In Absatz 1 sollte klargestellt werden, dass die Vorschrift nur für Beschäftigte von Verantwortlichen und Auftragsverarbeitern gelten soll.

   Vom Wortlaut umfasst sind auch Verstöße, die die DSGVO bereits regelt (Täter: Verantwortliche und Auftragsverarbeiter). Aus der Begründung ergibt sich, dass die Regelung (nur) Mitarbeiter betreffen soll. Durch eine entsprechende Klarstellung sollte der Eindruck vermieden werden, dass die Regelung gegen die DSGVO verstößt.

2. Der Wortlaut sollte an die Terminologie der DSGVO angepasst werden, indem auf die Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO Bezug genommen wird.

3. Für die neue Zuständigkeit nach Absatz 3 wird die LDI mehr Personal benötigen.

Teil 3
Umsetzung der Richtlinie (EU) 2016/680

Mit Teil 3 des Entwurfs soll die JI-RL im Allgemeinen umgesetzt werden. Jedoch eignen sich Regelungsbereiche der JI-RL, die konkrete Anforderungen an die Datenverarbeitung stellen, nicht für eine solch allgemeine Umsetzung. Dies gilt insbesondere für Ermächtigungsgrundlagen zur Datenverarbeitung und Regelungen zu Zweckänderungen (beispielsweise §§ 3, 39 und 45 d. E.). Hier sind Regelungen unmittelbar in den jeweiligen bereichsspezifischen Normen angezeigt. Im DSG NRW sollten hierzu allenfalls übergeordnete oder ergänzende Regelungen getroffen werden. Zu diesen und weiteren Punkten nehme ich wie folgt Stellung:

Zu § 36 d. E.

In § 36 Nr. 8 d. E. ist zu prüfen, ob die Stellen aus § 35 Absatz 2 d. E. ebenfalls aufzunehmen sind. Entsprechend der Begriffsbestimmung des Art. 3 Nr. 7 JI-RL sollten alle Stellen erfasst sein, die die JI-RL und die zu ihrer Umsetzung erlassenen Vorschriften anwenden. Das ist bis jetzt noch nicht der Fall.

Zu § 39 d. E.

Die materiell-rechtlichen Anforderungen für Datenverarbeitungen zu anderen Zwecken als dem Erhebungszweck sollten ausschließlich in bereichsspezifischen Regelungen getroffen werden.

Die in § 39 d. E. getroffene Regelung erfolgt in der gleichen generalklauselartigen Form, wie in § 3 d. E. in Bezug auf die grundsätzliche Zulässigkeit der Verarbeitung personenbezogener Daten. § 39 d. E. ist daher aus denselben Gründen zu kritisieren. Die Vorschrift ist zu allgemein, um den besonderen Anforderungen gerecht zu werden, die an die verschiedenen Formen der Datenverarbeitung zu richten sind. Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016 (1 BvR 966/09 und 1 BvR 1140/06) zum Bundeskriminalamtgesetz (BKAG) dezidierte Ausführungen dazu gemacht, wann bei Datenverarbeitungen durch Sicherheitsbehörden eine Zweckänderung vorliegt und unter wel-

chen Voraussetzungen die Verarbeitung personenbezogener Daten zu einem anderen Zweck als dem Erhebungszweck zulässig ist. Danach dürfen Informationen, die durch besonders eingriffsintensive Maßnahmen (beispielsweise Wohnungsdurchsuchung) erlangt wurden, auch nur zu besonders gewichtigen Zwecken (beispielsweise Abwehr erheblicher Straftaten) genutzt werden. Eine entsprechende Einschränkung enthält § 39 d. E. jedoch nicht. Es ist nicht ersichtlich, warum es überhaupt einer allgemeinen Regelung im DSG NRW bedürfen soll. Stattdessen böte es sich an, in das DSG NRW lediglich eine allgemeine Definition des Begriffs der Zweckänderung gemäß den Vorgaben des BVerfG-Urteils aufzunehmen.

Zu § 40 d. E.

Unklar ist, ob es sich um eine bloße Zweckänderungsregelung oder sogar um eine Rechtsgrundlage für die Verarbeitung von Daten handeln soll. Im letzteren Fall wäre die Regelung zu unbestimmt. Auch weiterhin sind spezifische Forschungsklauseln in den jeweiligen Regelungszusammenhängen bereichsspezifischer Gesetze erforderlich.

Zu § 45 d. E.

§ 45 d. E. wird den Vorgaben der JI-RL durchweg nicht gerecht. Die Regelung materiell-rechtlicher Vorgaben für die Verarbeitung besonderer Kategorien personenbezogener Daten im Anwendungsbereich der JI-Richtlinie sollte nicht im DSG NRW, sondern ausschließlich in bereichsspezifischen Normen erfolgen.

§ 45 Absatz 1 d. E. unterläuft die in Art. 10 JI-RL normierten Voraussetzungen. Art. 10 JI-RL verlangt neben der „unbedingten Erforderlichkeit“ und den Garantien das zusätzliche Vorliegen einer der drei Voraussetzungen a) „nach dem Recht … zulässig ist“, b) „dient lebenswichtigen Interessen“ oder c) „offensichtlich öffentlich“. § 45 d. E. lässt aber schon ausreichen, dass entsprechende Garantien im Sinne des Absatz 2 vorliegen und die Datenverarbeitung unbedingt erforderlich ist. Eine der oben genannten drei weiteren Voraussetzungen schreibt § 45 d. E., entgegen den Vorgaben der Richtlinie, nicht fest. Die Vorschrift bleibt damit hinter der Regelung des Art. 10 JI-RL zurück.

Der Gesetzgeber hat konkret festzulegen, unter welchen Voraussetzungen und Bedingungen besondere Kategorien personenbezogener Daten verarbeitet werden dürfen. Die Möglichkeiten und Begrenzungen, solche Daten zu verarbeiten, müssen unter Angabe der Art der Daten, der Zwecke und der Ziele der Verarbeitung sowie der im konkreten Fall geforderten geeigneten Garantien in der Ermächtigungsgrundlage geregelt werden. Dies ist in einer allgemeinen Regelung nicht möglich. Zudem könnte § 42 d. E. dazu führen, dass auf eine fachgesetzliche Konkretisierung verzichtet und stattdessen auch für besonders eingriffsintensive Datenverarbeitungen auf diese Generalklausel zurückgegriffen wird.

Zu § 46 d. E.

§ 46 d. E. genügt den Vorgaben des Art. 11 JI-RL nicht.

Nach Art. 11 JI-RL sind automatisierte Entscheidungsfindungen, die eine nachteilige Folge für eine betroffene Person haben oder diese erheblich beeinträchtigen, grundsätzlich unzulässig. Sie sind nur ausnahmsweise dann zulässig, wenn es eine Ermächtigungsgrundlage gibt, die geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet, mindestens jedoch das Recht der betroffenen Person auf persönliches Eingreifen seitens des Verantwortlichen vorsieht. In § 46 Absatz 1 d. E. werden die Forderungen der JI-RL nach geeigneten Garantien und dem persönlichen Eingreifen des Verantwortlichen unberücksichtigt gelassen. Art. 11 Absatz 1 JI-RL wird damit durch § 46 Absatz 1 d. E. nicht umgesetzt.

Zwar berücksichtigt der Entwurf die Forderung geeigneter Garantien für automatisierte Entscheidungen auf der Grundlage besonderer Kategorien personenbezogener Daten nach Art. 11 Absatz 2 JI-RL in § 46 Absatz 2 d. E. In diesem Bereich sind die Risiken automatisierter Entscheidungen aufgrund der besonderen Sensibilität der Daten jedoch besonders signifikant. Es wäre deshalb zu empfehlen, auf automatisierte Entscheidungen vollständig zu verzichten.

Sollte dennoch in Betracht gezogen werden, für besondere Ausnahmen automatisierte Einzelfallentscheidungen zuzulassen, müssten hierfür konkrete bereichsspezifische Vorschriften geschaffen werden. Dabei sind die Vorgaben der JI-RL, insbesondere die Schaffung geeigneter

Garantien sowie das jederzeitige Recht der betroffenen Person, das persönliche Eingreifen des Verantwortlichen zu fordern, in jedem Fall zu berücksichtigen.

Zu § 49 d. E.

Es sollte klargestellt werden, dass § 49 Absatz 1 d. E. einen Anspruch auf eine Negativauskunft einschließt (vgl. Art. 14 JI-RL sowie Erwägungsgrund 43).

Art. 15 JI-RL regelt, dass der nationale Gesetzgeber zu den dort genannten Zwecken Einschränkungen im Wege von Gesetzgebungsmaßnahmen regeln kann. Absatz 4 i. V. m. § 48 Absatz 2 d. E. wiederholt Art. 15 Absatz 1 JI-RL jedoch lediglich in Teilen. Damit ist der Umsetzung nicht Genüge getan. Art. 15 JI-RL ermöglicht vielmehr zu den dort genannten Zwecken spezielle Regelungen, die in den bereichsspezifischen Normen getroffen werden sollten.

In Absatz 6 Satz 2 sollte das Wort „wenn“ durch „soweit“ ersetzt werden. Dies stellt klar, dass nicht zwingend die gesamte Information nach Satz 1 unterlassen werden darf, nur weil die Ausnahme nach Satz 2 teilweise greift. Insofern entspricht die Änderung dem „soweit“, dass auch bereits in § 48 Absatz 2 und § 49 Absatz 4 i. V. m. § 48 Absatz 2 d. E. normiert ist. Absatz 6 Satz 3 sollte dementsprechend umgestellt werden und nach „zu begründen“ lauten: „soweit die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck nicht gefährdet.“ Hierdurch wird klargestellt, dass nicht die gesamte Begründung nach Satz 3 unterlassen werden darf, wenn die Ausnahme nur teilweise greift.

Absatz 7 sollte lauten: „Soweit die betroffene Person nach Absatz 6 zu unterrichten ist, kann sie ….“. Dies stellt klar, dass die betroffene Person von der Möglichkeit, das Auskunftsrecht über die LDI NRW auszuüben, auch dann Gebrauch machen kann, wenn der Verantwortliche eine mangels Ausnahme nach Absatz 6 Satz 2 abzugebende Mitteilung (pflichtwidrig) unterlässt. Bisher ist es von der tatsächlich vorgenommenen Mitteilung abhängig, ohne Rücksicht darauf, ob diese rechtmäßig oder rechtswidrig unterblieben ist.

Zu § 51 d. E.

Der Begriff „exzessiv“ in § 51 Absatz 3 d. E. sollte konkretisiert werden. Dies könnte in Anlehnung an Art. 12 Absatz 4 JI-RL („insbesondere im Fall häufiger Wiederholung“) erfolgen. Vorgeschlagen wird die Formulierung: „insbesondere im Fall häufiger sachgrundloser Wiederholung“. Dies dient der Bestimmtheit der Vorschrift. Das Kriterium des Fehlens eines Sachgrundes für die wiederholte Antragstellung sollte aufgenommen werden, denn wenn der Antrag nicht bearbeitet wird, besteht gerade ein Sachgrund für eine wiederholte Antragstellung.

Zu § 55 d. E.

Die Regelung zur Protokollierung sollte ergänzt werden. Die Vorgaben des Art. 25 JI-RL dürfen trotz ihres Umfangs und Detaillierungsgrades nicht als abschließende Vollregelung verstanden werden. Weder legt Art. 25 JI-RL abschließend alle revisionssicher auszugestaltenden Prozesse fest (beispielsweise sind Ordnen und Organisieren nicht erfasst), noch trifft die Vorschrift alle für den Umfang mit Protokolldaten erforderlichen Regelungen. Insbesondere enthält sie keine Regelung, nach welchen Kriterien bzw. unter welchen Voraussetzungen mehr als die genannten Verarbeitungsschritte zu protokollieren sind. Dies ist jedoch zu regeln, um klarzustellen, wann welche Verarbeitungsvorgänge über die in § 55 d. E. genannten hinaus – beispielsweise zur Erfüllung der Verpflichtung aus § 58 d. E. – zu protokollieren sind. Darüber hinaus sollte deutlich gemacht werden, dass auch Verarbeitungen durch den Administrator von § 55 d. E. erfasst sind. Ebenfalls bisher nicht erfasst ist die Protokollierung automatisierter Datenübertragungen an Schnittstellen zu anderen Verfahren.

Das Aufgreifen meiner Position, dass Protokolldateien einerseits baldmöglichst zu löschen sind, andererseits aber ausreichend lange aufbewahrt werden müssen, um es den Betroffenen zu ermöglichen, die Verarbeitung ihrer Daten zur Überprüfung der Rechtmäßigkeit der Verarbeitung nachvollziehen zu können, in der Gesetzesbegründung zu § 55 Absatz 4 d. E. ist zu begrüßen. Die vorgeschlagene starre Jahresfrist wird diesen Vorgaben allerdings nicht gerecht. Die in Absatz 4 vorgesehene Löschung am Ende des auf die Generierung folgenden Jahres erfüllt die sich aus der Entscheidung des EuGH in der Rechtssache

C-553/07 (Rijkeboer) ergebenden Anforderungen nämlich nicht. Die Protokolldaten sollten daher grundsätzlich so lange gespeichert werden, wie auch die ihnen zu Grunde liegenden Datensätze gespeichert sind, mindestens aber, bis die betroffene Person ausreichend Gelegenheit hatte, die rechtmäßige Verarbeitung ihrer Daten prüfen zu lassen.

Die in § 55 Absatz 3 d. E. vorgesehene Regelung lässt in Bezug auf Strafverfahren offen, ob und unter welchen konkreten Voraussetzungen gespeicherte Protokolldaten hierfür verwendet werden dürfen. Protokollierung ist eine Verfahrenssicherung, die den Grundrechtseingriff der Datenverarbeitung abmildern soll. Sie darf deshalb nicht ihrerseits zu Grundrechtsverletzungen führen. Eine Nutzung von Protokolldaten kommt somit allenfalls für Verfahren bezüglich Straftaten von besonderem Gewicht in Betracht. Die vorgesehene Regelung sollte daher konkretisiert werden.

Zu § 56 d. E.

In Absatz 4 Satz 1 sollte es statt nur „… den berechtigten Interessen...“ „den Rechten und berechtigten Interessen“ heißen. Dies entspricht der Vorgabe des Art. 27 Absatz 2 JI-RL. Den berechtigten Interessen des Verantwortlichen, welche über den Verweis auf Art. 35 Absatz 7 lit. a DSGVO zu beschreiben sind, sollen sowohl die Rechte, als auch die berechtigten Interessen der betroffenen Personen gegenübergestellt werden und somit in den Abwägungsprozess der Folgenabschätzung miteinbezogen werden.

Zu § 58 d. E.

Redaktioneller Hinweis: In Absatz 4 müsste es „Zur Umsetzung von Absatz 3“ statt „Absatz 2“ heißen.

Zu den §§ 62 bis 65 d. E.

Die Vorschriften zu Datenübermittlungen ins Ausland entsprechen nicht den verfassungsrechtlichen Vorgaben, wie sie das BVerfG zuletzt um-

fassend in seinem Urteil zum BKAG (1 BvR 966/09 und 1 BvR 1140/09, Randnummern 329-341) zusammengefasst hat:

Da die Übermittlung von Daten, die ursprünglich zu anderen Zwecken erhoben wurden, an einen anderen Verantwortlichen eine Zweckänderung darstellt, gelten zunächst die Ausführungen des BVerfG zu Zweckänderungen entsprechend. Hinzukommen Anforderungen zur Sicherstellung, dass im Empfängerland generell oder zumindest im Einzelfall ein gewisser Datenschutzstandard eingehalten wird. Danach erfordert die Datenübermittlung staatlicher Stellen in Deutschland an staatliche Stellen im Ausland grundsätzlich eine Begrenzung auf hinreichend gewichtige Zwecke, für die die Dateien übermittelt und genutzt werden dürfen, die Vergewisserung über einen rechtsstaatlichen Umgang mit diesen Daten im Empfängerland, die Sicherstellung einer wirksamen inländischen Kontrolle und entsprechende normenklare Grundlagen im deutschen Recht (vgl. Randnummern 329 f. a.a.O.).

Diese Vorgaben des BVerfG zur zweckändernden Weitergabe an Drittstaaten und internationale Organisationen berücksichtigt der Entwurf nicht in ausreichendem Maße. Er enthält teilweise fast uferlose Übermittlungsgrundlagen. Besonders erwähnt sei an dieser Stelle § 64 Absatz 1 Nr. 4 d. E. Danach ist die Übermittlung sämtlicher personenbezogener Daten, selbst solcher, die mittels Online-Durchsuchungen erhoben wurden, ohne weitere Voraussetzungen zulässig, solange die Daten für einen Zweck nach § 35 d. E. erforderlich sind. Hierzu gehören jedoch sämtliche Fälle von Gefahrenabwehr und Strafverfolgung. Die mittels Online-Durchsuchung erhobenen Daten dürften somit auch zur Verfolgung von Bagatelldelikten übermittelt werden. Dies widerspricht den verfassungsrechtlichen Vorgaben, die das BVerfG im o.g. Urteil zusammengefasst hat.

Im Einzelnen ist zu den genannten Vorschriften noch Folgendes anzumerken:

In § 62 Absatz 2 d. E. fehlen Vorgaben, wie die Sicherheitsbehörden das vom BVerfG geforderte gewisse Datenschutzniveau im Empfängerland feststellen können sollen. Das BVerfG hat hierzu ausführliche Vorschläge unterbreitet, die im Entwurf nicht aufgegriffen werden. Dabei ist zu betonen, dass sämtliche vorgenannten verfassungsrechtlichen Anforderungen selbst dann in den Vorschriften der §§ 59 ff. d. E. zu be-

rücksichtigen sind, wenn diese lediglich Auffangtatbestände darstellen sollen. Jede Ermächtigungsgrundlage, auf die Datenübermittlungen in Drittstaaten gestützt werden können, muss allen verfassungsrechtlichen Vorgaben entsprechen.

Kapitel 6 setzt außerdem die Vorgaben der JI-RL nicht vollständig um und bedarf der Klarstellung. So fehlt beispielsweise in § 62 d. E. ein Verweis darauf, dass die Übermittlung für die in § 35 Absatz 1 d. E. genannten Zwecke erforderlich sein muss (s. Art. 35 Absatz 1 lit. a JI-RL). Klarstellungen sind außerdem in § 62 Absatz 1 Nr. 1 d. E. mit Blick auf Art. 35 Absatz 1 lit. b JI-RL hinsichtlich § 36 Nr. 8 d. E. erforderlich.

Zur Umsetzung von Art. 37 Absatz 1 lit. a) und b) JI-RL ist § 63 Absatz 1 Nr. 1 d. E. hinsichtlich der Begriffe „rechtsverbindliches Instrument“ und „geeignete Garantien“ zu konkretisieren (siehe Erwägungsgrund 71 JI-RL). Der Umsetzungsspielraum hinsichtlich des Begriffes „geeignete Garantien“ muss dabei nach Maßgabe der vom BVerfG in seiner Entscheidung zum BKAG vom 20. April 2016 (1 BvR 966/09 und 1 BvR 1140/09, Randnummern 329-341) aufgestellten Anforderungen ausgefüllt werden.

In § 64 d. E. ist der Katalog der potentiellen Ausnahmen sehr weit gefasst und im Lichte eines effektiven Datenschutzes restriktiv auszulegen. Diese sind auf unbedingt notwendige Daten zu beschränken und nicht für häufige, umfassende und strukturelle Übermittlungen personenbezogener Daten sowie Datenübermittlungen im großen Umfang vorzusehen (siehe Erwägungsgrund 72 JI-RL).

Zu § 67 d. E.

Der Verweis auf Art. 26 DSGVO in dieser Form erscheint nicht stimmig. In Art. 21 JI-RL ist nämlich geregelt, dass zwingend („wird“) eine Anlaufstelle anzugeben ist. In Art. 26 DSGVO „kann“ dies lediglich erfolgen

Zu § 69 d. E.

Auf die Ausführungen zu § 33 d. E. wird verwiesen.

C Weitere Regelungsbedarfe

1. Direkterhebungsgrundsatz

Der bisher in § 12 Absatz 1 Satz 3 DSG geregelte Direkterhebungsgrundsatz ist im Bereich der Erfüllung öffentlicher Aufgaben weiterhin, z. B. als eigener Absatz in § 3, ausdrücklich festzuschreiben.

Eingriffe in das Recht auf informationelle Selbstbestimmung müssen verfassungskonform, insbesondere verhältnismäßig sein. Hierzu gehört, dass Datenerhebungen grundsätzlich unmittelbar bei der betroffenen Person und mit ihrer Kenntnis zu erheben sind: Bei einer persönlichen Befragung kann die betroffene Person ihr Recht, selbst über die Preisgabe ihrer Daten zu bestimmen, am ehesten ausüben. Befragungen Dritter bringen demgegenüber eine Information dieser Dritten über die Datenerhebung mit sich. Außerdem bergen sie die Gefahr weiterer, nicht erforderlicher Datenübermittlungen an diese Dritten und überschießender Datenübermittlungen der Dritten an den Verantwortlichen. Dies muss immer wo es möglich ist vermieden werden. Der Direkterhebungsgrundsatz ist daher weiterhin, z. B. als eigener Absatz in § 3, zu regeln. Die Öffnungsklausel hierfür liegt in Art. 6 Absatz 2 DSGVO.

2. Durchsetzbarkeit der Abhilfebefugnisse nach Art. 58 Absatz 2 DSGVO

Die Befugnisse, die der Aufsichtsbehörde durch die Grundverordnung zugewiesen sind, müssen im Recht der Mitgliedstaaten auch durchsetzbar sein, damit die Befugnisse effektiv ausgeübt werden können. Anweisungen etwa sind als Verwaltungsakte gegenüber nicht-öffentlichen Stellen über Verwaltungszwang nach dem Verwaltungsvollstreckungsgesetz durchsetzbar. Anweisungen gegenüber anderen Behörden sind jedoch mangels Außenwirkung, z. B. gegenüber Landesbehörden, in den meisten Fällen nicht als Verwaltungsakte qualifizierbar und deshalb auch nicht über das VwVG durchsetzbar. Gegen Behörden und juristische Personen des öffentlichen Rechts sind zudem Zwangsmittel unzulässig, soweit nicht etwas anderes bestimmt ist (§ 76 VwVG NRW, abweichende Regelungen z. B. in § 17 FinDaG, § 76 WVG, § 22 Absatz 3 Satz 4 ArbSchG).

Es ist daher geboten, eine Durchsetzbarkeit im Landesrecht zu ermöglichen, indem eine Abweichung von § 76 VwVG NRW geregelt wird und die Problematik der Verwaltungsaktqualität gelöst wird (z. B. durch Regelung im DSG NRW, dass Anweisungen, Anordnungen und sonstige Regelungen im Rahmen der Befugnisse nach Art. 58 DSGVO gegenüber öffentlichen Stellen mit den Mitteln des Verwaltungszwangs durchgesetzt werden können).

Dem müsste auch eine Rechtsschutzmöglichkeit entsprechen, die derzeit jedenfalls für Landesbehörden (Prozess Land./.Land) nicht besteht. Diese Rechtsschutz-Problematik stellt sich auch bei den Durchsetzungsinstrumenten an sich (z. B. Anordnungen gegen Landesbehörden).

Außerdem müssten Regelungen geschaffen werden, die es ermöglichen, dass gerichtliche Auseinandersetzungen zwischen dem Land Nordrhein-Westfalen, vertreten durch die LDI NRW und dem Land Nordrhein-Westfalen, vertreten durch die jeweilige verantwortliche öffentliche Stelle des Landes, geführt werden können. Hier fordern sowohl DSGVO als auch JI-RL eine aktive Möglichkeit, Gerichtsverfahren direkt oder indirekt einzuleiten (z. B. Art. 58 Absatz 5 DSGVO, vgl. hierzu Erwägungsgrund 129).

3. Verschwiegenheitspflicht der LDI NRW und ihrer Bediensteten

Artikel 54 Absatz 2 DSGVO und Artikel 44 Absatz 2 JI-RL sehen eine Verschwiegenheitspflicht aller Mitglieder und Bediensteten der Aufsichtsbehörde „gemäß dem Unionsrecht oder dem Recht der Mitgliedsstaaten“ vor. Es ist daher entweder eine eigene nationale Reglung zu schaffen oder auf das Unionsrecht zu verweisen. Im Entwurf fehlt eine derartige ausdrückliche Verschwiegenheitsverpflichtung.

Nach § 37 Beamtenstatusgesetz haben Beamtinnen und Beamte über die ihnen bei oder bei Gelegenheit ihrer amtlichen Tätigkeit bekannt gewordenen dienstlichen Angelegenheiten Verschwiegenheit zu bewahren. Fraglich ist, ob diese Regelung eine ausreichende Verschwiegenheitsverpflichtung im Sinne der DSGVO bzw. JI-RL darstellt. Weiterhin ist fraglich, nach welchen gesetzlichen Vorschriften im Sinne des § 3 Absatz 2 Tarifvertrag für den öffentlichen Dienst der Länder Beschäftigte bei der Aufsichtsbehörde zur Verschwiegenheit verpflichtet sind.

Durch nationale Regelungen muss gem. Art. 54 Absatz 2 DSGVO sichergestellt werden, dass alle Beschäftigten der Aufsichtsbehörde einer Verschwiegenheitspflicht unterliegen.

4. Gebühren

Es sollten die Voraussetzungen einer Gebührenerhebung für die Tätigkeit der LDI NRW in Einzelfällen geschaffen werden.

Art. 57 Absatz 3 DSGVO und Art. 46 Absatz 3 JI-RL gehen von einer grundsätzlichen Unentgeltlichkeit der Aufgabenerfüllung der Datenschutzaufsicht aus. Dies betrifft insbesondere die Befassung mit Eingaben von betroffenen Personen und die Kooperation mit den Datenschutzbeauftragten. Möglich ist eine Kostenerhebung (Gebühren und Auslagen) von betroffenen Personen und Datenschutzbeauftragten bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen (Art. 57 Absatz 4 DSGVO und Art. 46 Absatz 4 JI-RL). Weitere Kostenerhebungen gegenüber Verantwortlichen und anderen Stellen gemäß DSGVO sowie JI-Richtlinie sind nach allgemeiner Ansicht nicht ausgeschlossen. Eine effektive Durchsetzung der DSGVO und JI-RL verlangt jedoch, dass unverhältnismäßig hohe Kosten Verantwortliche und Auftragsverarbeiter nicht von der Konsultation der Datenschutzaufsicht abhalten. Zumindest im Rahmen des Akkreditierungsverfahrens und aufwändigen und intensiven Beratungen mit stark kommerziellem Nutzen der Beratenen sollte aber ein Gebührentatbestand geschaffen werden. Die Unabhängigkeit der Landesdatenschutzbeauftragten erfordert gegebenenfalls ihr Einvernehmen bei der Festlegung.

Artikel 2
Änderung des Informationsfreiheitsgesetzes Nordrhein-Westfalen

A. Allgemeines

Die Entscheidung, das Anrufungsrecht sowie die Aufgaben und Befugnisse der oder des Landesbeauftragten nunmehr im Wege einer Vollre-

gelung im IFG NRW selbst zu normieren, findet meine ausdrückliche Zustimmung.

Im Entwurf fehlen nach aktueller Rechtslage bestehende Zuweisungen von Aufgaben und Befugnissen: Das aktuelle IFG NRW enthält in § 13 Absatz 2 Satz 2 IFG NRW einen Verweis auf das DSG NRW. Umfasst von diesem Verweis sind §§ 22, 24 DSG NRW. Dies ergibt sich aus der Gesetzesbegründung vom 12.06.2001, Drs. 13/1311, S. 15:

„Besondere Regelungen für die Aufgaben und Befugnisse der oder des Landesbeauftragten für den Datenschutz im Hinblick auf die Durchführung dieses Gesetzes werden nicht getroffen. Stattdessen wird in Absatz 2 auf die Regelungen des Datenschutzgesetzes Nordrhein-Westfalen verwiesen."

Aufgaben und Befugnisse sind bisher in § 22 DSG NRW geregelt. § 13 d. E. übernimmt lediglich einige der in § 22 DSG NRW genannten Befugnisse. Die Vollregelung muss daher um die sinngemäßen Inhalte der Absätze 1, 3 Satz 2, 4 und 5 Satz 1 des § 22 DSG NRW ergänzt werden.

B. Zu den einzelnen Vorschriften

Zu § 10 d. E.

Im Gegensatz zur aktuellen Fassung des § 10 Absatz 2 IFG NRW, die durch den konkreten Verweis auf § 4 Absatz 6 DSG NRW eine gezielte, klar definierte Anordnung gegenüber den öffentlichen Stellen trifft, ist die im Entwurf gewählte Formulierung „nach dem geltenden Datenschutzrecht" wenig präzise und unklar. Vorzugswürdig ist es, den aktuellen Gesetzeswortlaut des § 4 Absatz 6 DSG NRW wörtlich zu übernehmen und auf einen Verweis zu verzichten. Dies trägt auch dem Ziel, die bisherige Vorgabe zu erhalten, umfassend Rechnung.

Zu § 13 d. E.

Wesentliche, aktuell in § 22 Absatz 1, 4 und 5 DSG NRW geregelte Aufgaben und Befugnisse der Informationsfreiheitsbeauftragten wie etwa

die Überwachung der Einhaltung der Vorschriften des IFG NRW, die Möglichkeit, Empfehlungen unabhängig von einer Beanstandung zu geben, zu beraten und zu informieren, fehlen komplett. Insoweit bedarf es unbedingt noch einer entsprechenden Ergänzung des Entwurfs.

Zu Absatz 5
Redaktioneller Hinweis: Der Verweis auf Absatz 5 in Satz 1 ist zu streichen.

Zu Absatz 6
In Satz 2 ist eine Begrenzung auf Verstöße gegen die Informationspflicht allein nicht ausreichend, da auch die Möglichkeit bestehen muss, eine Beanstandung im Falle etwa eines Verstoßes gegen § 11 IFG NRW aussprechen zu können. Vorzugswürdig wäre daher eine ähnlich lautende Formulierung wie in § 28 Absatz 2 DSG NRW-Entwurf („Verstöße gegen die Vorschriften dieses Gesetzes“).

Zu Absatz 9
Redaktioneller Hinweis: Beide Verweise müssen sich auf Absatz 6 anstatt auf Absatz 7 beziehen.

Artikel 7
Änderung des Landesbeamtengesetzes

Zu § 83 Absatz 4 Satz 1

Vorgeschlagen wird, Absatz 4 Satz 1 wie folgt zu fassen (Änderungen unterstrichen):

> „Der Dienstherr darf personenbezogene Daten über Bewerberinnen und Bewerber, Beamtinnen und Beamte und ehemalige Beamtinnen und Beamte verarbeiten, soweit dies im Rahmen der Personalverwaltung und der Personalwirtschaft zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen erforderlich ist oder eine Rechtsvorschrift <u>oder eine Dienstvereinbarung dies erlaubt oder die betroffene Person eingewilligt hat.</u>“

Die Ergänzung dient der Harmonisierung mit der Regelung des Art. 1 § 18 Absatz 1 Satz 1 d. E. Ebenso wie Art. 1 § 18 Absatz 1 Satz 1 d. E. sollte die vorstehende Vorschrift eine Regelung enthalten, die die Datenverarbeitung aufgrund einer Einwilligung der Betroffenen normiert. Ein sachlicher Grund für einen Verzicht hierauf ist nicht ersichtlich.

Richtigerweise wird die Vorschrift des Art. 7 § 83 Absatz 4 Satz 1 d. E. in der Gesetzesbegründung als zentrale Ermächtigungsnorm bezeichnet, die als bereichsspezifische Datenschutzregelung dem Dienstherrn erlaubt, personenbezogene Daten über die Beamtin oder den Beamten zu verarbeiten.

Ohne eine Ergänzung der Norm sind die expliziten Zulässigkeitsregelungen zur Einwilligung, die für nicht beamtete Beschäftigte des öffentlichen Dienstes gem. Art. 1 § 18 Absatz 1 Satz 1 d. E. gelten werden, nicht auf Beamtinnen und Beamte anwendbar, weil Art. 7 § 83 Absatz 4 Satz 1 d. E. lex specialis zu Art. 1 § 18 Absatz 1 Satz 1 d. E. ist.

Artikel 8
Änderung des Gesetzes über den Brandschutz, die Hilfeleistung und den Katastrophenschutz

Zu § 46 d. E.

Soweit in Absatz 3 die Informationspflichten nach Artikel 13 und 14 der Datenschutzgrundverordnung beschränkt werden sollen, entspricht dies nicht den europarechtlichen Vorgaben.
Zudem sollte zum Schutz der Rechte der betroffenen Personen der Direkterhebungsgrundsatz unbedingt weiterhin ausdrücklich festgeschrieben werden.

Eine Beschränkung der Informationspflichten ist nach Artikel 23 Absatz 1 lit. c und i DSGVO zwar möglich, gemäß Artikel 23 Absatz 2 lit. c DSGVO muss aber der Umfang der vorgenommenen Beschränkungen bezeichnet sein. Es reicht daher nicht, nur darauf hinzuweisen, dass die Informationspflichten beschränkt werden, sondern es muss dargelegt werden, in welcher Form diese beschränkt werden. Dabei muss die Be-

schränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen. Auch die übrigen Vorgaben des Artikel 23 Absatz 2 DSGVO müssen mit der Regelung erfüllt werden.

Hinsichtlich des Direkterhebungsgrundsatzes wird sinngemäß auf die bisherigen Ausführungen verwiesen.

Artikel 9
Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen

A. Allgemeines

Die Stellungnahme beschränkt sich auf die vorgelegten Vorschriften. Eine Prüfung dahingehend, welche weiteren Regelungen darüber hinaus geboten sein könnten, ist im Wesentlichen nicht erfolgt.

Das der Gesetzesbegründung zu entnehmende Ziel einer Harmonisierung wesentlicher Regelungen der Verfassungsschutzgesetze des Bundes und der Länder ist grundsätzlich verständlich. Andererseits ist eine gleichgelagerte Tendenz in anderen Bundesländern zumindest bislang nicht erkennbar. Vor diesem Hintergrund ist derzeit nicht nachvollziehbar, warum die Neuregelung durch den Verweis in § 31 d. E. auf bundesgesetzliche Regelungen des BDSG (2018) abstellt und nicht von der Möglichkeit Gebrauch gemacht wird, die notwendigen Regelungen im DSG NRW oder im Verfassungsschutzgesetz NRW zu treffen.

B. Zu den einzelnen Vorschriften

Zu § 12 d. E.

In § 8 Absatz 1 Nr. 9 des aktuellen DSG NRW sind bisher „die Fristen für die Sperrung und Löschung“ genannt. § 12 Absatz 2 Nr. 9 d. E. erwähnt lediglich die Löschung. Die Möglichkeit der Sperrung besteht jedoch grundsätzlich fort. Sie wurde ausweislich der § 10 Absatz 2 und 11

Absatz 2 d. E. lediglich durch den Begriff der „Einschränkung der Verarbeitung“ ersetzt. Es ist nicht ersichtlich, warum eine Erwähnung der Einschränkung der Verarbeitung in § 12 Absatz 2 Nr. 9 d. E. obsolet geworden sein soll. Die Vorschrift sollte dementsprechend ergänzt werden.

Im Zusammenhang mit § 12 d. E. wird weiterhin deutlich, dass nicht nur die bisher in § 8 Absatz 1 Nr. 11 des aktuellen DSG NRW vorgesehenen Ergebnisse der Vorabkontrolle nach § 10 Absatz 3 des aktuellen DSG NRW nicht mehr in das Verfahrensverzeichnis aufzunehmen sind. Vielmehr wird ebenfalls augenfällig, dass der aktuelle Entwurf weder die Erstellung eines Sicherheitskonzeptes inklusive der Vorabkontrolle im Sinne des § 10 Absatz 3 des aktuellen DSG NRW vorsieht, noch eine die-se Maßnahmen im allgemeinen Datenschutzrecht ablösende Datenschutzfolgenabschätzung im Entwurf verankert ist. Dass der Entwurf keinerlei derartige Maßnahme vorsieht, stellt eine deutliche Verschlechterung des Datenschutzniveaus gegenüber dem bisherigen Stand dar.

Zu § 15 d. E.

Wie im bisherigen § 25 Absatz 1 DSG NRW sollte es ausreichend sein, wenn eine Verletzung in Datenschutzrechten bevorsteht. Bediensteten öffentlicher Stellen sollte das Anrufungsrecht auch nach dem neuen Recht gegeben sein, ohne dass der Dienstweg eingehalten werden muss (vgl. § 25 Absatz 2 letzter Halbsatz des aktuellen DSG NRW). Weiterhin sollte auch künftig niemand benachteiligt oder gemaßregelt wer-den dürfen, weil er sich an die Landesbeauftragte für Datenschutz und Informationsfreiheit wendet (vgl. § 25 Absatz 2 des aktuellen DSG NRW).

In Absatz 2 Satz 1 sollte klargestellt werden, dass die LDI NRW die Einhaltung der Vorschriften über den Datenschutz im Hinblick auf alle in der Verantwortung der Verfassungsschutzbehörde verarbeiteten personenbezogenen Daten kontrolliert. Nach dem Entwurf erstreckt sich die Kontrolle der LDI NRW auf die Einhaltung des Datenschutzes „bei“ der Verfassungsschutzbehörde. Das Wort „bei“ könnte einschränkend dahingehend verstanden werden, dass gemeinsame Dateien mit anderen Nachrichtendiensten davon ausgeschlossen seien. Einer solchen Auslegung ist durch Klarstellung im Gesetz entgegenzuwirken.

Die LDI NRW begrüßt die in der Begründung vorgenommene Klarstellung, dass die Vorschrift nicht die Kenntnisnahme von G 10-Erkenntnissen durch die LDI NRW verhindern, sondern lediglich konträre Ergebnisse datenschutzrechtlicher Prüfungen ausschließen möchte. Wie auch bereits die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in ihrer Stellungnahme zum entsprechenden Entwurf des BVerfSchG (2017) ausgeführt hat, wäre eine Klarstellung im Gesetzestext selbst gegenüber dieser Lösung jedoch vorzuziehen (vgl. Stellungnahme der BfDI vom 30.11.2016).

Derzeit kann die oberste Landesbehörde im Einzelfall feststellen, dass die Sicherheit des Bundes oder eines Landes es gebietet, dass Auskunftsrechte nur von der LDI NRW persönlich ausgeübt werden (§ 22 Absatz 2 des aktuellen DSG NRW). Nur für den Fall, dass einer betroffenen Person von der datenverarbeitenden Stelle Vertraulichkeit besonders zugesichert worden ist, müssen deren personenbezogene Daten insoweit auch der LDI NRW persönlich nicht offenbart werden. Damit konnte bisher nur in einem zweistufigen Verfahren eine Prüfmöglichkeit der LDI NRW ausgeschlossen werden. § 15 Absatz 3 Satz 3 d. E. sieht nunmehr einen Ausschluss der Auskunftspflicht für jeden Fall vor, in dem die Verfassungsschutzbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde. § 15 Absatz 3 Satz 3 d. E. sollte daher dahingehend angepasst werden, dass das Datenschutzniveau der bisherigen Regelung beibehalten wird. Dabei sollte auch darauf hingewiesen werden, dass allgemeine Hinweise auf eine Gefährdung der Zusammenarbeit mit ausländischen Nachrichtendiensten für eine Anwendung der Ausnahme nicht ausreichen.

Zu § 31 d. E.

Wie bereits oben ausgeführt, wird die weitgehende Verweisung auf Normen des BDSG (2018) generell kritisch gesehen. Soweit Vorschriften des BDSG (2018), auf die verwiesen wird, inhaltlich solchen Vorschriften des Art. 1 d. E. entsprechen, wird auf die obige Kritik verwiesen. Dies gilt insbesondere für die Ausführungen zu Art. 1, § 43 d. E. im Hinblick auf § 54 BDSG (2018) sowie für die Ausführungen zu Art. 1, § 55 d. E. im Hinblick auf § 64 BDSG (2018).

Artikel 10
Änderung des Sicherheitsüberprüfungsgesetzes Nordrhein-Westfalen

Soweit die Änderungen in Art. 10 d. E. den Änderungen in Art. 9 d. E. entsprechen, wird auf die Ausführungen zu Art. 9 d. E. verwiesen.

Mit freundlichen Grüßen

Helga Block

Helga Block