www.datenschutzzentrum.de

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Gundermann
Durchwahl: 988-1214

Aktenzeichen:
LD2-01.03/04.800

Kiel, 12. März 2018

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Die Vorsitzende
Landeshaus
Düsternbrooker Weg 70
25105 Kiel

Schleswig-Holsteinischer Landtag
Umdruck 19/752

Schriftliche Anhörung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680
Gesetzentwurf der Landesregierung Drucksache 19/429

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

vielen Dank für die Gelegenheit zur Stellungnahme zum oben genannten Gesetzentwurf.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist in besonderer Weise von den in Rede stehenden Datenschutzregelungen betroffen, weil es als zuständige Aufsichtsbehörde prüfend und beratend für die Verantwortlichen tätig sein wird. Aus meiner Sicht muss das Umsetzungsgesetz sowohl den rechtlichen Anforderungen genügen, die sich aus der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, DSGVO) und der JI-Richtlinie (Richtlinie (EU) 2016/680 für Justiz und Inneres) ergeben, als auch praxistauglich aus Anwendersicht sein. Dort, wo eine Anschlussfähigkeit an die bisherigen rechtlichen Datenschutzregeln wie dem Landesdatenschutzgesetz (LDSG alte Fassung) besteht, sollte dies genutzt werden, um denjenigen, die sich bisher rechtskonform verhalten, den Übergang in das neue Datenschutz-Regime zu erleichtern.

Dabei ist zu beachten, dass der öffentliche Bereich in Schleswig-Holstein, für den die Datenschutznormen gelten werden, vielfach aus Mischverwaltungen besteht, die für einige Aufgaben den unmittelbar anzuwendenden Regeln der DSGVO unterliegen, für andere Aufgaben jedoch die in Landesrecht umzusetzende JI-Richtlinie einschlägig ist. Wie auch das Bundesdatenschutzgesetz (BDSG) führt der LDSG-E beide Anforderungen in einem Gesetzeswerk zusammen, das Konkretisierungen der DSGVO gemäß den Öffnungsklauseln

in einem Teil und in einem weiteren Teil die Umsetzung der JI-Richtlinie enthält (siehe Abbildung 1).

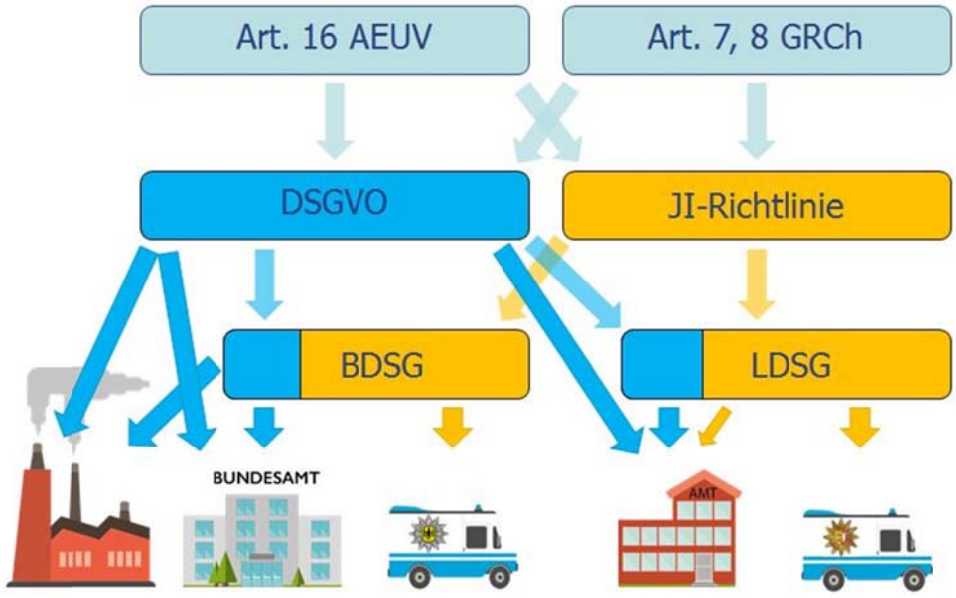

Abb. 1: Überblick über das EU-Datenschutzrecht und die Wirkungen auf Verantwortliche

Für eine Behörde in Schleswig-Holstein bedeutet dies, dass sowohl die DSGVO als auch Teil 1 des neuen LDSG für alle Aufgaben gilt, die nicht der JI-Richtlinie unterfallen, während Teil 2 des neuen LDSG Bedeutung hat, soweit Ordnungswidrigkeitenverfahren durchgeführt werden. Aus Praxissicht wäre es insbesondere für Behörden mit gemischten Aufgaben – und dazu gehören Städte und Kommunen – hilfreich, wenn in den Fällen innerhalb des Gesetzestextes, in denen dasselbe gemeint ist, auch dieselben Formulierungen verwendet würden.

Unsere Stellungnahme weist zudem auf besonders wichtige Aspekte durch Kennzeichnung mit einem Achtung-Piktogramm hin. Dies umfasst sowohl konzeptionelle Punkte als auch Änderungsvorschläge zu Textstellen, bei denen wir starke Bedenken bezüglich der europarechtlichen Konformität haben. Teilweise unterbreiten wir Formulierungsvorschläge, die durch eine graue Hinterlegung rasch erkennbar sind.

Unsere Stellungnahme geht nur geringfügig auf das „Errichtungsgesetz ULD“ (Artikel 2 des Gesetzentwurfs) und gar nicht auf die Modalitäten in Bezug auf die Landesbeauftragte für Datenschutz ein, da ich nicht den Anschein erwecken möchte, in eigener Sache tätig zu werden. Änderungen sind jedoch auch in diesem Bereich vorstellbar.

Sollte sich Nachfragebedarf – auch zu noch fehlenden Alternativformulierungen – ergeben, stehen mein Team und ich gerne zur Verfügung.

gez. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein

Stellungnahme des ULD zum Gesetzentwurf der Landesregierung Drucksache 19/429

Im Folgenden werden zunächst im ersten Teil bestehend aus den Punkten 1. bis 9. die aus Sicht des ULD wichtigsten Aspekte und Änderungsbedarfe dargelegt. Der zweite Teil enthält detaillierte Hinweise zu den im LDSG-E vorgeschlagenen Regelungen.

1. Artikel 1 – § 17 Abs. 2 LDSG-E: Aufgaben und Befugnisse: Ausübung der Befugnisse

Die Vorschrift regelt die Wahrnehmung der Befugnisse nach Art. 58 Abs. 2 DSGVO durch die oder den Landesbeauftragten für Datenschutz (LfD). Danach soll das ULD in Zukunft **vor der Ausübung aller Abhilfebefugnisse** gegenüber öffentlichen Stellen (bis auf die Warnung vor zukünftigen Rechtsverletzungen) seine Erkenntnisse zunächst der **jeweiligen Fach- oder Rechtsaufsichtsbehörde mitteilen** und dieser Gelegenheit zur Stellungnahme geben.

Schon im Hinblick auf das dem ULD gegenüber öffentlichen Stellen bisher alleine zustehende Recht zu Beanstandungen nach § 42 LDSG (dem wohl jetzt die Verwarnung nach Art. 58 Abs. 2 Buchstabe b) entspricht) wird damit das Verfahren auf den Kopf gestellt. Bisher galt, dass Beanstandungen gegenüber öffentlichen Stellen ausgesprochen werden und im Regelfall die zuständige Fach- oder Rechtsaufsichtsbehörde zu informieren war. Vor dem Aussprechen der Beanstandung hatte das ULD den Sachverhalt regelmäßig ausermittelt, so dass eine abschließende Bewertung möglich war. Nunmehr soll als weiterer Verfahrensschritt nach diesem Abschluss der Sachverhaltsermittlung der jeweilige Fach- oder Rechtsaufsichtsbehörde eine weitere Gelegenheit zur Stellungnahme gegeben werden. Es ist nicht erkennbar, welche zusätzlichen Erkenntnisse diese weitere Stellungnahme erbringen soll. Dagegen ist offensichtlich, dass das vorgeschlagene Verfahren zu **unnötige Verzögerungen** und zusätzlicher Bürokratie führen wird.

Vor allem aber begegnet diese Regelung schwersten Bedenken, da sie **nicht mit höherrangigem europäischen Recht vereinbar** ist. Der Zwang zur Einbeziehung der Aufsichtsbehörde, bevor überhaupt die Befugnisse nach Art. 58 DSGVO ausgeübt werden können, führt zu einer klaren Beschneidung dieser Befugnisse. Schon zur gebotenen Unabhängigkeit der Datenschutzbehörde unter der Richtlinie 95/46/EG hatte der EuGH ausgeführt: „Folglich müssen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen. Hierzu müssen sie **vor jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher** sein und nicht nur vor der Einflussnahme seitens der kontrollierten Einrichtungen." (Kommission / Deutschland, NJW 2010, 1265, Rn. 25).

Der EuGH hat die Anforderung an die Unabhängigkeit der Aufsichtsbehörden in der Rechtssache C-614/10 (Kommission / Österreich) konkretisiert:

> „62 Zur dritten Rüge der Kommission ist festzustellen, dass der **Bundeskanzler** gemäß Art. 20 Abs. 2 B-VG und § 38 Abs. 2 DSG 2000 das **Recht** hat, sich beim Vorsitzenden und beim geschäftsführenden Mitglied der DSK **jederzeit über alle Gegenstände ihrer Geschäftsführung zu unterrichten**.
>
> 63 Ein solches **Unterrichtungsrecht** ist ebenfalls dazu angetan, die DSK einem mittelbaren Einfluss seitens des Bundeskanzlers auszusetzen, der nicht mit dem Unabhängigkeitskriterium des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 vereinbar ist. (…)

> 64 Unter diesen Umständen steht das in Art. 20 Abs. 2 B-VG und in § 38 Abs. 2 DSG 2000 vorgesehene Unterrichtungsrecht einer Einstufung der DSK als Stelle entgegen, deren Handlungen unter allen Umständen über jeden Verdacht der Parteilichkeit erhaben sind."

Daraus ergibt sich, dass es die **Unabhängigkeit auch verletzt**, wenn die Regierung über das Recht verfügt, sich über alle Gegenstände der Geschäftsführung der Kontrollstelle zu informieren (Wolff, in Wolff/Schantz, Rn. 994). Ähnlich liegt die Sache hier, wo sich die Regierung des Landes das Recht verschaffen will, noch vor der Ausübung der Befugnisse des ULD Informationen über sämtliche aufsichtsbehördlichen Tätigkeiten zu erhalten. Dies gilt umso mehr, als der europäische Gesetzgeber die Unabhängigkeit der Datenschutzaufsicht beim Übergang von der Richtlinie 95/46/EG zur DSGVO stärken wollte.

In der Gesetzesbegründung zu der Vorschrift werden zwei Gründe für die Änderung genannt: Zum einen soll die Aufsichtsbehörde in die Lage versetzt werden, rechtzeitig auf datenschutzrechtliche Bedenken zu reagieren, die möglicherweise in einer Vielzahl von Fällen relevant sind oder die spezifischen Gründe für bestimmte Regelungen darzulegen. Zu diesem Argument ist nicht einsichtig, warum eine **Benachrichtigung der Aufsichtsbehörde zeitgleich mit der Ausübung der Befugnisse** nicht **ausreichen** soll.

Das zweite Argument lautet: „Eine Anhörung vor Erlass einer belastenden Maßnahme ist auch in anderen Rechtsbereichen wie insgesamt im Verwaltungsverfahren grundsätzlich üblich". Dieses Argument verkennt oder verschleiert die tatsächlichen Verhältnisse. Wie oben dargelegt, hat das ULD bereits in der Vergangenheit die betroffene öffentliche Stelle immer ausführlich angehört, bis der Sachverhalt unstreitig war und alle rechtlichen Argumente ausgetauscht waren. Unter der Geltung der DSGVO wird die Ausübung der Abhilfebefugnisse auch gegenüber öffentlichen Stellen einen Verwaltungsakt darstellen. Selbstverständlich wird sich das ULD an **geltendes Verfahrensrecht** halten und die potenziellen **Adressaten der Verwaltungsakte nach § 87 Landesverwaltungsgesetz anhören**. Dem Gesetzentwurf geht es jedoch nicht um die Anhörung der betroffenen öffentlichen Stellen selbst, sondern um die Anhörung der jeweiligen Fach- oder Rechtsaufsichtsbehörden dieser Stellen. Dafür gibt es „insgesamt im Verwaltungsverfahren" keine Vorbilder.

Auch der von der Gesetzesbegründung zitierte § 16 Abs. 1 Satz 2-4 BDSG-neu taugt nicht als Rechtfertigung der Einschränkung der Abhilfebefugnisse. Zum einen begegnet auch diese Regelung europarechtlichen Bedenken. Zum anderen ist die tatsächliche Lage im Bereich der öffentlichen Stellen des Bundes eine andere. Dort geht es regelmäßig um Verstöße oberster Bundesbehörden oder der diesen nachgeordneten Bereiche. Einen großen Teil der Aufsichtstätigkeit des ULD macht jedoch der kommunale Bereich aus. Hier gehört die Rechtsaufsicht einer anderen juristischen Person an als die Stelle, die Adressatin der aufsichtsbehördlichen Maßnahme ist.

Dass eine solche Einbeziehung eines nicht direkt beteiligten Rechtsträgers systemwidrig ist, zeigt auch der Blick auf § 20 Abs. 5 BDSG-neu. Die Vorschrift regelt, wer Beteiligter eines verwaltungsgerichtlichen Verfahrens über die Rechtmäßigkeit von aufsichtsbehördlichen Maßnahmen ist. Dies ist auf der einen Seite die mit den aufsichtsbehördlichen Maßnahmen nach Art. 58 Abs. 2 überzogene juristische Person als Klägerin oder Antragstellerin und auf der anderen Seite die Aufsichtsbehörde als Beklagte oder Antragsgegnerin. Eine weitere Stelle, wie eine andere juristische Person, die die Rechts- oder Fachaufsicht führt, ist in dieser Konstellation nicht vorgesehen

und kann daher auch nicht bei der Verhängung der aufsichtsrechtlichen Maßnahme selbst dazwischengeschaltet werden.

Es sollte daher unbedingt bei der bisherigen Rechtslage bleiben, die lediglich eine Information der Rechts- oder Fachaufsicht über Maßnahmen der Datenschutzaufsicht vorsieht. Dafür spricht auch die Regelung in Brandenburg, wo die oder der Landesbeauftragte der Fach- oder Rechtsaufsichtsbehörde lediglich mitteilt, dass von den Befugnissen nach Art. 58 Abs. 2 DSGVO Gebrauch gemacht wird (vgl. § 21 LDSG-E Brandenburg, dortige LTDrs. 6/7365).

2. Artikel 1 – § 64 LDSG-E: Abhilfebefugnisse der oder des LfD

Mit der Regelung § 64 Abs. 1 LDSG-E soll Art. 47 Abs. 2 der JI-Richtlinie umgesetzt werden. Art. 47 Abs. 2 der JI-Richtlinie lautet:

> „Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse wie etwa die beispielhaft genannten folgenden verfügt, die es ihr gestatten,
>
> a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die nach dieser Richtlinie erlassenen Vorschriften verstoßen,
>
> b) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung gemäß Artikel 16;
>
> c) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen."

Diese europarechtlichen Anforderungen setzt der Gesetzentwurf nicht um; er ist damit **europarechtswidrig.** Art. 47 Abs. 2 der JI-Richtlinie macht mit der Formulierung „wirksame Abhilfebefugnisse" und den dazu genannten Beispielen deutlich, dass es sich um Befugnisse zur Durchsetzung datenschutzrechtlicher Anforderungen handeln muss. Die in § 64 Abs. 1 LDSG-E vorgesehene Beanstandung ist nicht verbindlich und nicht durchsetzbar. Vertritt der Verantwortliche oder dessen Rechts- oder Fachaufsichtsbehörde eine andere Auffassung als die/der Landesbeauftragte, besteht keine Möglichkeit der Durchsetzung oder Einleitung einer gerichtlichen Klärung der Frage, ob die betreffende Verarbeitung rechtswidrig ist. Die oder der Landesbeauftragte kann in dieser Konstellation keine wirksame Abhilfe herbeiführen. Um den **Befugnissen Wirksamkeit zu verleihen, bedarf es – wie im Anwendungsbereich der DSGVO – der Möglichkeit, verbindliche Anordnungen zu treffen.** Erst hierdurch kann auch eine gerichtliche Klärung herbeigeführt werden.

Diese Kritik hat auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu der wortgleichen Vorschrift des § 16 Abs. 2 BDSG-neu geäußert und die Vorschrift als europarechtswidrig eingestuft (siehe BT-Ausschuss-Drs. 18(4)788 v. 3.3.2017, S. 5 f.).

Für eine europarechtskonforme Regelung sollte daher auf die Befugnisse nach Art. 58 Abs. 2 Buchstaben a)-g) und j) DSGVO verwiesen oder der Wortlaut des Art. 58 Abs. 2 DSGVO insoweit in § 64 LDSG-E mit aufgenommen werden.

Sofern nicht alle Befugnisse der DSGVO für den Bereich der JI-Richtlinie übernommen werden sollen, sollten mindestens die im Hessischen Gesetzentwurf vorgesehenen Befugnisse aufgenommen werden. § 14 Abs. 3 des Entwurfs für ein Hessisches Datenschutz- und Informationsfreiheitsgesetz (dortige LT-Drs. 19/5728, S. 15) lautet:

> „Die oder der Hessische Datenschutzbeauftragte kann bei Verstößen nach Abs. 2 Satz 1 darüber hinaus [Anm.: über Beanstandung und Warnung hinaus] anordnen,
>
> 1. Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise oder innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen,
> 2. personenbezogene Daten zu berichtigen,
> 3. personenbezogene Daten in der Verarbeitung einzuschränken,
> 4. personenbezogene Daten zu löschen,
>
> wenn dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist."

3. Vollstreckung gegen Behörden

Die DSGVO geht davon aus, dass die **Aufsichtsbehörden in Art. 58 „wirksame Befugnisse"** erhalten haben, damit sie „die einheitliche Überwachung und Durchsetzung" der DSGVO sicherstellen (EG 129). Dies ist allerdings aufgrund landesrechtlicher Besonderheiten gegenüber öffentlichen Stellen nicht vollständig gewährleistet.

Zwar ist nach Art. 58 Abs. 2 DSGVO der Erlass von Anordnungen und Verboten auch gegenüber öffentlichen Stellen möglich. Gegen solche Verwaltungsakte können sich die Adressaten auch nach Art. 78 Abs. 1 DSGVO i. V. m. § 20 BDSG vor dem Verwaltungsgericht zur Wehr setzen. Unterlässt es eine öffentliche Stelle allerdings, einer Anordnung nachzukommen, so kann diese derzeit nicht vollstreckt werden. Nach § 234 Landesverwaltungsgesetz ist der Vollzug gegen Träger der öffentlichen Verwaltung nur möglich, soweit er durch Rechtsvorschrift ausdrücklich zugelassen ist. An einer solchen Rechtsvorschrift fehlt es. Legt eine öffentliche Stelle als Adressatin einer Maßnahme nach Art. 58 Abs. 2 DSGVO keine Rechtsmittel ein und kommt sie gleichzeitig der Anordnung nicht nach, so entsteht eine **dauerhaft rechtswidrige Situation, die nicht aufgelöst werden kann**.

Dieses Problem wurde im Gesetzentwurf für ein neues Hessisches Datenschutz- und Informationsfreiheitsgesetz (dortige LT-Drs. 19/5728) wie folgt adressiert: Im ersten Teil des Gesetzes, der den Vorschriften zur Ausfüllung der Öffnungsklauseln der DSGVO bzw. zur Umsetzung der JI-Richtlinie vorangestellt ist und der für beide Regelungsbereiche gilt, wurde das Recht des Hessischen Datenschutzbeauftragten verankert, die Prüfung der Rechtmäßigkeit seiner Anordnungen gegenüber öffentlichen Stellen selbst vor das Verwaltungsgericht zu bringen, wenn die öffentliche Stelle, welche Adressatin der Anordnung ist, diese weder umsetzt noch dagegen Rechtsmittel einlegt. Damit wird sichergestellt, dass es nicht zu einem dauerhaft rechtswidrigen Zustand kommt, da die Anordnung in jedem Fall einer gerichtlichen Prüfung zugeführt werden kann. Kommt das Gericht zu dem Ergebnis, dass die Anordnung rechtmäßig war, kann es gegebenenfalls selbst die Vollstreckung nach § 172 VwGO vornehmen.

Es wird daher vorgeschlagen, nach dem Vorbild von § 19 Abs. 5 des Entwurfs eines Hessisches Datenschutz- und Informationsfreiheitsgesetz folgende Formulierung als neue Vorschrift nach § 2 aufzunehmen:

„**Rechtsschutz**

(1) Behörden und sonstige öffentliche Stellen des Landes können unbeschadet anderer Rechtsbehelfe gerichtlich gegen sie betreffende verbindliche Entscheidungen der oder des Landesbeauftragten vorgehen.

(2) Wenn die Behörde oder öffentliche Stelle eine verbindliche Entscheidung der oder des Landesbeauftragten nicht beachtet und nicht innerhalb eines Monats nach Bekanntgabe gerichtlich gegen diese vorgeht, kann die oder der Landesbeauftragte die gerichtliche Feststellung der Rechtmäßigkeit der getroffenen verbindlichen Entscheidung beantragen."

Absatz 1 der neu vorgeschlagenen Vorschrift regelt die Rechtsschutzmöglichkeit gegen Anordnungen der Aufsichtsbehörde nach dem Vorbild von § 56 des Entwurfs für ein Hessisches Datenschutz- und Informationsfreiheitsgesetz für den Bereich der Umsetzung der JI-Richtlinie. Diese Vorschrift wird erforderlich, wenn die oben unter Nr. 2 dieser Stellungnahme gegebene Hinweise umgesetzt werden.

Absatz 2 löst die Fälle, in denen der Adressat einer Anordnung dieser nicht nachkommt und zugleich keine Rechtsmittel einlegt.

4. Rechtsform des ULD

In Artikel 2 des Entwurfs ist für das ULD weiterhin die Rechtsform der Anstalt des öffentlichen Rechts vorgesehen. **Diese Rechtsform wurde bislang in keinem anderen Bundesland gewählt.** Vielmehr sind, größtenteils als Reaktion auf die Entscheidung des EuGH zur Unabhängigkeit der Datenschutzaufsicht, die Datenschutzaufsichtsbehörden im Bund und in vier Ländern (Berlin, Hessen, Niedersachsen, Rheinland-Pfalz) als oberste Bundes- oder Landesbehörden ausgestaltet worden bzw. ist dies so in den Entwürfen der neuen LDSG dieser Länder vorgesehen. **Die Rechtsform einer obersten Landesbehörde entspricht am ehesten den europarechtlichen Vorgaben** (siehe Gesetzentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes, BT-Drs. 18/2848, S. 2) und sollte daher **auch in Schleswig-Holstein** angestrebt werden.

5. Artikel 1 – § 14 LDSG-E: Videoüberwachung

Bei dieser Vorschrift besteht aus Sicht des ULD nach wie vor **erheblicher Änderungsbedarf**. Die gesamte Regelung erscheint **nicht ausgewogen** und lässt letztlich nicht erkennen, welche Art von Videoüberwachung durch öffentliche Stellen auf sie gegründet werden soll.

Das gilt bereits für den Bezug auf Art. 6 Abs. 1 Buchstabe f) DSGVO. Hintergrund für diese Regelung ist offenbar, dass die Gerichte die Wahrnehmung des Hausrechts durch Behörden nicht zu den diesen durch Rechtsvorschrift zugewiesenen hoheitlichen Aufgaben zählen. Daher ist das Abstellen auf den Zulässigkeitstatbestand Interessenabwägung in Art. 6 Abs. 1 Buchstabe f) dogmatisch wohl nicht zu beanstanden, obwohl dieser eigentlich nicht von Behörden in Anspruch genommen werden darf. Allerdings dürfte den wenigsten Rechtsanwendern dieser Zusammenhang geläufig sein, so dass die Vorschrift zumindest Irritationen hervorrufen wird.

Im Weiteren bleibt der Tatbestand vage, indem er lediglich die Generalklausel des Art. 6 Abs. 1 Buchstabe e) DSGVO wiederholt. Zielführender wäre es, hier in Anlehnung an § 4 BDSG-neu bzw. § 27 LDSG-E Brandenburg (dortige LT-Drs. 6/7365) kon-

krete Anwendungsszenarien, wie beispielsweise die Wahrnehmung des Hausrechts, zu definieren. **In der vorgeschlagenen Fassung dürfte die Vorschrift kaum anwendbar sein.**

Besorgniserregend ist, dass § 14 Abs. 1 LDSG-E auch die **Verarbeitung von Daten im Sinne von Art. 9 Abs. 1 DSGVO erlauben** soll. Damit würde sämtlichen öffentlichen Stellen unter anderem der Einsatz von Gesichtserkennungssoftware erlaubt. Andere Systeme, die die Betroffenen beispielsweise aufgrund ihrer Hautfarbe unterscheiden oder die die Gesundheit der Betroffenen erkennen, wären ebenfalls zulässig. Erfasst würden alle Personen, auch solche, die bloß einen überwachten Bereich passieren. Dies erscheint **exzessiv und mit den Freiheitsrechten unter dem Grundgesetz und den europäischen Grundrechten nicht vereinbar.**

Die Regelung ist auch nicht erforderlich, um die Videoüberwachung überhaupt zu ermöglichen. Hintergrund für die Einbeziehung der besonderen Kategorien personenbezogener Daten ist nach der Begründung (S. 144) die Annahme des Entwurfsverfassers, dass jede Videoüberwachung denklogisch mit der Erfassung solcher besonderer Daten einhergeht. Diese Annahme trifft nicht zu. Denn die Beobachtung und Aufzeichnung von Personen mittels optisch-elektronischer Einrichtungen ist nicht bereits deshalb eine Verarbeitung besonderer Arten personenbezogener Daten, weil durch solche Aufnahmen z. B. aufgrund der Hautfarbe, Kleidung oder sonstiger Umstände Rückschlüsse auf die Herkunft, Religionszugehörigkeit oder den Gesundheitszustand von Personen möglich sind (vgl. zur insoweit wortgleichen Regelung des Art. 8 der Richtlinie 95/46/EG Leitlinien des Europäischen Datenschutzbeauftragten zur Videoüberwachung vom 17. März 2010, S. 33 (Fn. 31); Scholz in Simitis, BDSG, 8. Auflage § 6b Rn. 99 (Fn. 262); ähnlich auch Gola/Schomerus, BDSG § 3 Rn. 56a). Eine Verarbeitung solcher Kategorien liegt vielmehr erst dann vor, wenn deren Erfassung und Verarbeitung zielgerichtet erfolgt, beispielsweise die Aufnahmen gezielt nach Personen einer bestimmten Herkunft gefiltert werden oder, wie oben bereits ausgeführt, ein automatisches Gesichtserkennungssystem eingesetzt wird. Eine solche Videoüberwachung zu erlauben, ist nach der Begründung (S. 144) jedoch nicht Ziel des Gesetzentwurfs. Daher kann auf die Erwähnung der Daten nach Art. 9 DSGVO verzichtet werden, ohne dass dies im Vergleich zur bisherigen Rechtslage mit Einbußen in den Möglichkeiten für öffentliche Stellen verbunden ist, Videoüberwachung zu betreiben. Für eine verfassungskonforme Regelung muss vielmehr auf die Einbeziehung dieser Daten verzichtet werden.

Absatz 3 der Vorschrift enthält eine Regelung zur **Zweckänderung**. Diese soll auch zur Vollstreckung von Straftaten erforderlich sein. Dies erscheint ebenfalls **zu weitgehend und nicht erforderlich**; eine entsprechende Regelung findet sich weder in § 27 Abs. 3 LDSG-E Brandenburg noch in § 4 Abs. 3 BDSG-neu.

6. Artikel 1 – § 17 LDSG-E: Aufgaben und Befugnisse: Zertifizierungen

Absatz 3 der Vorschrift weist der oder dem Landesbeauftragten die Aufgabe zu, verbindliche Kriterien für die Zertifizierung festzulegen und diese zu veröffentlichen. Im Hinblick auf die **gegenwärtig** unter § 43 Abs. 2 LDSG **durch das ULD durchgeführte Auditverfahren** wird eine **Überleitungsvorschrift erforderlich** werden. Es wird vorgeschlagen, § 17 Abs. 3 wie folgt zu fassen:

„Die oder der Landesbeauftragte legt Verfahren und Kriterien für die Zertifizierungen nach Art. 58 Abs. 3 Buchstabe f) Verordnung (EU) 2016/679 fest und veröffentlicht diese. Für vor Inkrafttreten dieses Gesetzes erfolgte Zertifizierungen und Auditierungen durch die oder den Landesbeauftragten legt sie oder er Verfahren und

Kriterien zur Überleitung auf die Zertifizierungen nach Verordnung (EU) 2016/679 fest und veröffentlicht diese."

Zur Erläuterung sollte in die Begründung zu § 17 LDSG-E folgender Satz aufgenommen werden:

„Durch den Verweis auf Art. 58 Abs. 3 Buchstabe f) DSGVO soll klargestellt werden, dass das ULD weiterhin eigene Zertifizierungen entsprechend Art. 42 Abs. 5 Satz 1 2. Alt. DSGVO vornehmen kann."

7. Artikel 1 – § 19 LDSG-E: Ordnungswidrigkeiten, Strafvorschrift

Absätze 2 bis 4 der Vorschrift enthalten Regelungen zur Strafbarkeit bei bestimmten Verstößen. Allerdings gibt es – anders als im geltenden LDSG – keine Vorschriften mehr, die Fehlverhalten durch Mitarbeiter öffentlicher Stellen mit Geldbuße belegen.

Dieses führt zu einer **Sanktionslücke, die geschlossen werden sollte**. Es kommt regelmäßig vor, dass Mitarbeiter öffentlicher Stellen unter Überschreitung ihrer Kompetenzen solche Daten, die nicht offenkundig sind, für eigene Zwecke nutzen. Dies geschieht nicht selten im Kontext von familiären Streitigkeiten oder anderen persönlichen Angelegenheiten. Zum einen würden solche Fälle nicht unter die Strafvorschrift in § 19 LDSG-E fallen. Zum anderen erschiene es ohnehin unverhältnismäßig, diese Verfehlungen als Straftat zu ahnden.

Hier wird vorgeschlagen, **einen Ordnungswidrigkeitentatbestand wie in § 31 LDSG-E Brandenburg** (dortige LT-Drs. 6/7365) **und § 22 LDSG-E Mecklenburg-Vorpommern** (dortige LT-Drs. 7/1568) **zu schaffen**. Dies ist nach der Öffnungsklausel des Art. 84 DSGVO zulässig. Danach können Vorschriften über andere Sanktionen als solche, die bereits in Art. 83 DSGVO geregelt sind, geschaffen werden. Dies wäre hier der Fall, denn die Sanktionen nach Art. 83 DSGVO richten sich nicht gegen Individuen, sondern gegen verantwortliche Stellen. Es bietet sich dann weiter an, **die Strafvorschrift als Qualifizierung des Ordnungswidrigkeitentatbestands zu fassen**, so dass bei Begehung der Ordnungswidrigkeit mit Bereicherungs- oder Schädigungsabsicht eine Straftat vorliegt.

8. Artikel 1 – § 33 Abs. 6 LDSG-E: Auskunftsrecht: eingeschränktes Kontrollrecht

§ 33 Abs. 6 Satz 3 LDSG-E enthält eine Einschränkung des Kontrollrechts der Landesbeauftragten für Datenschutz, die **zu einem kontrollfreien Raum führt** und daher gestrichen werden sollte. Soweit die zuständige oberste Landesbehörde im Einzelfall feststellt, dass durch die Auskunftserteilung an die Landesbeauftragte für Datenschutz die Sicherheit des Bundes oder eines Landes gefährdet würde, ist auch der Landesbeauftragten keine Auskunft mehr zu erteilen. Dies führt dazu, dass die Versagung einer Auskunft an betroffene Personen in solchen Fällen nicht mehr überprüft werden kann. Um diese Kontrollfreiheit herzustellen, reicht eine Erklärung der obersten Landesbehörde aus, die ihrerseits ebenfalls nicht überprüft werden kann. Diese Kontrolllücke ist mit den Grundrechten der Betroffenen, zu denen auch das Auskunftsrecht gehört, nicht vereinbar.

Sie entspricht auch nicht dem geltenden Landesrecht. Nach § 41 Abs. 2 LDSG dürfen in solchen Fällen die Kontrollrechte nur von der Landesbeauftragten für Datenschutz persönlich oder von ihr schriftlich besonders damit Beauftragten ausgeübt werden. Diese Regelung war bislang ausreichend, um Sicherheitsbelange von Bund und Ländern zu wahren. **Für einen vollständigen Ausschluss der Kontrollrechte der Lan-**

desbeauftragten ist auch kein Bedarf ersichtlich. Die oder der Landesbeauftragte ist regelmäßig sicherheitsüberprüft und bis zur Geheimhaltungsstufe „Streng geheim“ ermächtigt.

Die Regelung in § 33 Abs. 6 Satz 3 LDSG-E sollte daher dringend an die bestehende Rechtslage in § 41 Abs. 2 LDSG angepasst werden.

9. Artikel 7 – Änderung des Schulgesetzes, hier § 30 Abs. 3: Übermittlung von Daten an das Jobcenter bzw. die örtliche Agentur für Arbeit

In § 30 Abs. 3 Satz 3 des Gesetzentwurfs ist die Übermittlung von Daten an das Jobcenter bzw. die örtliche Agentur für Arbeit zu Zwecken der Förderung der beruflichen Ausbildung oder der Vermittlung in ein Ausbildungsverhältnis oder ein Qualifizierungsangebot vorgesehen.

An dieser Stelle muss aus Sicht des ULD **klargestellt** werden, dass es sich **lediglich um Übermittlungen im Einzelfall** handeln kann. Keinesfalls kann auf diese Vorschrift eine pauschale Übermittlung z. B. sämtlicher Daten der Absolventen eines Jahrgangs gestützt werden. Daher sollte nach dem Wort „darf“ folgender Passus eingefügt werden: „soweit im Einzelfall erforderlich“.

Außerdem sollten die hier **zu übermittelnden Daten näher bestimmt** werden. Nach der gegenwärtigen Formulierung könnten dies sämtliche bei den Schulen vorliegende Daten sein. Aus diesem Grund wird vorgeschlagen, den Absatz um einen neuen letzten Satz zu ergänzen, der z. B. lauten könnte: „Die Einzelheiten zu der Übermittlung an das Jobcenter bzw. die örtliche Agentur für Arbeit, insbesondere die dabei zu übermittelnden Daten, werden in der Verordnung nach Abs. 11 festgelegt.“

Die in den Punkten 1. bis 9. dieser Stellungnahme angemahnten Änderungen sind von entscheidender Wichtigkeit. Darüber hinaus sollte der Gesetzgeber aber auch die im Folgenden angesprochenen Punkte dringend berücksichtigen. Diese werden in der Reihenfolge der Normen des Gesetzentwurfs dargestellt.

10. Artikel 1 – § 1 LDSG-E: Gesetzeszweck

Nach § 1 Satz 1 besteht der Zweck des Gesetzes darin, bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen das Recht auf informationelle Selbstbestimmung zu wahren. Dagegen enthält die **DSGVO eine deutlich weitere Zweckbestimmung**: den **Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten**. Da der LDSG-E den durch EU-rechtliche Vorschriften gewährten Schutz nur ausgestaltet und z. T. auch einschränkt, ist der angegebene Gesetzeszweck zumindest irreführend. Es stellt sich auch die Frage, ob es nicht einen Verstoß gegen EU-Recht darstellt, wenn der Gesetzeszweck vom umfassenden Schutz der Grundrechte auf das im deutschen Recht verankerte informationelle Selbstbestimmungsrecht verengt wird.

Das BDSG sowie die meisten vorliegenden Gesetzentwürfe für ein neues LDSG verzichten auf die Angabe des Gesetzeszwecks. Soweit sich doch eine solche Vorschrift findet, wird als **Zweck die Ausgestaltung der notwendigen Ergänzungen der DSGVO** und die Umsetzung der JI-Richtlinie genannt (§ 1 LDSG-E Brandenburg, dortige LT-DRs. 6/7365; § 1 LDSG-E Mecklenburg-Vorpommern, dortige LT-Drs. 7/1568). Es wird empfohlen, diesem Beispiel zu folgen.

11. Artikel 1 – § 3 Abs. 2 LDSG-E: Zweckerstreckung zu Organisationsuntersuchungen etc.

In § 3 Abs. 2 LDSG-E werden nunmehr als zum Zweck der eigentlichen Verarbeitung gehörend auch die **Verarbeitung zur Durchführung von Organisationsuntersuchungen und zur Prüfung und Wartung** von automatisierten Verfahren definiert. Anders als die im folgenden Satz adressierte Verarbeitung zu Aus- und Fortbildungszwecken ist jene nicht unter den Vorbehalt gestellt, dass schutzwürdige Interesse der betroffenen Personen entgegenstehen. Es wird empfohlen, zumindest im Hinblick auf die Durchführung von Organisationsuntersuchungen ebenfalls das fehlende Entgegenstehen von schutzwürdigen Interessen der Betroffenen zur Voraussetzung der Verarbeitung zu machen.

Der in einer früheren Fassung des Gesetzentwurfs enthaltene Satz 2 „Die Verarbeitung der Daten zu Test- und Prüfungszwecken ist davon nicht erfasst." sollte wieder aufgenommen werden. Dafür spricht auch, dass sich dieser Satz in § 23 Abs. 2 LDSG-E, der eine Parallelregelung für den Anwendungsbereich der JI-Richtlinie darstellt, noch findet. Dazu sollte in der Begründung klargestellt werden, dass er sich auf Prüfungen im Rahmen von bestimmten Ausbildungen bezieht.

12. Artikel 1 – § 4 Abs. 3 LDSG-E: Zweckänderung bei Daten unter einem Berufsgeheimnis

§ 4 Abs. 3 LDSG-E regelt nunmehr, dass bei Daten, die einem Berufsgeheimnis unterliegen, eine **zweckändernde Verarbeitung nur bei Zustimmung des Schweigepflichtigen** zulässig ist. Im **geltenden LDSG gibt es keine vergleichbare Vorschrift**. Es ist nicht erkennbar, welche konkrete, ansonsten problematische Konstellation hier geregelt werden soll. Aus hiesiger Sicht besteht auch ein gewisser Gegensatz zwischen den allgemeinen datenschutzrechtlichen Regeln für öffentliche Stellen, die jeweils diese Stellen als Verantwortliche adressieren, und dieser Vorschrift, die einzelne Berufsgeheimnisträger adressiert. Es ist vorstellbar, dass es dadurch zu Konflikten zwischen dem organisatorisch vorgeschriebenen Vorgehen der verantwortlichen Stelle und dem Willen einzelner Berufsgeheimnisträger kommt. Ein Beispiel wäre ein Sozialpädagoge im Jugendamt, der im Rahmen der Familienberatung bekannt gewordene Informationen über eine Kindeswohlgefährdung nicht zur Abwehr dieser Gefährdung einsetzen möchte. Nach der Vorschrift wäre eine solche Blockade der Zweckänderung wohl zulässig, selbst wenn ein Tätigwerden zur Abwehr der Gefährdung (und damit eine Zweckänderung) durch die Organisation vorgeschrieben ist.

13. Artikel 1 – LDSG-E: Grundsatz der Direkterhebung

§ 13 Abs. 1 LDSG enthält gegenwärtig den Grundsatz der Direkterhebung, wonach als Grundregel personenbezogene Daten bei den Betroffenen mit ihrer Kenntnis zu erheben sind. Der Grundsatz der Direkterhebung ist als **Konkretisierung des** in der DSGVO in Art. 5 Abs. 1 Buchstabe a) enthaltenen **Grundsatzes der Transparenz** zu verstehen (vgl. EuGH, Urteil vom 01.10.2015, C-01/14). Der Grundsatz der Direkterhebung findet sich z. B. auch im Referentenentwurf eines Gesetzes zur Änderung des Bayerischen Datenschutzgesetzes (dort Art. 4 Abs. 2, siehe dortige LT-Drs. 17/19628). Es wird daher angeregt, den Grundsatz der Direkterhebung in das neue LDSG zu übernehmen, z. B. durch Übernahme des Regelungsgehaltes des § 13 Abs. 1 und Abs. 3 LDSG, etwa mit folgendem Wortlaut:

„**Erhebung beim Betroffenen**

(1) Personenbezogene Daten sind bei den Betroffenen mit ihrer Kenntnis zu erheben. Die Herkunft der Daten und der Zweck der Erhebung sind zu dokumentieren.

(2) Ohne Kenntnis der Betroffenen dürfen personenbezogene Daten nur erhoben werden, wenn

1. die Betroffenen darin eingewilligt haben,
2. eine Rechtsvorschrift dies erlaubt,
3. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechte einzelner dies gebietet oder
4. die Einholung der Einwilligung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre und offensichtlich ist, dass die Verarbeitung im Interesse der oder des Betroffenen liegt und sie oder er in Kenntnis des anderen Zwecks die Einwilligung erteilen würde."

Durch die Aufnahme der Einwilligung in Nr. 1 soll das sog. „Once only"-Prinzip realisiert werden, das z. B. bei dem Projekt Registermodernisierung des Nationalen Normenkontrollrates angestrebt wird. Dabei soll es auf Wunsch der Bürger möglich sein, bei bestimmten Verwaltungsleistungen zu veranlassen, dass vorhandene Daten aus anderen öffentlichen Quellen genutzt werden, um den Bürgern die wiederholte Vorlage solcher Unterlagen und Informationen zu ersparen, die bereits bei anderen Behörden vorhanden sind.

14. Artikel 1 – LDSG-E: Datenschutz-Folgenabschätzung

In Fällen, in denen die Verarbeitung der Daten auf einer Rechtsvorschrift beruht, eröffnet Art. 35 Abs. 10 DSGVO den Mitgliedstaaten die Möglichkeit, die Durchführung einer Datenschutz-Folgenabschätzung auch für den Fall anzuordnen, dass bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte. Von dieser Öffnungsklausel sollte Gebrauch gemacht werden. **Die Folgenabschätzung im Rahmen der Gesetzgebung bewegt sich auf einem anderen Abstraktionsniveau als eine Folgenabschätzung bei der konkreten Konzeption und Implementierung eines** Verfahrens in dem bei dem Verantwortlichen vorhandenen technisch-organisatorischen Umfeld. Während z. B. bei der ersten abstrakt die Einführung von technisch-organisatorischen Maßnahmen wie Pseudonymisierung gefordert werden kann, muss bei der konkreten Konzeption und Implementierung im Wege der Folgenabschätzung überprüft werden, ob die ausgewählten Verfahren und Algorithmen einen hinreichenden Schutz bieten und ob weitere Risiken eingedämmt werden müssen, die aus der Auswahl der Verfahren und Algorithmen oder der Interaktion mit dem konkreten Umfeld entstehen können. Die **konkrete Datenschutz-Folgenabschätzung** wird in solchen Fällen auf der bereits durchgeführten Folgenabschätzung im Rahmen der Gesetzgebung basieren.

Daher wird die Einführung eines weiteren Paragrafen nach dem bisherigen § 7 LDSG-E vorgeschlagen, der folgenden Wortlaut hat:

„Eine Datenschutz-Folgenabschätzung nach Art. 35 der Verordnung (EU) 2016/679 ist im Hinblick auf die Verarbeitungstätigkeit auch durchzuführen, falls die Verarbeitung auf einer gesetzlichen Grundlage beruht und bereits im Rahmen der allgemei-

nen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsnorm eine Datenschutz-Folgenabschätzung erfolgte."

15. Artikel 1 – § 7 LDSG-E: Automatisierte Verfahren

Es ist zu begrüßen, dass in den Gesetzentwurf die bewährten Vorschriften des § 5 Abs. 2 und Abs. 3 LDSG übernommen wurden, die die Freigabe von automatisierten Verfahren vorschreiben und der Landesregierung dazu eine Verordnungsermächtigung zur Regelungen der Einzelheiten bereitstellen.

Allerdings fehlt in § 7 Abs. 1 LDSG-E die **Verpflichtung, die automatisierten Verfahren vor der Freigabe zu testen,** so wie dies im geltenden Recht in § 13 Abs. 2 LDSG vorgeschrieben ist. Ohne Durchführung eines Tests der Funktionsfähigkeit des automatisierten Verfahrens vor der Freigabe verfehlt diese aber ihren Sinn. Es soll ja mit der Freigabe gerade manifestiert werden, dass das Verfahren fehlerlos läuft und daher in den Echtbetrieb übernommen werden kann. Dies lässt sich ohne Test nicht bewerkstelligen. Daher sollte in Abs. 1 nach dem Wort „Datenverarbeitung" eingefügt werden: „zu testen und".

§ 7 Abs. 4 LDSG-E bedarf einer Änderung, um **die Verantwortlichkeit der beteiligten Stellen an die Kriterien des EU-Rechts anzupassen**. Anders als das bisherige nationale Datenschutzrecht stellt das EU-Recht in Art. 26 Abs. 1 DSGVO für eine gemeinsame Verantwortlichkeit nicht darauf ab, ob gemeinsam personenbezogene Daten verarbeitet werden, sondern ob gemeinsam die Zwecke und Mittel der Datenverarbeitung festgelegt werden. Faktisch ist dies bereits gegenwärtig Kriterium für viele gemeinsame Verfahren, etwa im Bereich der Justiz. Hier ist das Justizministerium zwar nicht an einer gemeinsamen operativen Verarbeitung personenbezogener Daten beteiligt, legt aber gemeinsam mit den operativ tätigen Stellen die Zwecke und Mittel der Datenverarbeitung fest, indem Hardware, Software und Dienstleistungen beauftragt bzw. beschafft und für die Stellen der Justiz bereitgestellt werden.

Dementsprechend sollte § 7 Abs. 4 LDSG-E wie folgt geändert werden (Änderungen fett hervorgehoben):

„Für automatisierte Verfahren, **bei denen mehrere Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen**, kann die zuständige oberste Landesbehörde durch Verordnung Regelungen im Sinne von Artikel 26 Absatz 1 der Verordnung (EU) 2016/679 festlegen und eine zentrale Stelle bestimmen, der die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit des automatisierten Verfahrens übertragen wird."

16. Artikel 1 – § 8 LDSG-E: Beschränkung der Informationspflicht

Die Vorschrift enthält Beschränkungen der Informationspflicht nach Art. 13 Abs. 3 oder Art. 14 DSGVO, basierend auf Art. 23 DSGVO. Namentlich die Beschränkung in Abs. 1 Nr. 1 erscheint sehr weitgehend; das Abstellen auf die **ordnungsgemäße Erfüllung der in der Zuständigkeit** der jeweiligen Stellen **liegenden Aufgaben** könnte dahingehend missverstanden werden, dass die Beschränkung der Informationspflicht bereits dann greifen kann, wenn die Erteilung der Information einen gewissen Aufwand erfordert. Es wird daher angeregt, die Nr. 1 zu streichen; dies entspricht auch der Regelung in § 10 LDSG-E Brandenburg (dortige LT-Drs. 6/7365).

In jedem Fall ist zu berücksichtigen, dass die in § 8 Abs. 1 Nr. 2 LDSG-E genannten Aspekte der öffentlichen Sicherheit bereits durch § 8 Abs. 1 Nr. 1 LDSG-E abgedeckt

werden, denn der dort in Bezug genommene Art. 23 Abs. 1 Buchstabe c) DSGVO bezieht sich bereits auf die öffentliche Sicherheit.

17. Artikel 1 – § 9 LDSG-E: Beschränkung der Auskunftspflicht

In Absatz 2 der Vorschrift wird die grundsätzlich nach der DSGVO bestehende Auskunftspflicht ausgeschlossen, wenn die **Daten ausschließlich zu Zwecken der Datensicherung und der Datenschutzkontrolle** verarbeitet werden und die Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

Diese Vorschrift begegnet Bedenken im Hinblick auf die Reichweite des Ausschlusses des grundrechtlich garantierten Auskunftsrechts. Weiterhin ergeben sich terminologische Unklarheiten. So ist z. B. nicht klar, was Daten sein sollen, die nur zum Zwecke der Datenschutzkontrolle verarbeitet werden. Obwohl der Begriff auch im geltenden BDSG verwendet wird, findet sich einschlägigen Kommentaren keine Erläuterung dazu. Weiterhin steht der in der Vorschrift beschriebene Ausschluss der Verarbeitung zu anderen Zwecken durch technische und organisatorische Maßnahmen in einem Spannungsverhältnis zu der von der DSGVO definierten Einschränkung der Verarbeitung. In der Regel wäre davon auszugehen, dass im Falle einer Einschränkung der Verarbeitung entsprechende technische und organisatorische Maßnahmen getroffen werden, um die Einschränkung durchzusetzen. Es ist nicht klar, wie umgekehrt technisch-organisatorische Maßnahmen von sich aus zu einer Einschränkung der Verarbeitung führen sollten.

In Abs. 2 wird außerdem eine andere Formulierung verwendet als in Abs. 1. Während es in Abs. 1 heißt: „das Recht auf Auskunft besteht nicht“, verwendet Abs. 2 die Formulierung: „Die betroffene Person kann keine Auskunft verlangen“. Es wird angeregt, **einheitliche Formulierungen** zu verwenden, wenn die gleiche Regelung (Auskunft wird nicht erteilt) beabsichtigt ist.

18. Artikel 1 – § 12 LDSG-E: Verarbeitung besonderer Kategorien personen bezogener Daten

Im LDSG-E **fehlt es an einer eigenständigen allgemeinen Erlaubnis zur Verarbeitung besonderer Kategorien personenbezogener Daten** im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 (im Folgenden: „sensibler Daten“) wie sie z. B. in § 22 Abs. 1 Nr. 2 Buchstabe a) BDSG-neu enthalten ist. Dagegen schreibt § 12 Abs. 1 LDSG-E nur vor, dass spezielle technisch-organisatorische Maßnahmen dann einzusetzen, wenn sensible Daten auf der Grundlage des 2. Abschnitts des LDSG-E, also aller Vorschriften zur Umsetzung der DSGVO, verarbeitet werden.

Nach hiesiger Auffassung führt dies zu zwei Konsequenzen:

1. Es fehlt an einer allgemeinen Befugnis zur Verarbeitung sensibler Daten. Diese dürfen also nur dann verarbeitet werden, wenn dies in Abschnitt 2, Unterabschnitt 3 des LDSG-E zu den dort genannten speziellen Zwecken oder durch bereichsspezifische Vorschriften erlaubt ist.

   Dagegen ist es aus Sicht des ULD **von Vorteil, eine allgemeine Norm zu haben**, die die Verarbeitung sensibler Daten zulässt. Zwar werden in aller Regel spezielle Regelungen zur Verfügung stehen. Allerdings kommen erfahrungsgemäß immer wieder besonders gelagerte Fälle vor, die nur mit einer allgemeinen Norm zu lösen sind.

Das bisherige LDSG hält so eine allgemeine Norm in § 11 Abs. 3 Nr. 7 vor. Auch der Gesetzgeber des BDSG-neu hat ausweislich der Begründung (BR-Drs. 110/17, S. 94) die entsprechenden allgemeinen Normen aus dem bisherigen BDSG in das BDSG-neu übernommen. Ebenso findet sich eine allgemeine Rechtsgrundlage zur Verarbeitung von Daten im Sinne von Art. 9 Abs. 1 DSGVO im Gesetzentwurf für ein neues Hessisches Datenschutz- und Informationsfreiheitsgesetz (dortige LT-Drs. 19/5728) in § 20 Abs. 1 Nr. 4 Buchstabe a).

2. Auch die bereichsspezifischen Vorschriften im öffentlichen Bereich stützen sich größtenteils (soweit nicht der Gesundheitssektor betroffen ist) auf die Öffnungsklausel in Art. 9 Abs. 1 Buchstabe g) DSGVO. Daher müssen auch für diese Verarbeitungen die angemessenen und spezifischen Maßnahmen i.S.d. Art. 9 Abs. 2 DSGVO gelten.

Der Bundesgesetzgeber hat dies dadurch bewirkt, dass er den § 22 Abs. 1 Nr. 2 Buchstabe a) BDSG-neu gleichsam als Generalklausel allen bereichsspezifischen Verarbeitungsnormen für sensible Daten voranstellt. Daher soll auf Bundesebene gelten: „Die in Absatz 2 Satz 2 aufgeführten Maßnahmen treffen jeden Verantwortlichen und damit auch jeden, der besondere Kategorien personenbezogener Daten verarbeitet." (BR-Drs. 110/17, S. 94)

Dieses Vorgehen scheint vorzugswürdig gegenüber dem LDSG-E, wo ausweislich der Begründung zu § 12 Abs. 1 die bereichsspezifischen Regelungen quasi dazu eingeladen werden, auf § 12 LDSG-E zu verweisen und erst dadurch die Geltung der Pflicht zu speziellen technisch-organisatorischen Maßnahmen zu bewirken. Zwar werden im vorliegenden Artikelgesetz einige solche Verweise in Spezialgesetze eingefügt. Es muss aber wohl davon ausgegangen werden, dass dies nicht flächendeckend erfolgt ist.

Aus diesen Gründen wird empfohlen zu prüfen, ob in das LDSG eine Regelung analog zu der in § 22 Abs. 1 Nr. 2 Buchstabe a) (und ggfs. bis d)) BDSG-neu aufgenommen werden sollte.

19. Artikel 1 – § 13 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Absatz 2 der Vorschrift ordnet an, dass zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete sensible Daten anonymisiert werden, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist. Davor müssen sie pseudonymisiert werden.

Dies stellt einen **Rückschritt im Vergleich zur Rechtslage unter dem noch geltenden LDSG** dar. Dieses sieht in § 22 Abs. 1 vor, dass sämtliche zu wissenschaftlichen Zwecken verarbeitete Daten, nicht nur die sensiblen Daten, zu pseudonymisieren und später zu anonymisieren sind. Auch nach der entsprechenden Vorschrift des LDSG-E Brandenburg (§ 24 Abs. 2, dortige LT-Drs. 6/7365) trifft die Pflicht zur Pseudonymisierung und zur Anonymisierung sämtliche Daten.

Die Gesetzesbegründung gibt nicht an, warum von der bewährten Regelung abgewichen wird. Auch aus praktischer Sicht ist dies nicht nachvollziehbar. Wird von den forschenden Stellen eine Infrastruktur zur Pseudonymisierung bereitgehalten, wie dies zumindest im Hinblick auf die sensiblen Daten der Fall ist, so stellt es keine Mehraufwand dar, alle in der Forschung verwendeten Daten zu pseudonymisieren.

Darüber hinaus entspricht die hier vorgenommene **Legaldefinition des Begriffs „Anonymisierung" nicht den Vorgaben der DSGVO und der JI-Richtlinie**. Denn in Erwägungsgrund 26 der DSGVO bzw. gleichlautend in Erwägungsgrund 21 der JI-Richtlinie findet sich die Aussage:

> „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."

Dabei handelt es sich um eine absolute Definition der Anonymisierung, die eben nicht eine Einschränkung („nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft") bezüglich der Zuordenbarkeit enthält. Daher sollte eine abweichende Definition auch nicht in das LDSG aufgenommen werden. Anderenfalls spricht viel für einen **Verstoß des LDSG gegen EU-Recht**.

Daher sollte § 13 Abs. 2 Satz 1 wie folgt gefasst werden:

> „Zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete sind so zu verändern, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (Anonymisierung), sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen."

20. Artikel 1 – § 15 Datenverarbeitung im Beschäftigungszusammenhang

Absatz 2 der Vorschrift regelt, dass Daten von Beschäftigten, die im Rahmen der Durchführung technischer und organisatorischer Maßnahmen zur Datensicherheit verarbeitet oder in einem automatisierten Verfahren gewonnen werden, nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden dürfen. Dies entspricht der bisherigen Rechtslage nach § 23 Abs. 2 LDSG. Allerdings enthält die Vorschrift nun einen neuen Satz 2, welcher lautet:

> „Dies gilt im Bereich der justiziellen Tätigkeit nicht für die Auswertung von Akten zum Zweck der Dienstaufsicht, der dienstlichen Beurteilung und der Erteilung von Dienstzeugnissen."

In der Begründung finden sich dazu die folgenden Bemerkungen:

> „Satz 2 ermöglicht die Auswertung von Akten für dienstliche Zwecke, um etwa auch bei elektronischer Aktenführung die ordnungsgemäße Aufgabenerfüllung von Gerichten im Rahmen ihrer justiziellen Tätigkeit weiterhin beobachten und gewährleisten zu können. Bei der Umstellung auf eine elektronische Aktenführung wird für die dienstliche Beurteilung von Richterinnen und Richtern eine Verwertung elektronischer Akten erforderlich sein. Auch die Möglichkeit der Verwertung automatisch generierter Verfahrenszahlen erscheint für diese Zwecke unverzichtbar."

Diese Ausführungen überraschen, denn die Regelung in § 15 Abs. 2 LDSG-E **bezieht sich ausschließlich auf Daten, die im Rahmen technisch-organisatorischer Maßnahmen verarbeitet** werden oder anfallen, wie z. B. Protokolldaten.

Die in der Begründung angesprochenen automatisch generierten Verfahrenszahlen über erledigte oder offene Fälle werden nicht für technisch-organisatorische Maßnahmen verarbeitet. Abs. 2 Satz 1 der Vorschrift sperrt daher keineswegs die vorgesehene Auswertung solcher Verfahrenszahlen. Daher sollte der vorgesehene Satz 2 gestrichen werden.

Um deutlicher zu machen, dass mit dieser Vorschrift nur solche Daten erfasst werden, die im Rahmen von technischen und organisatorischen Maßnahmen zur Datensicherheit verarbeitet werden, können auch in Absatz 2 Satz 1 die Wörter „oder in einem automatisierten Verfahren gewonnen werden" gestrichen werden.

21. Artikel 1 – Abschnitt 3 LDSG-E: Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

Das ULD begrüßt, dass Regelungen zur Umsetzung der JI-Richtlinie im LDSG-E getroffen werden. Solche einheitlichen Vorgaben fördern gemeinsame Standards für die öffentlichen Stellen in Schleswig-Holstein bei der Verarbeitung personenbezogener Daten.

22. Artikel 1 – § 21 Nr. 17 und § 27 LDSG-E: Einwilligung

Die Einwilligung ist in der JI-Richtlinie nicht als eigenständige Rechtsgrundlage für die Verarbeitung personenbezogener Daten vorgesehen. Sie wird lediglich in zwei Erwägungsgründen (35 und 37) erwähnt. Auch dort ist sie nicht als eigenständige Grundlage für die Verarbeitung personenbezogener Daten gemeint. Ausdrücklich besagt Erwägungsgrund 35:

> „In einem solchen Fall sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen."

Vielmehr nimmt Erwägungsgrund 35 Regelungskonstrukte in den Blick, die durch Gesetz eine bestimmte Datenverarbeitung erlauben und hier zusätzlich die Einwilligung der betroffenen Personen vorsehen. Gedacht ist etwa an die Regelungen in der StPO über die Durchführung von DNA-Analysen. Hier ist die Einwilligung der Betroffenen Voraussetzung dafür, dass eine gerichtliche Anordnung entfallen kann. Die Einwilligung ist damit nicht Zulässigkeitsvoraussetzung der DNA-Analyse, sondern ermöglicht lediglich Verfahrenserleichterungen.

Streng genommen handelt es sich bei dieser „Einwilligung" nicht um eine Einwilligung im Sinne des Art. 6 Abs. 1 Buchstabe a DSGVO, da sie nicht Rechtsgrundlage für die Datenverarbeitung ist. Es wird daher empfohlen, dies schon begrifflich deutlich zu machen und anstelle der Einwilligung **in § 27 LDSG-E den Begriff „Zustimmung" zu verwenden**. Den Begriff „zustimmen" verwendet auch die **JI-Richtlinie** in Erwägungsgrund 35.

23. Artikel 1 – § 23 Abs. 2 LDSG-E: Zweckidentität

Die Regelung in Abs. 2 über Verarbeitungszwecke, die keine Zweckänderung darstellen, passt systematisch besser zur Zweckänderungsregelung des § 25 LDSG-E. Sie sollte daher als Abs. 2 zu § 25 LDSG-E aufgenommen werden.

In § 23 Abs. 2 LDSG-E werden als zum Zweck der eigentlichen Verarbeitung gehörend auch die **Verarbeitung zur Durchführung von Organisationsuntersuchungen und zur Prüfung und Wartung** von automatisierten Verfahren definiert. Anders

als die im folgenden Satz adressierte Verarbeitung zu Aus- und Fortbildungszwecken ist jene nicht unter den Vorbehalt gestellt, dass schutzwürdige Interesse der betroffenen Personen entgegenstehen. Es wird empfohlen, zumindest im Hinblick auf die Durchführung von Organisationsuntersuchungen ebenfalls das fehlende Entgegenstehen von schutzwürdigen Interessen der Betroffenen zur Voraussetzung der Verarbeitung zu machen.

24. Artikel 1 – § 24 LDSG-E: Verarbeitung besonderer Kategorien personenbezogener Daten

Die Vorschrift soll eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 10 der JI-Richtlinie schaffen.

Für bestimmte Kategorien im Sinne des § 21 Nr. 14 LDSG-E reicht die Erforderlichkeit zur Aufgabenerfüllung als Voraussetzung für die Datenverarbeitung allein nicht aus, um eine verhältnismäßige Eingriffsschwelle zu definieren. Dies gilt namentlich für genetische und biometrische Daten (§ 21 Nr. 11 und 12 LDSG-E). Bei der Verarbeitung solcher Kategorien von Daten handelt es sich um besonders schwerwiegende Grundrechtseingriffe. Das geltende Recht knüpft die Verarbeitung solcher Daten daher an besonders hohe Voraussetzungen (siehe etwa § 183 LVwG für erkennungsdienstliche Maßnahmen und § 183a LVwG für molekulargenetische Untersuchungen). Biometrische Verfahren oder die Erhebung genetischer Daten allein zum Zweck der Erfüllung jeglicher in Betracht kommender Aufgaben zuzulassen, wäre nicht verhältnismäßig. Dies sollte auch in Zukunft verhindert werden. Der **Entwurf ist hierfür nicht geeignet**.

Wir regen daher an, in § 24 jedenfalls **eine Ausnahme für genetische und biometrische Daten vorzusehen und deren Verarbeitung nur zuzulassen, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt.**

Ob die **in Absatz 2 festgelegten Garantien** für die Verarbeitung besonderer Kategorien personenbezogener Daten das Sicherheitsniveau für diese Daten tatsächlich erhöhen und damit dem besonderen Schutzbedarf entsprechen, muss ebenfalls **bezweifelt** werden. Denn größtenteils gelten die dort genannten Anforderungen auch für alle anderen personenbezogenen Daten.

25. Artikel 1 – § 26 LDSG-E: Datenverarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken

Die **Regelung in § 26 LDSG-E ist äußert vage** und unbestimmt. Unklarheiten beginnen bereits mit der Zweckrichtung der Norm. Die Überschrift spricht davon, dass die Verarbeitung zu archivarischen, wissenschaftlichen und statischen *Zwecken* erfolgt. Nach Satz 1 der Vorschrift sollen die Daten hingegen „im Rahmen der" in § 20 genannten Zwecken – also zur Verhütung oder Verfolgung von Straftaten – erfolgen, und zwar in archivarischer, wissenschaftlicher oder statistischer *Form*.

Wie ein Vergleich mit § 13 LDSG-E zeigt, ist hierfür eine weitaus **präzisere Regelung möglich**. Auch im geltenden Recht gibt es mit den Forschungsklauseln in § 22 LDSG Schleswig-Holstein oder in § 476 der Strafprozessordnung präzisere Regelungen. § 26 LDSG-E sollte **hinter diesen Standards nicht zurückbleiben**.

26. Artikel 1 – § 29 LDSG-E: Datengeheimnis

§ 29 LDSG-E sieht eine Verpflichtung auf das Datengeheimnis vor. Die Regelung begegnet keinen inhaltlichen Bedenken. Wir weisen jedoch darauf hin, dass an dieser

Stelle **keine Kongruenz** zwischen Abschnitt 2 und Abschnitt 3 besteht. Denn eine entsprechende Regelung fehlt im Abschnitt 2. Damit entspricht Abschnitt 2 der Rechtslage im bisherigen LDSG Schleswig-Holstein, und Abschnitt 3 entspricht der Rechtslage im Bund. Das LDSG Schleswig-Holstein verzichtet seit der Novellierung im Jahr 2000 auf das Datengeheimnis, da aufgrund der Verschwiegenheitspflichten von Beamtinnen und Beamten sowie Beschäftigten im öffentlichen Dienst und der Verpflichtung anderer Personen nach dem Verpflichtungsgesetz kein Bedarf für eine zusätzliche Verpflichtung auf das Datengeheimnis gesehen wird.

Zur **Aufrechterhaltung einheitlicher Standards** in Schleswig-Holstein sollte eine gleichartige Regelung für den Bereich der DSGVO (Abschnitt 2) und den Bereich der JI-Richtlinie (Abschnitt 3) getroffen werden. Beide Lösungen sind dabei möglich. Einer Streichung des § 29 LDSG-E stehen aus hiesiger Sicht keine Bedenken entgegen.

27. Artikel 1 – § 2 Abs. 2, § 8 Abs. 4, § 36, § 60 Abs. 1 und § 61 Abs. 2 LDSG-E: „justizielle Tätigkeit“

Bei dem Begriff der justiziellen Tätigkeit handelt es sich um einen **europarechtlichen Begriff**, der im deutschen Recht bislang in dieser Form nicht verwendet wurde. Eingeführt im deutschen Recht ist bislang lediglich der ebenfalls europarechtliche Begriff der justiziellen Zusammenarbeit in der EU. Da mit dem Begriff der justiziellen Tätigkeit vorliegend rein nationale Sachverhalte geregelt werden, kommt es auf eine EU-weite Einheitlichkeit des Begriffs hier nicht an. Wichtiger ist vielmehr, dass der Begriff den Anforderungen an die Normenklarheit und Bestimmtheit genügt. Hierfür eignen sich Begriffe aus dem nationalen Recht in der Regel besser als solche aus dem EU-Recht. Begriffe aus dem EU-Recht bilden die gemeinsame Schnittmenge aller Mitgliedstaaten ab, was naturgemäß eine gewisse Unschärfe erfordert. Dies trifft auch auf den Begriff der justiziellen Tätigkeit zu. **Klarer ist dagegen der Begriff der richterlichen Unabhängigkeit**, der seine Grundlage in Art. 97 GG findet. Er wird zudem **seit Jahren im LDSG verwendet, um die Kontrollbefugnisse des Unabhängigen Landeszentrums für Datenschutz abzugrenzen**.

Sofern der Begriff der justiziellen Tätigkeit im Gesetz beibehalten wird, sollte zumindest in der Begründung **klargestellt werden, dass damit Tätigkeiten in richterlicher Unabhängigkeit gemeint ist.** Diese Lösung wurde in Hessen gewählt. Der Entwurfstext für das Gesetz (LT-Drs. 19/5728) verwendet, z. B. in § 13 Abs. 5 HDSIG-E, den europarechtlichen Begriff der „justiziellen Tätigkeit“ und in der Begründung wird dieser Begriff wie folgt erläutert (z. B. Begründung zu § 13 Abs. 5 HDSIG, LT-Drs. 19/5728, S. 104):

> „Soweit in Abs. 5 von einem Handeln der Gerichte in justizieller Tätigkeit die Rede ist, ist dies als Tätigwerden in richterlicher Unabhängigkeit zu verstehen.“

Zudem sollte **geregelt werden, durch wen die Aufsicht im Bereich der „justiziellen Tätigkeit“** ausgeübt wird. Erwägungsgrund 20 der DSGVO führt zur Aufsicht in diesem Bereich Folgendes aus:

> „Damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt, sollten die Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch die Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein. Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollten **besondere Stellen im Justizsystem des Mitgliedstaats** betraut werden können, die insbesondere die Einhaltung der Vorschriften der Verordnung sicherstellen, Richter und Staatsanwälte besser für ihre

Pflichten aus dieser Verordnung sensibilisieren und Beschwerden in Bezug auf derartige Datenverarbeitungsvorgänge bearbeiten sollten."

Eine Aufsicht über die Datenverarbeitung im Bereich der justiziellen Tätigkeit ist also durchaus von der DSGVO vorgesehen, allerdings nicht durch eine Aufsichtsbehörde, sondern durch eine **justizeigene Aufsicht**, die die richterliche Unabhängigkeit wahrt. Die Erfahrungen des ULD zeigen, dass es einen **Bedarf für eine Aufsicht** gibt. Das ULD erreicht regelmäßig eine Vielzahl von Beschwerden, die nicht angenommen werden können, da sie Datenverarbeitungen in richterlicher Unabhängigkeit betreffen. Den Beschwerdeführern ist es in diesen Fällen nur schwer vermittelbar, dass es für ihre Anliegen keine Möglichkeit der datenschutzrechtlichen Überprüfung gibt.

28. Artikel 1 – Spezifische Regelungen für automatisierte Verfahren

In § 7 LDSG-E sind spezifische Regelungen für automatisierte Verfahren aufgenommen worden (Test und Freigabe, Verordnungsermächtigung für Regelungen zur ordnungsgemäßen Datenverarbeitung, Einrichtung gemeinsamer Verfahren und Abrufverfahren). Sie entsprechen der geltenden Rechtslage im LDSG, die bislang für alle öffentlichen Stellen gilt. Um diesen **einheitlichen Standard auch künftig aufrechtzuerhalten**, sollte die Regelung des § 7 Abs. 1-3 LDSG-E auch im Abschnitt 3 aufgenommen werden. Die Übernahme von § 7 Abs. 4 LDSG-E ist nicht erforderlich, da § 39 Satz 5 LDSG-E bereits eine entsprechende Regelung trifft. Alternativ kann § 39 Satz 5 LDSG-E gestrichen und § 7 Abs. 4 LDSG-E in diesen Abschnitt 3 übernommen werden. Als Standort bietet es sich an, **diese Regelung als neuen § 41** hinter den Regelungen über Gemeinsam Verantwortliche (§ 39) und Anforderungen an die Sicherheit der Datenverarbeitung (§ 40) aufzunehmen.

29. Artikel 1 – § 40 LDSG-E: Begriffe „Gefahr" und „betroffene Person"

Im Zusammenhang mit der Gewährleistung des Datenschutzes durch technische und organisatorische Maßnahmen verwendet der Gesetzentwurf nicht durchgängig dieselben Begriffe. So spricht der Entwurf in den §§ 40 ff. an einigen Stellen von einem Risiko der Datenverarbeitung für Rechtsgüter von Personen. An anderen Stellen ist die Rede von Gefahren oder erheblichen Gefahren.

Die JI-Richtlinie verwendet hingegen **durchgängig den Begriff des Risikos**. Dies ist auch **sachgerecht**, da alle erdenklichen Risiken der Datenverarbeitung, auch solche mit sehr geringer Eintrittswahrscheinlich zu betrachten und in eine Risikoabwägung einzustellen sind**. Diese Betrachtung von vornherein auf Gefahren im Sinne des Polizei- und Ordnungsrechts – was die Verwendung des Begriffs der „Gefahr" im Gesetzentwurf nahelegt – zu beschränken, würde den Sinn der JI-Richtlinie verfehlen.**

Zudem beschränkt der Gesetzentwurf die Betrachtung der Risiken/Gefahren oftmals auf die **Rechtsgüter der betroffenen Personen**. Die **JI-Richtlinie geht hingegen darüber hinaus**. Danach sind die Rechtsgüter aller natürlichen Personen einzubeziehen, unabhängig davon, ob Daten zu ihrer Person verarbeitet werden. Auf diese Weise können beispielsweise **auch Risiken der Diskriminierung von Personen oder Personengruppen** berücksichtigt werden.

Um das LDSG an die Vorgaben der JI-Richtlinie anzupassen, ist es **erforderlich, durchgängig statt des Begriffs der „Gefahr" den des Risikos und anstelle des Begriffs der „betroffenen Person(en)" den Begriff der „natürlichen Person(en)" zu verwenden.**

30. Artikel 1 – § 40 LDSG-E: Anforderungen an die Sicherheit der Datenverarbeitung

Es wird im Sinne einer verbesserten Handhabbarkeit der Regelung vorgeschlagen**, Absatz 3 ersatzlos zu streichen und Absatz 2 Satz 2 wie folgt neu zu fassen:**

„Die Maßnahmen nach Absatz 1 sollen gewährleisten, dass

1. grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden; diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit (Datenminimierung),
2. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
3. dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell und die zu ihrer Verarbeitung eingesetzten Systeme und Dienste integer bleiben (Integrität),
4. personenbezogene Daten und die zu ihrer Verarbeitung vorgesehenen Systeme und Dienste zeitgerecht zur Verfügung stehen (Verfügbarkeit),
5. jede Verarbeitung von personenbezogenen Daten ausschließlich im Rahmen im Vorhinein bestimmter Befugnisse für vorab festgelegte rechtmäßige Zwecke erfolgt und die Daten hierfür nach den jeweiligen Zwecken und nach unterschiedlichen Betroffenen getrennt werden können (Nichtverkettung),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten einschließlich der zur ihrer Umsetzung getroffenen technisch-administrativen Voreinstellungen vollständig, aktuell und einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können, personenbezogene Daten ihrem Ursprung zugeordnet werden können und festgestellt werden kann, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat (Transparenz), und
7. die Datenverarbeitung so organisiert und die eingesetzten technischen Systeme so gestaltet sind, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 54 und 55 wirksam ermöglichen (Intervenierbarkeit)."

Für den **Anwender des Gesetzes** ist die derzeitige Fassung der Absätze 2 und 3 in der Gesamtschau als Vermischung von „neuen Gewährleistungszielen" und „alten Kontrollmaßnahmen" **nicht handhabbar**. Die in Absatz 2 aufgezählten Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit folgen dem Grundgedanken der technikunabhängigen Formulierung von Sicherheitsanforderungen, decken jedoch noch nicht alle erforderlichen Aspekte der Datenverarbeitung ab. Stattdessen werden hier sieben Gewährleistungsziele normiert, die auch die Basis für das Standard-Datenschutzmodell bilden. Sie beschreiben die Schutzrichtung des Datenschutzes und sind sowohl in Art. 4 der JI-Richtlinie und in Art. 5 der DSGVO bereits vorgebildet. Sie sind vor allem **seit 2012 Bestandteil des LDSG Schleswig-Holstein und haben ihre Praxistauglichkeit bewiesen**. Zudem sind sie **in verschiedenen Dokumenten des IT-Planungsrates verankert** (etwa in der Nationalen E-Government-Strategie).

31. Artikel 1 – § 52 Abs. 3 LDSG-E: Verwendung von Protokolldaten für Strafverfahren

§ 52 Absatz 3 eröffnet die Möglichkeit, durch eine weitere Rechtsvorschrift die Verwendung der **Protokolldaten**, die aufgrund der Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters – insbesondere bezüglich der Tätigkeiten der Beschäftigten – anfallen, für Straf- oder Ordnungswidrigkeitenverfahren zu erlauben. Der ursprüngliche Zweck der Protokolldatenerhebung besteht in der Durchführung von Aufsichts- und Kontrollaufgaben sowie zur Gewährleistung der Datensicherheit und Datenintegrität. Diese Zwecke dienen internen Abläufen. Die **Nutzung für Straf- und Ordnungswidrigkeitenverfahren kommt allenfalls dann in Betracht, wenn diese mit internen Abläufen der Datenverarbeitung in einem Zusammenhang stehen**. Dies sollte im Gesetz oder zumindest in der Begründung **klargestellt** werden.

32. Artikel 1 – §§ 58-60 LDSG-E: Datenschutzbeauftragte

Die Regelung über die behördlichen Datenschutzbeauftragten gilt ausschließlich für den Abschnitt 3. Für Datenschutzbeauftragte im Bereich der DSGVO gilt diese unmittelbar. Durch diese unterschiedlichen Regelungen kann eine vollständige Harmonisierung der Anforderungen an die Benennung, die Stellung und die Aufgaben behördlicher Datenschutzbeauftragter der öffentlichen Stellen in Schleswig-Holstein nicht erreicht werden. Dies ist vor allem deshalb ungünstig, weil vermutlich in den unter den Abschnitt 3 fallenden öffentlichen Stellen die Datenschutzbeauftragten sowohl für die Datenverarbeitung nach Abschnitt 2 als auch für die nach Abschnitt 3 benannt sein werden. Denn üblicherweise werden in den Stellen personenbezogene Daten auch zu anderen Zwecken als zur Verhütung und Verfolgung von Straftaten verarbeitet (z. B. Beschäftigtendaten).

Daher würde eine **einheitliche Regelung der Benennung, Stellung und Aufgaben von behördlichen Datenschutzbeauftragten** im Abschnitt 1 die größtmögliche **Rechtssicherheit und Anwendungserleichterung für die öffentlichen Stellen** bieten. Diese Lösung hat der Bundesgesetzgeber gewählt und in einem allgemeinen Teil Regelungen für alle Datenschutzbeauftragten von Bundesbehörden geschaffen. Zur Begründung ist dort ausgeführt (BT-Drs. 18/11325, Begründung zu §§ 5 bis 7, S. 81):

> „Kapitel 3 enthält Vorschriften für die Benennung, die Stellung und die Aufgaben der Datenschutzbeauftragten öffentlicher Stellen des Bundes. Die Rechtsstellung der behördlichen Datenschutzbeauftragten in der Bundesverwaltung sollte im Anwendungsbereich der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und für die Bereiche außerhalb des Unionsrechts (z. B. für die Nachrichtendienste) einheitlich ausgestaltet sein."

Sofern die Regelungen nicht zusammengeführt werden, sollten sie **zumindest inhalts- und wortgleich gestaltet** werden. Der überwiegende Teil der §§ 58-60 entspricht dem Wortlaut der DSGVO und der JI-Richtlinie, so dass insoweit kein Änderungsbedarf besteht. Abweichungen von Wortlaut und Regelungstiefe der DSGVO sind lediglich in § 59 Abs. 4 und Abs. 6 LDSG-E enthalten.

Nach Absatz 4 der Vorschrift ist die **Abberufung** der oder des Datenschutzbeauftragten nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Zusätzlich wird ein besonderer **Kündigungsschutz** geregelt. Für behördliche Datenschutzbeauftragte, die nach der DSGVO bestellt werden, fehlt es an vergleichbaren Vorgaben. Anders als für den nichtöffentlichen Bereich werden solche **Schutz-**

normen für den öffentlichen Bereich vom ULD als verzichtbar angesehen. Sie finden sich auch nicht im Entwurf für ein Hessisches Datenschutz- und Informationsfreiheitsgesetz. In jedem Fall sollte eine **Regelung gefunden werden, die nicht zwischen behördlichen Datenschutzbeauftragten unterscheidet, die unter der DSGVO bzw. der JI-Richtlinie und deren Umsetzung im LDSG bestellt** werden.

Eine **weitere Ungleichbehandlung** findet sich auch hinsichtlich des **Zeugnisverweigerungsrechts** in Absatz 6 der Vorschrift. Die nach der DSGVO bestellten Datenschutzbeauftragten verfügen nicht über ein solches Zeugnisverweigerungsrecht, obwohl sie in der Praxis eher häufiger mit Daten in Berührung kommen, die unter die beruflichen Schweigepflichten fallen; man denke nur an Gesundheitsämter und Jugendämter. Ein solches Zeugnisverweigerungsrecht für beide Gruppen von behördlichen Datenschutzbeauftragten ist z. B. im Entwurf für ein Hessisches Datenschutz- und Informationsfreiheitsgesetz (§ 6 Abs. 5) und im Entwurf für ein geändertes Landesdatenschutzgesetz Nordrhein-Westfalen (§ 29 Abs. 3, ggf. in Verbindung mit § 64) enthalten.

Es wird daher empfohlen, die Vorschrift um einen weiteren Absatz mit folgendem Wortlaut zu ergänzen:

> „Absatz 6 gilt entsprechend für Datenschutzbeauftragte, die nach Art. 37 der Verordnung (EU) 2016/679 bestellt wurden."

33. Artikel 1 – § 62 LDSG-E: Aufgaben der oder des LfD: Information

§ 17 Abs. 4 LDSG-E sieht vor, dass die oder der Landesbeauftragte **über Planungen des Landes zum Aufbau oder zur wesentlichen Änderung von Systemen zur automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten** ist. Dies sollte auch im Bereich des Abschnitts 3 des LDSG gelten, der die Vorschriften zur Umsetzung der JI-Richtlinie enthält. Daher sollte **§ 62 LDSG-E um eine entsprechende Regelung ergänzt** werden. Diese Unterrichtung ist nicht gleichzusetzen mit der Anhörung nach § 45 LDSG-E. Anders als bei der Anhörung handelt es sich hier lediglich um eine **Information** an die oder den Landesbeauftragten.

34. Artikel 1 – § 64 LDSG-E: Untersuchungsbefugnisse der oder des LfD

§ 64 Abs. 2 und 3 LDSG-E regeln ebenso wie § 18 LDSG-E die **Untersuchungsbefugnisse** der oder des Landesbeauftragten für Datenschutz bzw. die damit einhergehenden Unterstützungspflichten der verantwortlichen Stellen.

Im Bundesdatenschutzgesetz sind die Regelungen hierzu in einem allgemeinen Teil für den Bereich der DSGVO und der JI-Richtlinie gemeinsam getroffen worden. Dies ist hier, wie für viele andere allgemeine Fragen, nicht der Fall. Es wäre **im Interesse einer einheitlichen Rechtssetzung und –anwendung wünschenswert, die Regelung in beiden Abschnitten gleichartig auszugestalten**. Dies ist bislang nicht der Fall. Die Regelungen in § 18 und § 64 haben zwar weitgehend denselben Regelungsgegenstand, jedoch **vollkommen unterschiedliche Formulierungen**. Sofern jeweils dasselbe gemeint ist, sollten hierfür auch dieselben Formulierungen gewählt werden.

35. Artikel 1 – § 68 LDSG-E: Ordnungswidrigkeiten

Die Aufnahme eines Ordnungswidrigkeitenstatbestands ist zu begrüßen (siehe oben Punkt 6).

36. Artikel 7 – § 30 Abs. 1 Nr. 1 SchulG-E

In § 30 Abs. 1 Nr. 1 SchulG-E fehlt die bisherige Regelung über Lichtbilder für Verwaltungszwecke. Nach dem geltenden § 30 Abs. 1 Satz 2 Nr. 1 und Satz 5 SchulG sind die Erhebung und Verarbeitung eines Lichtbildes nur mit schriftlicher Einwilligung der Eltern oder der volljährigen Schülerin oder des volljährigen Schülers zulässig. Diese Vorschrift wurde erst mit der Reform im Jahr 2014 eingefügt, weil die Praxis an großen Schulen gezeigt hat, „dass die Verfügbarkeit eines Lichtbildes insbesondere für Lehrkräfte mit z. B. nur zwei Stunden Unterricht in einer Klasse/Lerngruppe zur sicheren Zuordnung von Schülerinnen und Schülern erforderlich sein kann" (Gesetzentwurf der Landesregierung, Begründung zu § 30 Abs. 1 SchulG-E, LT-Drs. 18/1124, S. 33 f.). Zugleich hat der Gesetzgeber das Recht am eigenen Bild der Schülerinnen und Schüler berücksichtigt, indem „einerseits die Erhebung und Verarbeitung als zur Aufgabenerfüllung erforderlich benannt" und „diese andererseits abweichend von den sonst aufgezählten personenbezogenen Daten unter den Vorbehalt der schriftlichen Einwilligung der Eltern oder der volljährigen Schülerin bzw. des volljährigen Schülers" gestellt wurde.

Eine **Regelung über Lichtbilder fehlt im SchulG** nun vollständig. Dies lässt mehrere Auslegungen zu. Zum einen kann das Fehlen einer bereichsspezifischen Befugnis so verstanden werden, dass die Verarbeitung von Lichtbildern nicht (mehr) erlaubt sein soll. Zum anderen kann es auch so verstanden werden, dass für die Verarbeitung unmittelbar die Vorschriften der DSGVO anwendbar sein sollen.

Dies sollte im Interesse der Rechtssicherheit vorzugsweise im Gesetzestext unmittelbar geklärt werden, indem die Voraussetzungen für die Verarbeitung von Lichtbildern dort aufgenommen werden. Zumindest sollte jedoch eine Erläuterung in die Begründung aufgenommen werden, wie die künftige Regelung im Hinblick auf Lichtbilder zu verstehen ist.

Wichtig ist eine **Regelung auf der Ebene des Gesetzes** vor allem auch deshalb, weil in untergesetzlichen Vorschriften, namentlich in der Schul-Datenschutzverordnung die Anforderungen an die Verarbeitung von Lichtbildern konkretisiert werden. Diese Vorgaben sind **für die Praxis von erheblicher Bedeutung**. Es sollte daher Klarheit darüber hergestellt werden, dass auch der Umgang mit Lichtbildern noch von der Verordnungsermächtigung des § 30 Abs. 2 Satz 2 SchulG-E umfasst ist.

37. Notwendige Änderungen des IZG

Nach § 14 Satz 1 und 2 des **Informationszugangsgesetzes Schleswig-Holstein (IZG)** gilt: „Eine Person, die der Ansicht ist, dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass sie von einer informationspflichtigen Stelle eine unzulängliche Antwort erhalten hat, kann die oder den Landesbeauftragten für Datenschutz anrufen. Die Regelungen des Landesdatenschutzgesetzes über die Aufgaben und die Befugnisse der oder des Landesbeauftragten für Datenschutz finden entsprechend Anwendung."

Der bestehende Verweis ist insbesondere vor dem Hintergrund der Neufassung des LDSG **missverständlich**. Hier regen wir an, **eine Ergänzung zu den Aufgaben und Befugnissen der oder des Landesbeauftragten für Datenschutz im IZG aufzunehmen**. Als Vorbild kann wiederum Art. 3 des Anpassungsgesetzes Mecklenburg-Vorpommern (dortige LT-Drs. 7/1568, S. 21) dienen.