SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 20/989**
20. Wahlperiode 10.05.2023

Bericht

der Landesregierung –

Ministerium für Inneres, Kommunales, Wohnen und Sport

Bericht über die Evaluation des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

Inhalt

A. Vorbemerkung

Der europäische Gesetzgeber hat im Jahre 2016 das Datenschutzrecht grundlegend neu geordnet. So löste die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO) die bis dahin geltende Datenschutz-Richtlinie (Richtlinie 95/46/EG) durch eine in allen Mitgliedstaaten unmittelbar geltende Verordnung ab. Parallel wurde durch die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (sog. JI-Richtlinie) die Verarbeitung personenbezogener Daten durch Behörden zum Zweck der Strafverfolgung und -vollstreckung harmonisiert.

Beide Rechtsakte lösten in den Mitgliedsstaaten unmittelbare Handlungserfordernisse aus:

Die bis dahin geltenden Datenschutzgesetze des Bundes und der Länder, die der Umsetzung der Datenschutz-Richtlinie dienten, wurden mit dem Geltungsbeginn der unmittelbar geltenden DSGVO im Mai 2018 im Wesentlichen unanwendbar. Gleichzeitig enthält die DSGVO zahlreiche sog. Öffnungsklauseln. Diese geben dem nationalen Gesetzgeber Regelungsaufträge auf bzw. gestatten abweichende oder ergänzende eigene Regelungen. Letztlich war die JI-Richtlinie bis Mai 2018 in nationales Recht umzusetzen.

Der Schleswig-Holsteinische Landtag hat zu diesem Zweck das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 2. Mai 2018 (GVOBl. 2018, S. 161) beschlossen. Mit ihm wurde insbesondere das Landesdatenschutzgesetz (LDSG) neu erlassen. Daneben wurde bereichsspezifisches Datenschutzrecht in 36 Fachgesetzen angepasst.

Hierbei hat der Landesgesetzgeber auch eine Evaluierung vorgesehen (Artikel 40 des Gesetzes vom 2. Mai 2018). Evaluiert werden sollen alle betroffenen datenschutzrechtlichen Vorschriften, insbesondere die Regelungen der §§ 9, 33 Absatz 6 und 64 LDSG sowie § 1 Errichtungsgesetz ULD.

Zu beachten war, das sowohl die DSGVO selbst als auch das BDSG ihrerseits Evaluierungen vorsehen. Diese waren daher nicht Gegenstand der hiesigen Evaluierung. Allerdings sollten die von der Kommission bzw. dem Bundesministerium des Innern, für Bau und Heimat (BMI) durchgeführten Evaluierungen abgewartet werden, um die dortigen Erkenntnisse einbeziehen zu können.

Das für das Datenschutz-Anpassungsgesetz federführende Ministerium für Inneres, Kommunales, Wohnen und Sport hat mittels eines Fragebogens die Einschätzungen insbesondere der maßgeblichen Rechtsanwender gesammelt. Adressat des LDSG sind Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung (§ 2 Absatz 1 LDSG). Befragt wurden daher alle Ressorts inkl. zu- oder nachgeordneter sowie beaufsichtigter Bereiche, Landtagsverwaltung, Landesrechnungshof, das Unabhängige Landeszentrum für Datenschutz (ULD) und die kommunalen Landesverbände. Zusätzlich wurden die Digitale Wirtschaft Schleswig-Holstein (DiWiSH), die Industrie- und Handelskammer Schleswig-Holstein, die Handwerkskammer Schleswig-Holstein und die Vereinigung der Unternehmensverbände in Hamburg und Schleswig-Holstein e. V. (UVNord) befragt.

Der Fragebogen lautete in seiner umfassendsten Version:

I. Anwendungsbereich und Begriffsbestimmungen

1. Ist der Anwendungsbereich in § 2 LDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?
2. Ist der Anwendungsbereich in § 20 LDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?
3. Sind die Begriffsbestimmungen in § 21 LDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

II. Besondere Verarbeitungssituationen

Sind die Regelungen in Bezug auf besondere Verarbeitungssituationen in den §§ 12 bis 16 und §§ 26 bis 31 LDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

III. Betroffenenrechte

1. Sind die Regelungen zu den Betroffenenrechten in den §§ 8 bis 11 LDSG, insbesondere die Beschränkung der Auskunftspflicht in § 9, aus Ihrer Sicht sachgerecht, praktikabel und normenklar?
2. Sind die Regelungen zu den Betroffenenrechten in den §§ 33 bis 37 LDSG, insbesondere die Beschränkung der Auskunftspflicht in § 33 Absatz 6, aus Ihrer Sicht sachgerecht, praktikabel und normenklar?
3. In wie vielen Fällen haben die Regelungen der §§ 8 und 9 bzw. § 33 Absatz 4-6 LDSG Anwendung gefunden (sofern statistisch erfasst, ansonsten wird um Angabe einer Größenordnung gebeten)?

IV. Aufsichtsbehörde

1. Sind die Aufgaben und Befugnisse der Aufsichtsbehörde in §§ 17, 18 und 64 LDSG sachgerecht, praktikabel und normenklar geregelt?
2. Ist die Rechtsform des ULD als rechtsfähige Anstalt des öffentlichen Rechts, auf die die §§ 50-52 LVwG nicht anzuwenden sind, sachgerecht gewählt und ausgestaltet?
3. Haben sich die Regelungen zum Amtsverhältnis – insbesondere die Ausgestaltung dessen Endes in § 6 Absatz 2 Errichtungsgesetz ULD – bewährt, auch im Hinblick auf eine etwaige Konkurrentenklage bei der (Neu-)Besetzung des Amtes?
4. Wie bewerten Sie das Errichtungsgesetz ULD insgesamt in Bezug auf die Sachgerechtheit, Praktikabilität und Normenklarheit der Bestimmungen?
5. Gibt es aus Ihrer Sicht anderweitige Anpassungsbedarfe im Hinblick auf das Errichtungsgesetz ULD?

V. Allgemein

1. Wie bewerten Sie das LDSG insgesamt in Bezug auf die Sachgerechtheit, Praktikabilität und Normenklarheit der Bestimmungen?
2. Bestehen in Ihrer datenschutzrechtlichen Praxis Schwierigkeiten mit der Auslegung und Anwendung des LDSG? Wenn ja, welche Schwierigkeiten sind das und auf welche Regelungen des LDSG beziehen sie sich?

3. Gibt es aus Ihrer Sicht Anpassungsbedarfe in Fachgesetzen, die aus dem Zusammenspiel von LDSG und bereichsspezifischem Datenschutzrecht herrühren? Wenn ja, welche?

Die speziellen Fragen zur Ausgestaltung der Aufsichtsbehörde (IV. 2.-5.) wurden wegen der nur dort bestehenden Betroffenheit lediglich an das ULD und die Staatskanzlei gerichtet.

Es sind Rückmeldungen von allen obersten Landesbehörden, dem ULD, der ARGE KLV sowie gesondert zwei Städten, einem Kreis und einem Amt sowie der Handwerkskammer Schleswig-Holstein und dem Universitätsklinikum Schleswig-Holstein eingegangen. Aus dem Hochschulbereich gab es Rückmeldungen der Fachhochschule Kiel, der Universität zu Lübeck, der Technischen Hochschule Lübeck und der Christian-Albrechts-Universität zu Kiel.

Die Antworten konzentrieren sich im Wesentlichen auf die im Fragebogen abgefragten Aspekte der Sachgerechtheit, Praktikabilität und Normenklarheit. Insbesondere auf die offenen Fragen IV. 2. und 3. wurden jedoch auch Änderungsvorschläge unterbreitet, die sowohl inhaltlicher Natur sind als auch die Normenklarheit betreffen.

Im nachstehenden Bericht werden die wesentlichen Rückmeldungen dargestellt und zu ihnen bewertend Stellung genommen. Sofern ein Handlungserfordernis gesehen wird und verschiedene Handlungsoptionen bestehen, wird ein Votum für die aus Sicht der Landesregierung vorzugswürdige Lösung abgegeben. Nicht behandelt werden rein redaktionelle Anmerkungen, die nicht über sprachliche Änderungen hinausgehen; diese werden allerdings bei einer etwaigen Gesetzesänderung berücksichtigt werden.

B. Zusammenfassung der wesentlichen Ergebnisse und Schlussfolgerungen

Die durchgeführte Evaluierung hat gezeigt, dass die Regelungen des Landesdatenschutzgesetzes von Rechtsanwendern und Aufsichtsbehörde ganz überwiegend als sachgerecht, praktikabel und normenklar angesehen werden. Schwierigkeiten in der Rechtsanwendung resultieren vornehmlich aus dem „unübersichtlichen“ Regelungsgefüge des Rechtsgebiets mit unterschiedlichen Rechtsquellen auf europäischer,

Bundes- und Landesebene sowie dem Nebeneinander von allgemeinem und bereichsspezifischem Recht. Diese Probleme lassen sich (mit Ausnahme einer Klarstellung in § 2 Absatz 6 LDSG) nicht durch Änderungen des Landesdatenschutzgesetzes abstellen. Die Landesregierung wird insoweit die Veröffentlichung einer Handreichung für öffentliche Stellen prüfen.

Weiter zu beobachten sind derzeit laufende Entwicklungen auf europäischer Ebene, die nach Abschluss ggf. im Landesrecht nachzuvollziehen sein werden. Die betrifft vor allem die Fragen der Anwendbarkeit der DSGVO auf den Landtag (siehe unter I. 1. c) und der Umsetzung der JI-Richtlinie (siehe unter IV. 1. c) (i)).

Defizite wurden hinsichtlich des Beschäftigtendatenschutzes gemeldet, der in § 15 LDSG nur knapp geregelt ist. Hier sollte eine Anpassung erfolgen, die auch die anstehenden Entwicklungen auf Bundesebene berücksichtigen sollte (siehe unter II. b)).

Der europäische Gesetzgeber hat im Zuge der Neuordnung des Datenschutzrechts durch DSGVO und JI-Richtlinie die Rechte der betroffenen Personen in den Mittelpunkt gestellt. Insofern hat die Evaluierung gezeigt, dass die landesrechtlichen Anpassungen und Umsetzungen keinen grundlegenden Bedenken begegnen und keine zwingenden Änderungsbedarfe zu verzeichnen sind.

Einige der Änderungsvorschläge werden weiter geprüft werden. Im Einzelnen sind dies:

- die Ausweitung der Regelung des § 9 Absatz 3 Satz 5 LDSG, wonach die die Information der betroffenen Person durch die oder den Landesbeauftragten Rückschlüsse auf die Inhalte zulassen darf, auch auf andere Auskunftsverfahren (siehe unter IV. 1. b));
- der Bedarf für den Erlass einer Landesverordnung nach § 7 Absatz 2 bzw. § 40 Absatz 5 LDSG (siehe unter V.1.g));
- eine Regelung der Verschwiegenheitspflicht von Datenschutzbeauftragten öffentlicher Stellen (siehe unter V.1.h));
- das Erfordernis für die Schaffung einer Rechtsgrundlage für die Veröffentlichung von sog. Funktionsträgerdaten (siehe unter V.2.a))
- die Aufnahme einer Vertretungsregelung bei längerer Verhinderung der oder des Landesbeauftragten für Datenschutz (siehe unter IV. 3.).

Letztlich sind im Zuge einer Gesetzesänderung einige redaktionelle Anpassungen vorzunehmen.

C. Die Ergebnisse des Berichts im Einzelnen

Nachstehend werden die Rückmeldungen zu den Einzelnen Fragen und die jeweilige Bewertung durch das MIKWS dargestellt.

I. Anwendungsbereich und Begriffsbestimmungen

Im ersten Block wurden die Rechtsanwender nach ihren Erfahrungen mit den Regelungen zum Anwendungsbereich des LDSG bzw. seiner Abschnitte 2 und 3 sowie zu Begriffsbestimmungen befragt.

1. Anwendungsbereiche von LDSG und Fachrecht

a) Abgrenzung LDSG/Fachgesetze

Einige wenige Rückmeldungen sind auf die Frage eingegangen, wann das LDSG Anwendung findet, und wann andere Rechtsquellen. Teilweise wird insoweit eine Anpassung des LDSG angeregt.

Tatsächlich ist das Recht zum Schutz personenbezogener Daten einigermaßen fragmentiert. Denn die Regelungskompetenzen im Datenschutzrecht liegen sowohl beim EU-Gesetzgeber als auch bei den Bundes- und den Landesgesetzgebern, die auch alle von ihren Kompetenzen Gebrauch gemacht haben, da das Grundgesetz keine spezifische Gesetzgebungskompetenz für das Datenschutzrecht enthält. Das durch den Bundesgesetzgeber geregelte Datenschutzrecht ist nach ständiger Rechtsprechung des Bundesverfassungsgerichts ein Anwendungsfall der Bundeskompetenz kraft Sachzusammenhangs, wenn der Bund eine ihm zur Gesetzgebung zugewiesene Materie verständigerweise nicht regeln kann, ohne dass die datenschutzrechtlichen Bestimmungen mitgeregelt werden (BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260 ff.).

Der Bundesgesetzgeber ist aufgrund seiner Gesetzgebungsbefugnis für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nr. 11 Grundgesetz) für Regelungen über den Datenschutz im nicht-öffentlichen Bereich zuständig. Auch bei öffentlich-rechtlichen Rechtsmaterien, für die dem Bundesgesetzgeber eine Gesetzgebungskompetenz zusteht

(bspw. im Steuerrecht oder im Pass- und Meldewesen sowie in weiteren Bundesgesetzen) sind datenschutzrechtliche Regelungen enthalten.

Dort, wo der Bundesgesetzgeber keine ausschließliche Gesetzgebungskompetenz (vgl. Artikel 73 Absatz 1 GG) besitzt oder im Rahmen der konkurrierenden Gesetzgebungskompetenz (vgl. Artikel 74 Absatz 1 GG), sind die Bundesländer für die Regelungen zum Datenschutz verantwortlich.

Die grundlegenden Vorgaben werden daher durch die DSGVO gemacht, die als europarechtliche Verordnung unmittelbar geltendes Recht ist (s. auch Vorbemerkung). Soweit der Bund von den Möglichkeiten der DSGVO zu Abweichungen oder Ergänzungen Gebrauch gemacht hat, ist dies im BDSG erfolgt. Das BDSG gilt ausweislich seines § 1 Absatz 1 für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes sowie für öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist.

Das Land Schleswig-Holstein hat den Datenschutz für seine öffentlichen Stellen jedoch durch das LDSG geregelt, sodass für diese das LDSG und nicht das BDSG Anwendung findet.

Das LDSG wiederum wird als allgemeines Gesetz von spezielleren landesrechtlichen Vorschriften, die in Fachgesetzen den Datenschutz bereichsspezifisch regeln, verdrängt (Grundsatz des Vorrangs des lex specialis).

Eine Änderung des LDSG erscheint daher innerhalb dieses Regelungsgefüges nicht als geeignet, etwaige Unklarheiten zu bereinigen.

b) § 2 Absatz 2 Satz 2 LDSG

Nach § 2 Absatz 2 Satz 2 LDSG unterfällt die Datenverarbeitung der Gerichte im Rahmen ihrer justiziellen Tätigkeit nicht der Aufsicht des ULD. Diese Beschränkung sei nach Auffassung des ULD europarechtlich, und, soweit die richterliche Unabhängigkeit betroffen ist, auch verfassungsrechtlich geboten. Gleichwohl erhalte das ULD immer wieder Beschwerden von Bürgerinnen und Bürgern, die Verarbeitungen in diesem Bereich zum Gegenstand haben. Im Jahr 2019 seien es 7, im Jahr 2020 4 und im Jahr 2021 bislang 5 Beschwerden gewesen. Für diese Verarbeitungen gelte zwar

das Datenschutzrecht in vollem Umfang, doch die von der DSGVO vorgesehene unabhängige Kontrolle über die Datenverarbeitung gäbe es in Schleswig-Holstein nicht. Die betroffenen Personen könnten ihr Beschwerderecht nach Artikel 77 DSGVO in diesem Bereich faktisch nicht ausüben. Hierüber habe das ULD auch im 39. Tätigkeitsbericht unter der Ziffer 4.3.5 („Beschwerden über justizielle Tätigkeiten gehen ins Leere“) berichtet.

Hinzu komme, dass der Begriff der justiziellen Tätigkeit nicht klar definiert sei. Es sei in der Anwendung des Gesetzes unklar, ob die Ausnahme nur für Verarbeitungen gelte, die in richterlicher Unabhängigkeit durchgeführt werden, oder ob der Begriff der justiziellen Tätigkeit weiter zu verstehen sei.

Die DSGVO habe für diesen Bereich, der einer Aufsicht durch eine Exekutivbehörde nicht zugänglich ist, in Erwägungsgrund 20 vorgesehen, dass besondere Stellen im Justizsystem mit der Aufsicht betraut werden. Hiervon habe Schleswig-Holstein bislang keinen Gebrauch gemacht. Es wird dringend dazu geraten, die Aufgabe der Aufsicht in der Justiz einer Stelle zuzuweisen, ähnlich wie es im Landtag schon seit Jahrzehnten praktiziert werde. Dies würde auch die Auslegungsfrage des Begriffs der justiziellen Tätigkeit entschärfen, da es dann nicht mehr darum ginge, ob eine Kontrolle überhaupt stattfindet, sondern nur um die Frage, welche Stelle die Kontrolle ausübt.

Bewertung:

Zur Frage der Aufsicht ist darauf hinzuweisen, dass sich die Zuständigkeit der Aufsichtsbehörden nach Erwägungsgrund 20 der DSGVO nicht auf „die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit“ erstrecken soll. Diese Ausnahme ist erfolgt, „damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt“. Die Landesregierung beabsichtigt nach wie vor nicht, von der in Erwägungsgrund 20 erwähnten Möglichkeit Gebrauch zu machen, stattdessen „besondere Stellen im Justizsystem“ mit der Aufsicht über Datenverarbeitungsvorgänge zu betrauen. Denn für den Schutz der richterlichen Unabhängigkeit nach Artikel 92 GG spielt es keine Rolle, ob Eingriffe durch Akteure von außerhalb oder innerhalb des Justizsystems erfolgen. Es ist ein unabänderbarer Grundsatz unseres Staatswesens, dass die Rechtsprechung ausschließlich an Gesetz und Recht gebunden ist und eben nicht an die Weisungen fachlich vorgesetzter Stellen.

Eine Überprüfung von gerichtlichen Entscheidungen erfolgt nach der Konzeption des Grundgesetzes vielmehr allein durch andere, ebenfalls durch Artikel 92 GG geschützte Richterinnen und Richter – in der Regel im Instanzenzug im Rahmen von Rechtsbehelfsverfahren. Dies gilt nicht nur für die verfahrensabschließende Sachentscheidung, sondern ebenso für das zur Entscheidungsfindung durchzuführende Verfahren. Bei einer Einrichtung besonderer Stellen für die Datenschutzaufsicht würde daher die Unabhängigkeit der Justiz nicht „unangetastet“ bleiben, wie es übrigens nicht nur Erwägungsgrund 20 beabsichtigt, sondern auch Artikel 47 Absatz 2 EU-Grundrechtecharta und Artikel 6 Absatz 1 EMRK. Aus diesen Gründen sind – soweit hier bekannt – derartige Stellen bislang weder vom Bund noch von einem der anderen Länder eingerichtet worden.

Um die Zuständigkeit der Aufsichtsbehörden zu begrenzen, verwendet § 2 Absatz 2 Satz 2 LDSG den Begriff der „justiziellen Tätigkeit“ der Gerichte. Dieser Begriff ist wörtlich aus Erwägungsgrund 20 übernommen worden und gibt damit den Willen des EU-Gesetzgebers möglichst unverfälscht wieder. Dass die Einführung neuer Terminologie in der DSGVO mitunter zu Unklarheiten führt, stellt keine Besonderheit dieses Erwägungsgrundes dar und ist vom EU-Gesetzgeber so hingenommen worden. Aus hiesiger Sicht wäre es dagegen verfehlt, aus Vereinfachungsgründen europarechtliche Begriffe kurzerhand mit ähnlich erscheinenden Begriffen des nationalen Rechts gleichzusetzen, die zwar durch jahrzehntelange Anwendung vertraut sein mögen, aber letztlich doch einen anderen Inhalt haben.

Nach hiesigem Verständnis geht der Begriff der „justiziellen Tätigkeit“ der Gerichte über den im deutschen Recht gängigen Begriff der richterlichen Unabhängigkeit hinaus, der sich nur auf die einzelne Richterin und den einzelnen Richter bezieht. Diese personengebundene Eingrenzung wird in Erwägungsgrund 20 mit seinen unpersönlichen Ausdrücken wie „Justiz“, „gerichtlich“ und „justiziell“ gerade vermieden. Stattdessen wird dort die Institution insgesamt in den Blick genommen und nicht nur die Richterschaft. Beispielsweise erstreckt sich die richterliche Unabhängigkeit nach Artikel 92 GG nicht auch auf die vielen an den Gerichten tätigen hochqualifizierten Rechtspflegerinnen und Rechtspfleger, die etwa Kostenentscheidungen treffen oder Erbscheine erteilen. Einfachgesetzlich ist aber auch ihnen in § 9 RPflG die sachliche Unabhängigkeit garantiert, da sie historisch Aufgaben übernommen haben, die vormals Richterinnen und Richtern oblagen. Auch sie führen daher „justizielle Tätigkeiten“ aus.

Von dem Begriff der „justiziellen Tätigkeit“ werden nach dem Verständnis der Landesregierung auch solche Tätigkeiten der Gerichte umfasst, die zwar selbst nicht der richterlichen Unabhängigkeit unterfallen, bei denen Eingriffe von außen aber die richterliche Unabhängigkeit berühren könnten. So ist beispielsweise die Verfügung einer Richterin oder eines Richters, in einem konkreten Verfahren eine bestimmte Zustellung auszuführen, von der richterlichen Unabhängigkeit umfasst; die Ausführung dieser Verfügung durch die Geschäftsstelle ist es dagegen nicht. Unterläge diese Geschäftsstellentätigkeit einer externen Datenschutzaufsicht, könnte dadurch die richterliche Aufgabenerfüllen mittelbar gelenkt und dadurch in die richterliche Unabhängigkeit eingegriffen werden. Auch solche Tätigkeiten von nichtrichterlichen Mitarbeiterinnen und Mitarbeitern des Gerichts, die der Durchführung einzelner Verfahren dienen, sind daher als „justiziell“ anzusehen, damit – in den Worten des Erwägungsgrundes 20 – „die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt“.

c) § 2 Absatz 3 Satz 1

Nach § 2 Absatz 3 Satz 1 unterliegen der Landtag, seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie die Landtagsverwaltung nicht den Bestimmungen des LDSG, soweit sie in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten.

Mit dem Urteil vom 09.07.2020 hat der Europäische Gerichtshof (EuGH) auf ein Vorabentscheidungsersuchen des Verwaltungsgerichts Wiesbaden festgestellt, dass der Petitionsausschuss des Hessischen Landtages „insoweit, als dieser Ausschuss allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als ‚Verantwortlicher‘ im Sinne von Art. 4 Nr. 7 der Verordnung 2016/679 einzustufen“ ist (Rs. C-272/19), er also dem Anwendungsbereich der DSGVO unterfällt. Damit nimmt der EuGH die gegenteilige Position zur bislang herrschenden datenschutzrechtlichen Meinung ein, die auch von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vertreten wurde, und die der Auffassung ist, dass die parlamentarisch-legislativen Tätigkeiten der Mitgliedstaaten nicht in den Anwendungsbereich des Gemeinschaftsrechts und damit auch nicht der DSGVO fallen.

Die Auswirkungen des Urteils und seine Übertragbarkeit auf andere parlamentarische Bereiche werden in der datenschutzrechtlichen Literatur noch diskutiert (vgl. etwa Roßnagel/Rost: Ist die Datenschutz-Grundverordnung auch in den Landtagen anwendbar?, NVwZ 2021, 1641). Insbesondere ist noch als offen zu bezeichnen, ob das Urteil aufgrund ihrer besonderen Natur und Aufgaben nur für Petitionsausschüsse gelten soll oder ob es sich auf die Verarbeitung personenbezogener Daten durch Parlamente in Gänze erstreckt, worauf der Hinweis des EuGH hindeuten könne, in der DSGVO sei „keine Ausnahme in Bezug auf parlamentarische Tätigkeiten vorgesehen“.

Der EuGH wird aufgrund eines Vorabentscheidungsersuchens des österreichischen Verwaltungsgerichtshofs (Rechtssache C-33/22) Gelegenheit haben, sich dazu zu äußern, ob parlamentarische Untersuchungsausschüsse eines Mitgliedstaats dem Anwendungsbereich der DSGVO unterfallen.

Die weitere Diskussion der Frage wird durch die Landesregierung beobachtet. Ein unmittelbarer Änderungsbedarf des LDSG resultiert aus dem Urteil jedoch nicht. Denn durch § 2 Absatz 3 Satz 1 wird der Landtag lediglich von der Anwendung des LDSG ausgenommen. Das LDSG verhält sich hingegen nicht zur Frage der Anwendbarkeit der DSGVO. Das könnte es aufgrund des Geltungsvorrangs der unmittelbar geltenden EU-Verordnung auch nicht. Das LDSG schöpft lediglich die von der DSGVO eröffneten Handlungsspielräume aus und regelt dabei teilweise Erleichterungen für öffentliche Stellen. Sollte die weitergehende datenschutzrechtliche Diskussion und Rechtsprechung zu dem Ergebnis kommen, dass jegliche parlamentarische Tätigkeit der DSGVO unterworfen ist, würde diese eben unverändert gelten. Etwaig für erforderlich erachtete Anpassungen wären dann in der gem. § 2 Absatz 3 Satz 2 vom Landtag unter Berücksichtigung seiner verfassungsrechtlichen Stellung sowie der Grundsätze der DSGVO und des LDSG zu beschließenden Datenschutzordnung zu regeln.

d) § 2 Absatz 6

Weitere Stellungnahmen sind speziell zu § 2 Absatz 6 LDSG eingegangen. Nach dieser Regelung sind die Vorschriften der DSGVO auch dann entsprechend anzuwen-

den, wenn die Verarbeitung personenbezogener Daten nicht in den Anwendungsbereich der Verordnung DSGVO oder der JI-Richtlinie fällt, es sei denn, dieses Gesetz oder andere spezielle Rechtsvorschriften enthalten abweichende Regelungen.

Insbesondere im Hinblick auf die DSGVO sind hier Unklarheiten rückgemeldet worden. Denn nach Artikel 2 Absatz 1 gilt die DSGVO „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“. Diese Vorschrift bestimmt den sachlichen Anwendungsbereich der DSGVO sehr weit, denn nach der Begriffsbestimmung in Artikel 4 Nr. 6 ist ein „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. Daher fällt auch die in der Verwaltung noch vorzufindende Papierakte in den Anwendungsbereich der DSGVO. Ausgenommen ist im Wesentlichen lediglich die nicht-automatisierte Verarbeitung, bei der nicht in einem strukturierten System gespeichert wird.

Nach Artikel 2 Absatz 2 findet die DSGVO ferner keine Anwendung auf die Verarbeitung personenbezogener Daten a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt, b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen, c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (sog. Haushaltsausnahme), d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

Die Unklarheiten bestehen daher in der Frage, was genau mit dem Anwendungsbefehl des § 2 Absatz 6 LDSG bezweckt wird: Soll die DSGVO auch bei der nichtautomatisierten Verarbeitung ohne Speicherung in einem Dateisystem Anwendung finden (also der Ausschluss aus dem Anwendungsbereich nach Artikel 2 Absatz 1 aufgehoben werden), soll die DSGVO auch in den nach Artikel 2 Absatz 2 ausgenommenen Bereichen entsprechend angewendet werden oder sind beide Fälle gemeint?

Bewertung:

Die gesetzliche Regelung sollte klargestellt werden.

Der Wortlaut der Norm lässt alle drei vorgenannten Auslegungen zu.

Ausweislich der Gesetzesbegründung (LT-Drs. 19/429, S. 131) wurde die entsprechende Anwendbarkeit angeordnet, da DSGVO sowie JI-Richtlinie „aufgrund der begrenzten Regelungskompetenz der Europäischen Union nicht für alle Bereiche der Landesverwaltung Geltung haben können“. Der historische Wille des Gesetzgebers spricht daher dafür, dass in § 2 Absatz 6 LDSG jedenfalls der Ausschluss der Anwendbarkeit aus Artikel 2 Absatz 2 DSGVO aufgehoben werden soll.

Hinsichtlich der nichtautomatisierten Verarbeitung ist die Lage weniger eindeutig. So ist die DSGVO – ihrem eigenen Anwendungsbereich entsprechend und diesen voraussetzend – deutlich darauf zugeschnitten, dass die Rechte und Freiheiten betroffener Personen vor den Gefahren geschützt werden sollen, die insbesondere aus der automatisierten Verarbeitung herrühren, aber auch aus der Speicherung in einem Dateisystem, in dem personenbezogene Daten vergleichsweise einfach ausgelesen, verknüpft und bspw. zu anderen Zwecken weiterverarbeitet werden können. Die Risikobewertung des EU-Gesetzgebers kommt durch den Anwendungsbereich der DSGVO, wie er eben normiert wurde, zum Ausdruck: Das Risiko ist bei der automatisierten Verarbeitung höher als bei der der nichtautomatisierten. Insofern ist zu hinterfragen, ob die Ausweitung der Anwendbarkeit DSGVO auf Bereiche, in denen der EU-Gesetzgeber selbst sie gar nicht angewandt wissen wollte, sinnvoll ist.

Allerdings ist zu berücksichtigen, dass das LDSG in der Fassung vor Inkrafttreten der DSGVO nicht zwischen der automatisierten und der nichtautomatisierten Datenverarbeitung ohne Speicherung in einem Dateisystem unterschieden hat. Die durch das LDSG a.F. vermittelten Betroffenenrechte galten ausnahmslos für jede Verarbeitung. Das wäre nicht der Fall, sollte der Geltungsbereich der DSGVO „1:1“ übertragen werden, da die Rechte der Betroffenen nunmehr unmittelbar aus der DSGVO erwachsen und diese eben im nichtautomatisierten Bereich nicht per se gilt. Die Ausweitung des Grundrechtsschutzes auch auf die nichtautomatisierte Verarbeitung spräche für einen weiten Anwendungsbereich.

Gleichwohl ist zu konstatieren, dass der Unterschied in der Praxis eher gering sein dürfte. Denn die öffentlichen Stellen, für die das LDSG gilt, werden mittlerweile entweder ohnehin überwiegend automatisiert arbeiten oder jedenfalls – auch bei nichtautomatisierter Datenverarbeitung – ihre Daten in einer geordneten Aktenstruktur gemäß Aktenordnung und damit in einem „Dateisystem“ im Sinne des Artikels 4 Nr. 6

DSGVO speichern. Die DSGVO findet dann ohnehin bereits unmittelbar Anwendung, nicht erst über den Befehl des § 2 Absatz 6 LDSG. Lediglich in Fällen, in denen nicht digital verarbeitet und nicht strukturiert gespeichert wird (bspw. Prüfung von 3G-Nachweisen durch bloße Einsicht ohne Speicherung, Sammeln von Visitenkarten oder Notiz einer Telefonnummer in einem handschriftlichen Gesprächsvermerk), bestünde derzeit eine Lücke, die durch den Anwendungsbefehl im LDSG geschlossen wird.

Jedenfalls müssten Rückausnahmen vorgehsehen werden, durch die die Geltung derjenigen Vorschriften der DSGVO abbedungen werden, die für die nichtautomatisierte Verarbeitung ohne Speicherung in einem Dateisystem zu nicht sachgerechten Ergebnissen kommen (da sie hierfür eben nicht konzipiert sind, s.o.). Alle acht Länder, die ausdrückliche Regelungen zur Anwendbarkeit der DSGVO im nichtautomatisierten Bereich in ihren Landesdatenschutzgesetzen haben, sind so vorgegangen.

e) § 2 Absatz 7 LDSG

Für die Verfassungsschutzbehörde des Landes Schleswig-Holstein gelten nach § 2 Absatz 7 LDSG neben dem Landesverfassungsschutzgesetz nur ausgewählte Vorschriften des LDSG (Nr. 1) und des BDSG (Nr. 2). Das ULD merkt an, dass von der getroffenen Auswahl nicht alle Regelungen des allgemeinen Datenschutzrechts umfasst seien. Es fehlten insbesondere Aufgabenzuweisungen für die Datenschutzaufsichtsbehörde (da § 62 LDSG, § 14 BDSG oder Artikel 57 DSGVO nicht anwendbar seien) und das Beschwerderecht betroffener Personen (da § 36 LDSG, § 60 BDSG oder Artikel 77 DSGVO nicht anwendbar seien).

Bewertung:

Der Hinweis des ULD ist insoweit zutreffend, als § 2 Absatz 2 LDSG ausdrücklich nur einige Bereiche des allgemeinen Datenschutzrechts aus dem LDSG und dem BDSG für anwendbar erklärt. Daraus folgt zwangsläufig, dass diese Auswahl nicht alle Regelungen des allgemeinen Datenschutzrechts umfasst. Ein konkreter Änderungsbedarf an § 2 Absatz 7 LDSG lässt sich hieraus jedoch nicht ableiten. Denn durch § 2 Absatz 7 LDSG wird gerade sichergestellt, dass insbesondere die Betroffenenrechte nicht beschnitten werden. Dies wird nach Auffassung der Landesregierung durch § 25 Absatz 4 Landesverfassungsschutzgesetz garantiert, nach dem Betroffene auf die

Möglichkeit, sich an das ULD zu wenden, hinzuweisen sind. In Verbindung mit der auch auf die Verfassungsschutzbehörde anzuwendende Regelung des § 17 LDSG, der die Aufgabenbeschreibung und Befugnisse des ULD definiert, sowie der angeordneten entsprechenden Anwendbarkeit von § 16 Absatz 2 BDSG mit den dort geregelten Befugnissen, ist kein zwingender Änderungsbedarf erkennbar. In der Praxis ist zudem festzustellen, dass einer Beschwerde beim ULD bislang stets ein Auskunftsersuchen vorangegangen ist, was zur Wahrung der Rechte der Betroffenen beiträgt. Auch die Zusammenarbeit mit dem ULD hat sich bewährt und lässt keine Regelungslücke erkennen. Insgesamt hält die Landesregierung eine Änderung von § 2 Absatz 7 LDSG aufgrund der Berücksichtigung der Betroffenenrechte in § 25 LVerfSchG und der Aufgabenbeschreibungen und Befugnisse des ULD aus § 17 LDSG und der analogen Anwendung von § 16 Absatz 2 BDSG nicht für erforderlich. Erwogen werden könnte allenfalls die Ergänzung eines klarstellenden Satzes in § 2 Absatz 7 LDSG, wonach die oder der Landesbeauftragte für Datenschutz zuständige Aufsichtsbehörde für die Verfassungsschutzbehörde des Landes ist.

2. Abgrenzung §§ 2/20

Innerhalb des LDSG bereitet die Abgrenzung zwischen dem zweiten und dritten Abschnitt des Gesetzes den Rechtsanwendern teilweise Schwierigkeiten. So würde aufgrund der in § 2 gewählten Formulierung zunächst das gesamte LDSG für öffentliche Stellen als anwendbar erklärt. Erst in § 20 erfolge dann die Einschränkung, dass die nachfolgenden Bestimmungen nur für einen Teil der öffentlichen Verwaltung gelten.

Bei ausschließlicher Lektüre des § 2 Absatz 1 LDSG kann dieses Missverständnis entstehen. Allerdings ergibt sich aus der Überschrift des 2. Abschnitts, dass dieser die Durchführungsbestimmungen für Verarbeitungen im Anwendungsbereich der unmittelbar anwendbaren DSGVO enthält. Ebenso weist die Überschrift des 3. Abschnitts darauf hin, dass dort Verarbeitungen zu Zwecken der JI-Richtlinie geregelt sind. § 20 Absatz 1 beginnt sodann mit Worten „Die Vorschriften dieses Abschnitts gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten.“ Die Regelungen der 2. und 3. Abschnitts ergänzen ei-

nander also nicht oder bauen aufeinander auf, sondern stehen für verschiedene Anwendungsbereiche nebeneinander. Sie könnten gar, wie ebenfalls angeregt wurde, in zwei unterschiedliche Gesetze ausgegliedert werden (etwa ein Landesdatenschutzgesetz mit ergänzenden Regelungen zur DSGVO und ein „Gesetz über die Datenverarbeitung der Polizei und der Justiz“ zur Umsetzung der JI-Richtlinie).

Nach Auffassung der Landesregierung ist gleichwohl auch bei der vorliegenden Regelung innerhalb eines Gesetzes hinreichend deutlich, welche Regelungen Anwendung auf welche Verarbeitungssituationen finden. Eine Gesetzänderung erscheint nicht als zwingend erforderlich. Es wird jedoch geprüft, ob als Handreichung für die Rechtsanwender ein Hinweisblatt, etwa in Form eines Fließdiagramms, veröffentlicht werden kann, in dem sich die Anwendungsbereiche der Normen nochmals klargestellt werden.

Ohnehin schwieriger dürfte in der Praxis die materielle Abgrenzung sein, welches Rechtsregime (DSGVO oder nationales Recht in Umsetzung der JI-Richtlinie) anzuwenden ist. Dies betrifft die Frage, ob die vorstehende Definition des § 20 Absatz 1 Satz 1 LDSG erfüllt ist. Denn wenn die Verarbeitung personenbezogener Daten nicht dem Zweck der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten dient, sondern dem Verwaltungsbereich zuzuordnen ist, ist auch bei den hierfür zuständigen öffentlichen Stellen, wie etwa der Polizei oder Staatsanwaltschaften, die DSGVO anzuwenden.

Als Hintergrund dieser Abgrenzungsproblematik wird angeführt, dass sich der datenschutzrechtliche Begriff der „Straftat“ an der unionsrechtlichen Auslegung orientiere und somit nicht zwangsläufig deckungsgleich mit dem nationalen Verständnis des Begriffs sei.

Die Kritik kann nur teilweise nachvollzogen werden. Bei dem Begriff der Straftat im Sinne der JI-Richtlinie handelt es sich um einen eigenständigen Begriff des Unionsrechts (Erwägungsgrund 13 zur Richtlinie (EU) 2016/680), der gleichwohl unter Berücksichtigung der unterschiedlichen Rechtstraditionen der Mitgliedstaaten zu bestimmen ist. Der Gesetzgeber hat mit dem Verweis auf Straftaten und Ordnungswidrigkeiten den Anwendungsbereich des 3. Abschnitts des LDSG insoweit abschließend und klar geregelt. Bei Straftaten und Ordnungswidrigkeiten handelt es sich um feststehende Rechtsbegriffe, die im jeweiligen Fachrecht legaldefiniert sind (§ 11 Absatz 1 Nr. 5 StGB, § 1 OWiG).

Nach Auffassung der Landesregierung handelt es sich daher um praktische Subsumtionsprobleme, die durch eine Rechtsänderung im LDSG nicht behoben werden können. So wird auch aus dem Polizeibereich gemeldet, dass anfänglich durchaus Probleme bei der Schnittstelle zwischen DSGVO und JI-Richtlinie gesehen worden seien. Nachdem ausreichende Erfahrungen mit der mittlerweile seit 2018 geltenden Rechtslage gesammelt wurden, bestünden diese Probleme jedoch nicht mehr. Im Übrigen wären es ansonsten auch möglich, die Beratung des ULD nach Artikel 57 Abs. 1 Buchst. c DSGVO in Anspruch zu nehmen.

3. § 21

Zu den in § 21 LDSG niedergelegten Begriffsbestimmungen sind nur uneinheitliche Rückmeldungen eingegangen. Einerseits werden diese als vollständig und detailliert gelobt. Anderseits werden jedoch auch Unklarheiten kritisiert.

Soweit eine Rückmeldung aus Gründen besserer Rechtsklarheit für wünschenswert erachtet, wenn in § 21 Nr. 2 auch die dort genannten Verarbeitungsvorgänge (also etwa Erfassen, Speicherung, Löschen usw.) näher definiert würden, wird dies nicht für erforderlich erachtet. Es handelt sich um Begriffe, die auch in der DSGVO Verwendung finden und durch Rechtsprechung, Kommentierung und weitere datenschutzrechtliche Literatur hinreichend konkretisiert sind.

Aus dem Bereich der Justiz wird moniert, dass die in § 21 LDSG bzw. § 46 BDSG normierten Begriffsbestimmungen überwiegend unscharf blieben, weshalb in der (Strafverfolgungs-)Praxis insbesondere Schwierigkeiten bezüglich der Abgrenzung zwischen personenbezogenen Daten und Verfahrensdaten sowie hinsichtlich der Definition der besonderen Kategorien von personenbezogenen Daten zu verzeichnen seien. Diesbezüglich wird beispielsweise auf die Frage verwiesen, ob bereits ein ohne weitere Angaben benanntes Aktenzeichen ein personenbezogenes Datum darstelle, sowie auf die Frage, ob der Geburtsort einer Person stets als besonderes personenbezogenes Datum zu qualifizieren sei, weil hieraus gegebenenfalls Rückschlüsse auf die rassische und ethnische Herkunft des Betroffenen gezogen werden könnten.

Der Hinweis auf einen möglichen Rückschluss über den Geburtsort auf ethnische und rassische Herkunft ist nach Auffassung der Landesregierung zutreffend. Ein sol-

cher Rückschluss ist aber auch über Schreibweisen von Namen (bspw. mit Sonderzeichen) und sogar dem Namen selbst möglich. Denkbare Fälle sind derart vielfältig, dass dies nicht in den Begriffsbestimmungen aufgelöst werden kann. Es bedarf der Subsumtion im Einzelfall, ggf. unter Anwendung der anerkannten Auslegungsmethoden. Etwa Geburtsort und Geburtsnamen sind überdies Bestandteil des Grunddatensatzes zu einer Person nach § 111 Ordnungswidrigkeitengesetz. Ein Verzicht auf einen solchen Standard erscheint bspw. für den polizeilichen Bereich im Rahmen von Identitätsfeststellungen und gerade bei der Anzeigenfertigung als ausgeschlossen. Im Übrigen gilt ohnehin das Erforderlichkeitsprinzip.

Aus Sicht der Landesregierung wäre eine Klarstellung im Wortlaut des § 21 LDSG diesbezüglich nicht zielführend.

Vereinzelt wird die Frage aufgeworfen, warum die Begriffsbestimmung gesetzessystematisch erst in § 21 geregelt werden, wenn sie doch auch bereits in den §§ 1 bis 20 vorausgesetzt würden. Es handelt sich um ein Missverständnis (s.o.): § 21 dient ausschließlich der Umsetzung von Artikel 3 JI-Richtlinie in nationales Recht und gilt daher nur für die §§ 20 bis 68 LDSG. Für die §§ 3 bis 20 findet die DSGVO unmittelbare Anwendung. Es gelten daher die Begriffsbestimmungen aus Artikel 4 DSGVO. Diese können auch nicht aus Gründen der Übersichtlichkeit im LDSG wiedergegeben werden, da dies gegen das unionsrechtliche Wiederholungsverbot verstieße. Dieses untersagt den Mitgliedstaaten, im nationalen Recht Regelungen zu treffen, die unmittelbar anwendbarem EU-Recht entsprechen. Hierdurch soll verhindert werden, dass die Normadressaten über den Gemeinschaftscharakter einer Rechtsnorm im Unklaren gelassen oder die Zuständigkeit des Europäischen Gerichtshofs zur Entscheidung über Fragen der Auslegung des Gemeinschaftsrechts oder der Gültigkeit der von den Organen der Gemeinschaft vorgenommenen Handlungen beschnitten werden (EuGH, Urt. v. 10.10.1973 – C-34/73, Rz. 10, 11). Erwägungsgrund 8 der DSGVO lässt daher die Aufnahme von Inhalten der Verordnung in nationales Recht nur in engen Grenzen zu, insbesondere, soweit dies erforderlich ist, die Kohärenz zu wahren.

II. Besondere Verarbeitungssituationen

In Abschnitt 2 wurden die Vorschriften zu besonderen Verarbeitungssituationen behandelt.

1. § 12 LDSG

§ 12 LDSG regelt die Verarbeitung besonderer Kategorien personenbezogener Daten. Darunter versteht der Unionsgesetzgeber besonders sensible Daten wie bspw. politische Meinungen, religiöse oder weltanschauliche Überzeugungen, genetischen oder biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person. Aufgrund des hohen Risikos für die Rechte und Freiheiten der Betroffenen ist die Verarbeitung nach Artikel 9 Absatz 1 DSGVO grundsätzlich verboten.

Das grundsätzliche Verarbeitungsverbot gilt nicht, wenn ein Ausnahmetatbestand greift. Artikel 9 Absatz 2 DSGVO enthält unmittelbare Ausnahmen von dem Verbot. In den Fällen der ausdrücklichen Einwilligung, der Verarbeitung von Daten, die die betroffene Person offensichtlich öffentlich gemacht hat oder bei der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen entstammt die Rechtsgrundlage der Verarbeitung daher direkt der DSGVO. Daneben enthält die DSGVO mehrere Öffnungsklauseln, die es den Mitgliedstaaten ermöglichen, unter bestimmten Voraussetzungen im nationalen Recht weitere Ausnahmen vom Verbot vorzusehen. Hiervon hat der Landesgesetzgeber in § 12 LDSG Gebrauch gemacht.

Eine Rückmeldung zu der Norm regt die Klarstellung an, dass auch unter den in § 12 genannten Voraussetzungen eine bereichsspezifische Norm als Rechtsgrundlage für die Datenverarbeitung erforderlich sei.

Dem liegt jedoch ein falsches Verständnis der Norm zu Grunde. § 12 Absatz 1 LDSG dient unter Rückgriff auf die Öffnungsklauseln des Artikels 9 Absatz 2 Buchstabe b, g, h und i DSGVO dem Ziel, für die Fälle, in denen keine bereichsspezifische Verarbeitungsbefugnis besteht, im Sinne einer Auffang-Datenverarbeitungsbefugnis festzulegen, unter welchen Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise zulässig ist. Eine zusätzliche bereichsspezifische Rechtsgrundlage ist in diesen Fällen gerade nicht von Nöten. Gleichwohl ist die

Schaffung von leges speciales in Fachgesetzen stets möglich. § 12 verfolgt ausschließlich den Zweck der Absicherung, damit keine planwidrige Regelungslücke entsteht, sollte im Fachrecht versehentlich eine erforderliche Rechtsgrundlage fehlen.

Zu beachten ist jedoch, dass für eine zulässige Verarbeitung besonderer Kategorien von Daten stets auch die Voraussetzungen des Absatzes 2 vorliegen müssen. Danach müssen geeignete technische und organisatorische Maßnahmen ergriffen werden, um die Grundrechte und Interessen betroffener Personen zu wahren. Diese spezifischen Schutzmaßnahmen werden in Absatz 3 in Form von Regelbeispielen näher konkretisiert.

Eine weitere Rückmeldung fordert, die in § 12 Abs. 2 und 3 aufgestellten Anforderungen bzw. Beispiele für mögliche Maßnahmen nicht nur in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten vorzusehen, sondern generell bezogen auf sämtliche personenbezogenen Daten. Insofern seien konkrete Vorgaben zur Risikobewertung und eine geeignete Risiko-Methodik zielführender.

Durch die Vorgaben in den Absätzen 2 und 3 des § 12 LDSG kommt die landesgesetzliche Regelung den unionsrechtlichen Anforderungen nach Artikel 9 Absatz 2 Buchstaben b, g, h und i DSGVO nach, wonach Rechtsgrundlagen zur Verarbeitung stets auch angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und der Interessen der betroffenen Personen vorzusehen haben. Für die Verarbeitung der Daten besonderer Kategorie im Sinne des Artikel 9 DSGVO ist diese Regelung also verpflichtend, während dies bei „normalen“ Daten nicht zwingend vorzusehen ist.

Während das Einhalten von technischen und organisatorischen Maßnahmen indes bei allen Datenverarbeitungen geboten ist, selbst wenn dies nicht explizit im § 12 LDSG geregelt ist, wird die besondere Bedeutung der „Artikel 9-Daten“ durch die bestehende, unionsrechtlich gebotene Regelung betont. Die Landesregierung geht davon aus, dass diese unterschiedliche gesetzliche Behandlung auch sachgerecht ist. Das Landesdatenschutzgesetz hat nicht die Funktion eines Leitfadens für jede Form der Datenverarbeitung, sondern soll in möglichst kurzer Form und ohne die Vorgaben der DSGVO zu wiederholen das Notwendige regeln. Die Risikoabwägung und die zu treffenden technischen und organisatorischen Maßnahmen ergeben sich aus der DSGVO und ihren Erwägungsgründen, insbesondere Erwägungsgrund 75, und allgemein aus der Anwendung des Datenschutzrechts in der Praxis. Hierbei macht der technische Wandel unter Umständen andere Maßnahmen erforderlich. Eine zu

differenzierte Ausgestaltung im LDSG könnte eine häufige Änderung des Gesetzes erforderlich machen.

2. § 15 LDSG

Mehrere kritische Rückmeldungen sind zu § 15 LDSG, der die Verarbeitung im Beschäftigungszusammenhang regelt, eingegangen.

Nach dessen Absatz 1 dürfen öffentliche Stellen personenbezogene Daten (einschließlich besonderer Kategorien von Daten) von Bewerberinnen und Bewerbern sowie von Beschäftigten vorbehaltlich besonderer gesetzlicher oder tarifvertraglicher Regelungen nur nach Maßgabe des Landesbeamtengesetzes verarbeiten. Absatz 2 schließt aus, dass Daten von Beschäftigten, die im Rahmen der Durchführung technischer und organisatorischer Maßnahmen zur Datensicherheit verarbeitet oder in einem automatisierten Verfahren gewonnen werden, zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden. Sie dürfen abweichend davon im Bereich der justiziellen Tätigkeit allerdings bei der Auswertung von Akten zum Zweck der Dienstaufsicht, der dienstlichen Beurteilung und der Erteilung von Dienstzeugnissen herangezogen werden. Dies betrifft insbesondere die Verwertung automatisch generierter Verfahrenszahlen.

Die Stellungnahmen merken – zutreffend – an, dass sich der Bezug auf das Landesbeamtengesetz nur auf die Regelungen zum Personalaktenrecht, § 85 ff., beziehen könne. Dieser regele jedoch speziell die Datenverarbeitung im Zusammenhang mit Personalakten. Beschäftigtendaten hätten indes nicht immer die Qualität einer Personalakte (vgl. § 50 BeamtStG), sodass diese bei einem engen Verständnis nicht erfasst wären. Besondere gesetzliche oder tarifvertragliche Regelungen existieren regelmäßig ebenfalls nicht. Die bestehende Regelungslücke sollte durch eine Bestimmung zur Verarbeitung von Beschäftigtendaten geschlossen werden, wie es im Bund beispielsweise in § 26 BDSG der Fall ist. Dort würden detaillierte Regelungen zur Verarbeitung (besonderer) personenbezogener Daten getroffen, insbesondere zu Aufbewahrungsfristen, Einwilligung, Kollektivvereinbarungen oder der Definition des Begriffs „Beschäftigte“. Auch einige andere Länder hätten in ihren Landesdatenschutzgesetzen bereits dezidierte Regelungen.

Bewertung:

Die Kritik ist zutreffend. Die bisherige Regelung wird den komplexen Fragen im Zusammenhang mit der Verarbeitung von Beschäftigtendaten nicht vollständig gerecht, sodass eine Neuregelung erwogen werden sollte. Das ULD hat in diesem Zusammenhang verschiedene Anregungen unterbreitet, die geprüft werden.

Allerdings haben die regierungstragenden Parteien im Bund angekündigt, Regelungen zum Beschäftigtendatenschutz schaffen zu wollen, „um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen“ (Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands, BÜNDNIS 90/DIE GRÜNEN und den Freien Demokraten, S. 17). Hier sollten ggf. zunächst die Einflussmöglichkeiten des Landes, auch im Rahmen der Bundesratsbeteiligung, genutzt werden, um im Anschluss möglichst konsistente landesrechtliche Regelungen zu schaffen.

3. § 26 LDSG

§ 26 LDSG regelt die Verarbeitung zur archivarischen, wissenschaftlichen und statistischen Zwecke im Rahmen der Verarbeitung nach § 20 LDSG, also im Anwendungsbereich der JI-Richtlinie.

a) Anwenderperspektive

Hierzu wurde aus Sicht von Rechtsanwendern zurückgemeldet, es nicht klar, wie eine Verarbeitung zu „archivarischen“ (besser sei „archivischen“) Zwecken im Rahmen der in § 20 LDSG genannten Zwecke erfolgen soll. Archivierung richte sich dem Zweck nach auf die Nutzung von Unterlagen, und das Recht auf Nutzung von Archivalien stehe gemäß § 9 Absatz 1 Landesarchivgesetz (LArchG) allen Personen unabhängig von ihrem Nutzungsinteresse zu. Der Schutz personenbezogener Daten und sonstiger schutzwürdiger Belange werde dabei über Regelungen zur Einschränkung und Versagung der Nutzung von Archivgut (§ 9 Absatz 2 LArchG) sowie über die archivgesetzlichen Schutzfristen (§ 9 Absatz 3 LArchG) gewährleistet. Eine Zweckbindung bei der Nutzung von Archivalien könne lediglich im Zusammenhang mit der Verkürzung von Schutzfristen relevant werden (§ 9 Absatz 6 Nr. 2 LArchG). Es sei daher

wichtig, dass der archivische Zweck – also die nicht unmittelbar zweckgebundene Bereitstellung von Unterlagen für die Nutzung – nicht durch die in § 20 LDSG aufgeführten Zwecke eingeschränkt werde. Die Stellungnahme empfiehlt vor diesem Hintergrund, die Wörter „im Rahmen der in § 20 genannten Zwecke“ in § 26 LDSG zu streichen. § 26 LDSG stünde damit im Einklang mit Artikel 4 Absatz 3 Richtlinie (EU) 2016/680 und die Gefahr eventueller Unklarheiten bei der Auslegung von § 26 LDSG in Verbindung mit § 6 Absatz 2 LArchG wäre beseitigt.

Bewertung:

§ 26 LDSG setzt Artikel 4 Absatz 3 JI-Richtlinie nach Auffassung der Landesregierung exakt um. Hiernach darf der Verantwortliche Daten auch zu wissenschaftlichen, statistischen und historischen Zwecken verarbeiten, solange diese Verarbeitung unter den Anwendungsbereich des Artikel 1 JI-Richtlinie fällt. Es ist also Bedingung, dass die Verarbeitung personenbezogener Daten *zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit* erfolgt. Diese Bedingung ist gleichlautend in § 26 LDSG übernommen. Der Anwendungsbereich damit auch dem des § 20 LDSG, auf welchen in § 26 LDSG Bezug genommen wird. Die Norm des § 26 LDSG gleicht im Übrigen der des § 50 BDSG.

§ 26 LDSG richtet sich an den Verantwortlichen im Anwendungsbereich der JI-Richtlinie, der „seine“ Daten zu den in dieser Norm beschriebenen Zwecken verarbeiten möchte. Die Gesetzesbegründung zur gleichlautenden Norm des § 50 BDSG macht dies deutlich; sie nennt dann auch als Beispiel die im Bundeskriminalamt durchgeführte kriminologische oder kriminaltechnische Forschung (BT-Drs. 18/11325, S. 111). Vergleichbares gilt durch § 26 LDSG in SH für das Landeskriminalamt (polizeiliche Forschung, wissenschaftliche Arbeit, Gutachten). Damit wird ein Spielraum eröffnet, der über die grundsätzliche Zweckbindung aus § 188 Absatz 1 Satz 1 LVwG und die Fälle der Zweckänderung i. S. von § 188a LVwG hinausgeht.

Für die Abgabe der Datenträger an das Landesarchiv anstelle der Löschung und Vernichtung gelten gem. § 196 Absatz 4 LVwG die Bestimmungen des Landesarchivgesetzes. Die Verpflichtung für die Behörden und ihre Organisationen aus § 6 LArchG (Anbieten) sowie die Nutzung des Archivgutes nach § 9 LArchG werden durch § 26 LDSG nicht eingeschränkt.

Die vorgeschlagene Streichung der Wörter „im Rahmen der in § 20 genannten Zwecke“ in § 26 LDSG würde Artikel 3 Absatz 3 JI-Richtlinie widersprechen.

Eine Besonderheit gilt allerdings für Schriftgut zu polizeilichen Ermittlungsvorgängen, die bspw. im Zusammenhang mit der Kriminalitäts- bzw. Verbrechensbekämpfung stehen. Die Originalvorgänge werden von den Staatsanwaltschaften bzw. den Bußgeldbehörden dem Landesarchiv angeboten. Strafanzeigen bzw. Verfahrensakten sind bei den Staatsanwaltschaften nach Abschluss des Verfahrens auf einen Bild- oder anderen Datenträger zu übertragen. Diese Datenträger werden, soweit besondere archivrechtliche Regelungen dies vorsehen, an ein Staatsarchiv abgegeben (vgl. § 489 Abs. 7 StPO).

Das Landesarchiv erhält aus dem polizeilichen Bereich zudem Schriftgut auch mit personenbezogene Daten aus dem Anwendungsbereich der DSGVO (Generalakten der Polizeiabteilung, der Ämter und Behörden). Hier ist § 13 LDSG einschlägig. § 13 LDSG ersetzt und erweitert § 22 des LDSG a. F. Die Vorschrift setzt den in Artikel 89 DSGVO enthaltenen Regelungsauftrag an die Gesetzgeber der Mitgliedstaaten, Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden wissenschaftlichen und historischen Forschungszwecken sowie statistischen Zwecken zu schaffen, um.

b) Perspektive der Aufsichtsbehörde

Das ULD teilt zu § 26 mit, dass aus der Aufsichtstätigkeit bezüglich der Anwendung der Vorschrift keine besonderen Erkenntnisse vorlägen. Es werde jedoch darauf hingewiesen, dass die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in ihrer Stellungnahme zur Evaluierung des BDSG vom 02.03.20211 zu der im Wesentlichen inhaltsgleichen Regelung des § 50 BDSG die Auffassung vertrete, § 50 BDSG gehe nicht über die Vorgaben des Artikel 4 Absatz 3 JI-Richtlinie hinaus und stelle keine Konkretisierung dar. Insofern mangele es der Vorschrift an der erforderlichen Bestimmtheit, insbesondere mit Blick auf die Forderung nach geeigneten Garantien. Es bedürfe einer Ausgestaltung im jeweiligen Fachrecht; dies solle klargestellt werden.

Bewertung:

Die Richtlinie ist für jeden Mitgliedstaat nach dem Grundsatz der loyalen Zusammenarbeit hinsichtlich des zu erreichenden Ziels bzw. Ergebnisses verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel. Die finale Umsetzung des Richtlinienziels ist gemäß der Umsetzungsverpflichtung nach Artikel 288 Absatz 3 AUEV und der Richtlinienbestimmung des Artikel 4 Absatz 3 JI-Richtlinie entsprechend erfolgt. Sie trägt der Rechtsangleichung Rechnung und dient der Stärkung des Datenschutzniveaus innerhalb der EU. Im Übrigen besteht im Falle einer Übernahme des Wortlauts im Rahmen der nationalen Richtlinienumsetzung, anders als bei Verordnungen, kein Normwiederholungsverbot. Bei der hier in Frage stehenden Mindestharmonisierung ist eine Konkretisierung Wortlauts nicht zwingend. Die Auffassung, die Norm sei nicht hinreichend bestimmt, wird nicht geteilt.

4. § 27 LDSG

§ 27 LDSG regelt die Anforderungen an eine wirksame Einwilligung, deren jederzeitige Widerrufbarkeit sowie die Dokumentationspflichten des Verantwortlichen.

a) Anwenderperspektive

Aus dem Bereich der Staatsanwaltschaften wird angemerkt, dass die die datenschutzrechtliche Einwilligung betreffenden Regelungen des § 27 LDSG bzw. § 51 BDSG aus dortiger Sicht als nicht praxistauglich zu bewerten seien. Ungeachtet des aus den dort normierten Belehrungs- und Dokumentationspflichten resultierenden erheblichen administrativen Aufwandes sind Anwendungsbereich und Inhalt der betreffenden Normen bundesweit umstritten. Insoweit wird unter anderem vertreten, die Wirksamkeit im Rahmen des strafrechtlichen Ermittlungsverfahrens erteilter Einwilligungen bzw. Zustimmungen sei an den Anforderungen des § 51 BDSG zu bemessen. Diese Norm beinhalte einen strengen Gesetzesvorbehalt mit der Folge, dass eine strafprozessuale Maßnahme nur dann auf eine Einwilligung des Betroffenen gestützt werden könne, wenn die zugrundeliegende strafprozessuale Norm ausdrücklich eine Einwilligung als Rechtsgrundlage vorsehe. In Anbetracht dessen seien ins-

besondere auf eine Einwilligung des Betroffenen gestützte Durchsuchungen und Atemalkoholmessungen als rechtswidrig zu bewerten. Der Gegenansicht nach seien entsprechende strafprozessuale Maßnahmen als zulässig zu erachten. Die Möglichkeit eines verfassungsrechtlich legitimierten Grundrechtsverzichts könne nicht durch einfachgesetzliches Datenschutzrecht beschränkt werden. Zweifelhaft sei zudem, ob eine Ermittlungsmaßnahme stets als Datenverarbeitung zu qualifizieren sei. Gegen die Auslegung der in Rede stehenden Norm im Sinne eines strengen Gesetzesvorbehaltes spreche schließlich der Inhalt der betreffenden Gesetzesmaterialien. Diesen sei zu entnehmen, dass im Rahmen der Gesetzgebung gerade nicht beabsichtigt worden sei, über die Voraussetzungen der korrespondierenden Regelung der DSGVO hinausgehende Anforderungen aufzustellen. Die in Rede stehende Vorschrift der DSGVO sehe indes einen Gesetzesvorbehalt nicht vor.

Bewertung:

Die Ausführungen zur Einwilligung die Normen § 27 LDSG und § 51 BDSG betreffend sind für die Landesregierung nachvollziehbar. Das Spannungsfeld zwischen einer freien Willensentscheidung und der Durchsetzung strafprozessualer oder polizeilicher Maßnahmen, wenn keine Einwilligung vorliegt oder diese (auch während einer Maßnahme) widerrufen wird, ist im Rahmen des Gesetzgebungsverfahrens intensiv diskutiert worden. Bezogen auf das LDSG ist aber auch klar, dass es sich bei § 27 LDSG eben nicht um eine Rechtsgrundlage zur Datenverarbeitung handelt, sondern diese Norm einen Rahmen vorgibt, wenn personenbezogene Daten aufgrund einer Rechtsvorschrift verarbeitet werden, welche ihrerseits selbst die Einwilligung als Voraussetzung enthält. Gerade vor dem Hintergrund, dass das Instrument der Einwilligung im Anwendungsbereich der JI-Richtlinie umstritten ist, ist der Gesetzesvorbehalt zu begrüßen, damit nicht das allgemeine Datenschutzrecht mehr zulässt, als spezialgesetzlich erlaubt ist.

b) Perspektive der Aufsichtsbehörde

Das ULD verweist hinsichtlich § 27 LDSG auf die Stellungnahme der DSK zur Einwilligung nach § 51 BDSG. Danach gebe die Einwilligung schon dem Wortlaut des § 51 BDSG nach keine Befugnis zur Datenverarbeitung. Sie unterscheide sich insoweit ganz wesentlich von der Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchst. a

DSGVO, die bei Vorliegen der gesetzlichen Voraussetzungen die Verarbeitung von personenbezogenen Daten zulasse. Demgegenüber bedürfe es im Anwendungsbereich von Teil 3 BDSG stets einer spezifischen fachgesetzlichen Rechtsgrundlage, die eine bestimmte Verarbeitung im Falle der Einwilligung zulasse. Insoweit verweist die DSK auf Erwägungsgrund 35 JI-Richtlinie. § 51 BDSG regele sodann den weiteren Umgang mit einer entsprechend erteilten Zustimmung. Irreführend sei hier vor allem die Platzierung der Vorschrift unter der Kapitelüberschrift „Rechtsgrundlagen der Verarbeitung personenbezogener Daten“. Diese sollte geändert werden.

Bewertung:

Der Einschätzung durch das ULD ist zunächst zu entgegnen, dass § 27 Absatz 1 LDSG von § 51 Absatz 1 BDSG abweicht. So ist im LDSG klar geregelt, dass eine Verarbeitung von personenbezogenen Daten nur dann zulässig ist, wenn sie auf Grundlage einer (anderen) Rechtsvorschrift erfolgt, welche die Einwilligung der betroffenen Person zur Voraussetzung hat, und nicht – wie im BDSG – wenn eine Rechtsvorschrift die Verarbeitung auf der Grundlage einer Einwilligung gestattet. Die unterschiedliche Formulierung erfolgte seinerzeit auf Anregung des ULD bei der Anpassung des LDSG, hat in der praktischen Anwendung aber keine besondere Bedeutung.

Die Ausführung der DSK sind in analoger Betrachtung zum LDSG gesehen dahingehend zutreffend, dass sich auch § 27 LDSG von Artikel 6 DSGVO unterscheidet und keine Befugnis zur Verarbeitung von personenbezogenen Daten darstellt. Die Formulierung in § 27 LDSG ist eindeutig.

Die Kritik an der systematischen Platzierung der Vorschrift im Abschnitt 3, Unterabschnitt 2, also unter der Überschrift „Rechtsgrundlagen der Verarbeitung personenbezogener Daten“, wird nicht geteilt. Zuzugestehen ist zwar, dass es sich quasi um einen Verweis in anderen Rechtsvorschriften handelt. Allerdings erwartet der Anwender des Gesetzes den Hinweis, ob eine Einwilligung nach dem allgemeinen Datenschutzrecht im Anwendungsbereich der JI-Richtlinie bzw. des § 20 LDSG möglich ist, gerade in diesem Unterabschnitt.

5. § 30 Absatz 2 LDSG

§ 30 LDSG regelt die Zulässigkeit von automatisierten Einzelfallentscheidungen. Das ULD mahnt an, in § 30 Absatz 2 LDSG sollte als eine der Maßnahmen zum Schutz

der betroffenen Personen das Recht auf persönliches Eingreifen durch den Verantwortlichen ausdrücklich aufgenommen werden. Dieses Recht sei in Artikel 11 JI-Richtlinie (wie auch in Artikel 22 Absatz 3 DSGVO) ausdrücklich vorgesehen.

Bewertung:

Der Hinweis entspricht der Stellungnahme der DSK zu § 54 Absatz 2 BDSG. Praktische Auswirkungen der angeregten Änderung werden jedoch nicht aufgezeigt. Richtig ist, dass die Ergänzung einen Gleichklang zur DSGVO herstellen würde. Allerdings kann die Möglichkeit des persönlichen Eingreifens auch bereits jetzt eine vorgesehene Schutzmaßnahme nach § 30 Absatz 2 LDSG sein. Dies wird jedenfalls nicht dadurch ausgeschlossen, dass sie nicht ausdrücklich im Wortlaut enthalten ist. Insoweit erscheint die Aufnahme eines Rechts auf persönliches Eingreifen als unschädlich, aber auch nicht als erforderlich.

III. Betroffenenrechte

Der dritte Fragenkomplex behandelt die Rechte der betroffenen Personen, die im Anwendungsbereich der DSGVO sowie der JI-Richtlinie unterschiedlich geregelt sind.

1. Betroffenenrechte nach der DSGVO

a) allgemein zu Betroffenenrechten nach der DSGVO

Von zwei befragten Stellen wurden zu den in § 8 (Informationspflicht) und § 9 (Auskunftspflicht) behandelten Rechten der Betroffenen praktische Schwierigkeiten zurückgemeldet, die jedoch aus der Reichweite der durch die DSGVO gewährten Rechte herrühren und nicht aus den Regelungen des LDSG.

So wurde angeführt, die Auskunftserteilung aus Papierakten könne ggf. zu einem immensen Aufwand bei der Auffindung der Akten, auch in Archiven, führen, um die Auskünfte erteilen zu können. Hier würde ein Abstellen auf die Verhältnismäßigkeit gewünscht. Es sei ggf. eine Ablehnung bei offensichtlichem Missbrauch zu erwägen sowie eine Ergänzung, dass die persönliche Betroffenheit nachzuweisen ist.

Bewertung:

Wenngleich die Probleme nachvollziehbar sind, setzt die DSGVO diesem Ansinnen enge Grenzen. Die Information der betroffenen Personen bei Erhebung der Daten (Artikel 13 und 14) und das Recht auf Auskunft über vorhandene Daten (Artikel 15) sind grundlegend für die Ausübung der weiteren Rechte der Betroffenen. Denn nur, wer zutreffend und umfassend über seine verarbeiteten Daten informiert ist, kann seine Rechte auf Berichtigung und Löschung, Übertragung oder Widerspruch sachgerecht ausüben. Die DSGVO sieht daher in Artikel 23 nur geringe Möglichkeiten der Mitgliedsstaaten vor, die gewährten Rechte einzuschränken.

Teilweise hat der Landesgesetzgeber im LDSG hiervon Gebrauch gemacht (siehe sogleich). Im Übrigen sieht die DSGVO selbst Schutzmechanismen vor. So können die Betroffenenrechte ohnehin nur von den von der Verarbeitung betroffenen Personen ausgeübt werden, Artikel 12 Absatz 1 DSGVO. Bei offenkundig unbegründeten oder exzessiven Anträgen, insbesondere im Fall von häufiger Wiederholung, kann der Verantwortliche entweder angemessene Verwaltungsgebühren verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. Ein genereller Verhältnismäßigkeitsvorbehalt, der nicht nur punktuelle Einschränkungen vorsieht, wäre als erhebliche Beschneidung der Betroffenenrechte nach Ansicht des BMI (Evaluierungsbericht zum BDSG, Ziff. 5.6.2.1) nicht mehr von der Öffnungsklausel des Artikel 23 Absatz 1 Buchst. i DSGVO gedeckt.

Eine konkretere Ausgestaltung erfolgt derzeit durch die vermehrt ergehende auch höchstrichterliche Rechtsprechung (etwa BVerwG, Urteil vom 16.09.2020 - 6 C 10.19 - oder BGH, Urteil vom 15.06.2021 - VI ZR 576/19 - sowie Urteil vom 22.2.2022 - VI ZR 14/21), die die unterschiedlichen Interessen der Beteiligten in Ausgleich bringt.

b) § 8 LDSG

Hinsichtlich der Beschränkung der Informationspflichten gegenüber den Betroffenen nach § 8 Absätze 1 bis 3 LDSG wurden lediglich sehr vereinzelte Fälle zurückgemeldet.

Aus dem Bereich der Justiz wird darauf hingewiesen, dass die durch § 8 Absatz 4 eröffnete Möglichkeit, die Informationspflichten gegenüber nicht am Verfahren beteiligter Dritter in allgemeiner Form und für jedermann zugänglich durchzuführen, aus der

dortigen Sicht eine enorme praktische Bedeutung habe und einen sachgerechten Ausgleich zwischen dem Informationsinteresse der Betroffenen und der Erhaltung der Funktionsfähigkeit der Gerichte darstelle.

Auch die mit der Vorschrift des § 9 Absatz 4 LDSG geschaffene Möglichkeit, den Auskunftsanspruch eines Betroffenen durch die Gewährung von Akteneinsicht zu erfüllen, werde als wichtige Regelung im Spannungsfeld von Datenschutzrecht und Prozessrecht angesehen.

c) § 9 Absatz 2 LDSG

Das ULD ist der Auffassung, für die Vorschrift des § 9 Absatz 2 LDSG greife kein Ausnahmetatbestand nach Artikel 23 Absatz 1 DSGVO, sodass diese unionsrechtswidrig sei. Die Anknüpfung am Kriterium des „unverhältnismäßigen Aufwands“ sowie die Ausklammerung von Verarbeitungen zu Zwecken der Datensicherung oder der Datenschutzkontrolle von der Auskunftspflicht würden sachfremde Erwägungen darstellen, die in Artikel 23 Absatz 1 Buchstaben a bis j DSGVO keine Stütze fänden. Vor diesem Hintergrund sollte eine Streichung von § 9 Absatz 2 LDSG erfolgen.

Bewertung:

Die Vorschrift beruht auf der Öffnungsklausel des Artikels 23 Absatz 1 Buchst. i DSGVO. Die Vermeidung eines übermäßigen Aufwands dient der Sicherstellung der Rechte des Verantwortlichen als anderer Person.

Der Kritik an der Regelung ist entgegenzuhalten, dass die Anforderungen an den Ausschluss der Auskunftspflicht hoch sind. Es müssen drei einschränkende Voraussetzungen kumulativ vorliegen. So ist die Auskunftspflicht nur dann ausgeschlossen, wenn es sich um Daten handelt, die ausschließlich noch zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. Berührt sind also bspw. Protokolldaten. Hinsichtlich der Primärdaten der betroffenen Personen besteht der Auskunftsanspruch nach Artikel 15 DSGVO unverändert. Zudem muss die Auskunftserteilung einen unverhältnismäßigen Aufwand verursachen und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen sein. Die Ablehnung ist zu begründen, soweit nicht die Voraussetzungen des Absatz 3 Satz 1 vorliegen. Die betroffene Person kann die Aufsichtsbehörde anrufen.

Insgesamt handelt es sich um eine maßvolle und zulässige Beschränkung des Auskunftsanspruchs zum Schutz der Funktionsfähigkeit der öffentlichen Stellen, die beibehalten werden sollte.

d) § 11 LDSG im Allgemeinen

§ 11 regelt für bestimmte Fälle Einschränkungen des Widerspruchsrechts der Betroffenen aus Artikel 21 DSGVO.

Hierzu wurde zurückgemeldet, das Verhältnis von § 11 LDSG zu Artikel 21 DSGVO sei unklar. Aufgrund der nicht eindeutigen Formulierung des § 11 LDSG sei in der Literatur streitig, ob § 11 LDSG abweichend zu Artikel 21 DSGVO das Widerspruchsrecht der betroffenen Person in zulässiger Weise ausschließen könne. Insbesondere die unterschiedlichen Wortlaute beider Normen (Artikel 21 DSGVO „zwingende schutzwürdige Gründe“ bzw. § 11 LDSG „zwingendes öffentliches Interesse“) würden in der Anwendungspraxis zu Unsicherheiten führen. Die Notwendigkeit des § 11 LDSG sei insoweit fraglich.

Nach Auffassung der Landesregierung besteht für Unsicherheiten bzgl. des Wortlauts kein Anlass. Der Begriff des „zwingenden öffentlichen Interesses“ ist eine Ausfüllung bzw. Präzisierung des von der DSGVO verwendeten allgemeineren Begriffs der „zwingenden schutzwürdige Gründe“. Dies begründet sich darin, dass das LDSG ausschließlich die Datenverarbeitung durch öffentliche Stellen regelt (vgl. § 2 Absatz 1 LDSG), während die DSGVO auch die Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen, etwa Wirtschaftsunternehmen und Privatpersonen, umfasst. „Schutzwürdige“ Interessen von öffentlichen Stellen bei der Aufgabenwahrnehmung können nur solche „öffentlicher“ Natur sein.

e) Zu § 11, 2. Variante LDSG:

Nach § 11, 2. Variante LDSG besteht das Widerspruchsrecht aus Artikel 21 Absatz 1 DSGVO nicht, soweit „eine Rechtsvorschrift zur Verarbeitung verpflichtet.“

Das ULD weist darauf hin, dass die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung nach Artikel 6 Absatz 1 Buchst. c DSGVO, welche inhaltlich § 11, 3. Halbsatz LDSG entspricht, in Artikel 21 Absatz 1 DSGVO überhaupt nicht erwähnt werde. Dieser erfasse nur Widersprüche im Rahmen der Verarbeitungen nach Artikel 6 Absatz 1 Buchst. e und f DSGVO.

Bewertung:

Der Hinweis ist zutreffend. Die Regelung – die im Übrigen gleichlautend zu § 36 BDSG ist – dürfte auf seinerzeit anfängliche Unsicherheiten bei der Auslegung der neuen Erlaubnistatbestände in Artikel 6 Absatz 1 DSGVO zurückzuführen sein. Mittlerweile ist gesichert, dass Artikel 21 Absatz 1 DSGVO schon kein Widerspruchsrecht gewährt, wenn die Verarbeitung auf einer rechtlichen Verpflichtung beruht.

Votum:

Es ist entbehrlich, dieses nichtexistente Widerspruchsrecht im nationalen Recht auszuschließen. Der Passus kann gestrichen werden.

f) Erweiterung des Anwendungsbereichs des § 13

In einer Stellungnahme wurde bemängelt, dass die Privilegierung des § 13 LDSG lediglich für den Bereich der Forschung gelte, nicht für den der Lehre. Eine Datenverarbeitung ist hiernach möglich, wenn schutzwürdige Belange nicht beeinträchtigt werden oder das öffentliche Interesse an der Verarbeitung überwiegt, selbst wenn die betroffene Person nicht eingewilligt hat.

Bewertung:

§ 13 LDSG bildet hier das datenschutzrechtliche Forschungsprivileg des Artikel 89 DSGVO ab. Die Verarbeitung von Daten zu wissenschaftlichen oder historischen Forschungsvorhaben oder zu statistischen Zwecken dient dem im öffentlichen Interesse liegenden Erkenntnisgewinn und wird daher von der DSGVO als förderungswürdig gesehen. Dies gilt insbesondere mit Blick auf das Ziel einer Verwirklichung des gemeinsamen Europäischen Forschungsraums. Da gerade die Forschung, anders als viele andere Bereiche, gezwungen ist, auf große Mengen personenbezogener Daten zurückzugreifen, sieht § 13 LDSG für diesen Bereich eine Privilegierung vor. Im Hinblick auf andere Verarbeitungszwecke, wie etwa die Lehre, ist indes nicht klar, wieso ein Personenbezug aufrechterhalten werden sollte, bzw. eine Einwilligung

der betroffenen Personen nicht eingeholt werden kann. Nach Ansicht der Landesregierung besteht daher kein den Datenschutz überwiegendes Bedürfnis für eine Änderung der bestehenden Vorschrift.

g) Einwilligungsfreie Veröffentlichung nach § 13 LDSG

Aus dem Bereich der Wissenschaft wurde der Wunsch geäußert, auch die Veröffentlichung von Datensätzen in pseudonymisierter Form als weiteren einwilligungsfreien Tatbestand in den § 13 Absatz 1 LDSG aufzunehmen. Immer häufiger bestehen bei Fördermittelgebern oder im Hinblick auf gute wissenschaftliche Praxis die Erwartung, dass Rohdatensätze auf Open-Data-Plattformen veröffentlicht werden. Auch Zeitschriftenherausgeber möchten, dass Forschungsergebnisse unabhängig nachprüfbar sind. Während die Forschungsarbeit selbst also datenschutzrechtlich einwilligungsfrei sein kann, ist diese Veröffentlichung aufgrund der weiterhin bestehenden Personenbeziehbarkeit einwilligungspflichtig und damit mit größeren Hürden verbunden.

Bewertung:

Das Ansinnen sowohl der Fördermittelgeber, als auch der Herausgeber wissenschaftlicher Zeitungen und letztendlich der Forschenden ist nachvollziehbar und wurde dementsprechend intensiv geprüft und länderübergreifend besprochen. Eine solche Veröffentlichung von unter Umständen sehr großen Mengen von teilweise – etwa im Medizinbereich – zudem besonders sensiblen Daten stellt einen außergewöhnlich großen Eingriff in die Persönlichkeitsrechte der betroffenen Personen dar. Eine einwilligungsfreie Veröffentlichung muss daher auf die Fälle beschränkt bleiben, in denen eine Anonymisierung tatsächlich nicht in Frage kommt.

Ein überragendes Interesse an guter datenbasierter Forschung hat indes auch die Europäische Union erkannt und entwickelt derzeit unionsweite Lösungen. Da Forschung fast immer international angelegt ist und selten nur durch eine öffentliche Stelle durchgeführt wird, sind Lösungen hier stets grenzübergreifend zu denken, um die Forschenden nicht mit unterschiedlichen Datenschutzregimen zu konfrontieren. Ein geplanter spezifischer Datenraum ist hier der „Europäische Raum für Gesundheitsdaten“ (European Health Data Space – EHDS) nach Artikel 1 Absatz 1 EHDS-E, der Vorschriften, gemeinsame Standards und Verfahren, Infrastrukturen und einen Governance-Rahmen für die Primär- und Sekundärnutzung elektronischer Gesund-

heitsdaten schaffen soll. Der bisher bestehenden Fragmentierung innerhalb der Mitgliedstaaten, die in Deutschland noch durch unterschiedliche Landeskrankenhausgesetze verstärkt ist, soll hiermit entgegengetreten werden. Auch die Bundesregierung plant zu Januar 2024 ein Gesundheitsdatennutzungsgesetz, das unter anderem eine zentrale Datenzugangs- und Koordinierungsstelle vorsieht, die die Verknüpfung unterschiedlicher Datenquellen über Forschungspseudonyme ermöglichen soll.

h) Erweiterung des § 13 LDSG um eine Beschränkung der Informationspflicht

In einer Stellungnahme wird gefordert, auch die nach Artikel 13 Absatz 3 und Artikel 14 Absatz 4 DSGVO bestehende Informationspflicht in den Katalog der nach § 13 beschränkbaren Betroffenenrechte aufzunehmen. Nach derzeitigem Stand können bei zu Forschungszwecken verarbeiteten Daten die Betroffenenrechte nach den Artikeln 15, 16, 19 und 21 DSGVO (u. a. Auskunftsrecht, Recht auf Berichtigung) beschränkt werden, wenn ihre Wahrnehmung die spezifischen Forschungs- oder Statistikzwecke voraussichtlich unmöglich machen oder ernsthaft beeinträchtigen würde.

Bewertung:

Eine Erweiterung der Beschränkung auch auf das Recht der betroffenen Personen auf Information über eine Datenverarbeitung würde eine Erleichterung für die datenverarbeitenden Stellen bedeuten. Allerdings bildet § 13 Absatz 5 LDSG hier die in Artikel 89 Abs. 2 vorgesehene Öffnungsklausel ab, die diese Privilegierung ausdrücklich nur für die Betroffenenrechte nach den Artikeln 15, 16, 19 und 21 DSGVO vorsieht. Eine pauschale Erweiterung auch auf Zwecke der Lehre dürfte unionsrechtswidrig sein, zumal ohne die Information über eine Datenverarbeitung die betroffene Person in Unkenntnis verbliebe und die Wahrnehmung von Betroffenenrechten damit gänzlich ausgeschlossen wäre.

2. Betroffenenrechte nach der JI-Richtlinie

a) § 33 LDSG

§ 33 LDSG regelt das Recht betroffener Personen, auf Antrag Auskunft darüber zu erhalten, ob eine öffentliche Stelle sie betreffende Daten verarbeitet, und dessen Einschränkungen.

Das ULD verweist auf die Stellungnahme der DSK zu § 57 BDSG, soweit diese Vorschrift mit § 33 LDSG deckungsgleich ist. Artikel 12 Absatz 3 DSGVO regele, dass auf die Ausübung der meisten Rechte von betroffenen Personen (z. B. Auskunft) unverzüglich, spätestens aber nach einem Monat, reagiert werden müsse (Verlängerung möglich). Eine solche Regelung fehle in der JI-Richtlinie. Deren Artikel 12 Absatz 3 fordere, dass „die betroffene Person unverzüglich schriftlich darüber in Kenntnis“ zu setzen sei, „wie mit ihrem Antrag verfahren wurde“. Dies sei auch so in § 35 Absatz 2 LDSG umgesetzt worden. In der Praxis werde nicht selten die Monatsfrist überschritten, ohne dass die betroffenen Personen informiert werden. Dies führe in der Praxis zu Beschwerden bei den Datenschutzaufsichtsbehörden. Für die Aufsichtsbehörde stelle sich regelmäßig die Frage, welche Frist für die Reaktion bzw. für eine Zwischennachricht noch angemessen ist. Für die Reaktion der Aufsichtsbehörde gegenüber Beschwerdeführerinnen und Beschwerdeführern würden wiederum gesetzliche Fristen gelten, § 37 Absatz 2 LDSG. Hier wäre zu überlegen, auch für die Verfahren der Wahrnehmung der Betroffenenrechte Fristen vorzusehen.

Bewertung:

Die Verweisung auf die Stellungnahme der DSK betrifft zunächst § 57 Absatz 3 BDSG, welcher in dem angesprochenen Kritikpunkt nicht der Regelung des sonst im Wesentlichen gleichlautenden § 33 Absatz 3 LDSG entspricht. Letzterer ist entgegen der zwingenden Regelung im BDSG nämlich als Ermessensnorm ausgestaltet.

Die weiteren Hinweise zu § 57 BDSG könne zwar nachvollzogen werden, werden aber nicht geteilt:

So betreffen die in § 57 Absatz 2 BDSG bzw. § 33 Absatz 2 LDSG genannten Daten keinerlei personenbezogene Daten aus der polizeilichen Sachbearbeitung, sondern technische Protokolldaten. Insofern ist richtig dargestellt, dass sich diese Daten dem allgemeinen Zugriff durch Jedermann in der Behörde entziehen.

Nach § 57 Absatz 4 BDSG bzw. § 33 Absatz 4 LDSG bestehen Einschränkungsmöglichkeiten hinsichtlich des Auskunftsanspruches unter den gleichen Voraussetzungen wie bei Benachrichtigungspflichten. Dies stellt letztlich die Prüfung sicher, ob anderweitige Rechtsgüter (namentlich die Erfüllung von Aufgaben nach § 45 BDSG/§ 20 LDSG, die öffentliche Sicherheit oder Rechtsgüter Dritter) einer Beauskunftung entgegenstehen. Der Hinweis der DSK, den sich das ULD zu eigen macht, wonach dies nicht bedeute, dass zwangsläufig kein Auskunftsanspruch besteht, wenn zuvor die

Benachrichtigung unterblieben ist, ist zwar richtig. Diese Erkenntnis erfordert aber keine Gesetzesänderung. Es ist vielmehr eine Frage des tatsächlichen Umgangs mit Anträgen auf Auskunft. Ein Automatismus besteht bereits jetzt nicht.

Hinsichtlich der Regelungen in § 57 Absatz 6 Satz 2 BDSG bzw. § 33 Absatz 5 Satz 2 LDSG, wonach im Ausnahmefall nicht nur von der inhaltlichen Beauskunftung, sondern auch von der Unterrichtung hierüber abzusehen ist, ist anzumerken, dass diese im Rahmen von länderübergreifenden Diskussionen durchaus kritisch gesehen werde. Denn soweit von dieser Regelung Gebrauch gemacht wird, könnte dies dem Auskunftsbegehrenden suggerieren, es seien über ihn tatsächlich keine personenbezogenen Daten gespeichert. Ein solches Verschweigen könnte als eine gewisse Unehrlichkeit (quasi eine „staatliche Lüge“) angesehen werden.

Eine Form des Umgangs, der dieses Verschweigen verhinderte, wäre ein In-die-Länge-Ziehen des Verwaltungsvorganges zum Auskunftsbegehren. Eine solche Praxis wird von der Landespolizei SH nicht angewandt.

Fallzahlen nach § 33 Absatz 4 - 6 LDSG aus dem staatsanwaltschaftlichen Bereich sind nicht bekannt; dem Ministerium für Inneres, Kommunales, Wohnen und Sport (Polizeiabteilung) werden pro Jahr ca. 30 - 35 Fälle vorgelegt, in dem die Auskunft eingeschränkt erteilt oder gänzlich verweigert wird.

Soweit das ULD bzw. die Stellungnahme der DSK zu § 57 BDSG abschließend auf die einzuhaltenden Fristen eingeht, ist anzumerken, dass zur Umsetzung des Artikels 12 der Richtlinie (EU) 2016/680 der Wortlaut aus Absatz 3 mit „unverzüglich schriftlich darüber in Kenntnis zu setzen“ unverändert in § 35 Absatz 2 LDSG übernommen worden ist. Eine Fristenkollision mit § 37 Absatz 2 LDSG kann nicht nachvollzogen werden. Diese ist auf 3 Monate festgelegt und beschreibt den Fall, dass die Aufsichtsbehörde die betroffene Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat. Das Delta beträgt bei Überschreiten einer – in Anlehnung an Artikel 12 DSGVO festgelegten – vierwöchigen Frist, wenn diese als Vorbild dienen sollte, immerhin noch zwei Monate. Selbst eine Überschreitung dieser angedachten 4-Wochenfrist bei der Beauskunftung durch die Polizei ist grundsätzlich ohne negative Wirkung auf die Arbeitsweise der Aufsichtsbehörde nach Vorgabe aus § 37 LDSG. Im Übrigen sieht § 37 Absatz 2 auch vor, dass die betroffene Person innerhalb dieser

Drei-Monatsfrist über den Stand der Beschwerde in Kenntnis gesetzt werden kann. Einer Anpassung der Fristen bedarf es daher nach hiesiger Auffassung nicht.

b) § 34 LDSG

§ 34 LDSG regelt die Rechte der Betroffenen auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung. § 34 Absatz 2 LDSG besagt insbesondere, dass die betroffene Person das Recht hat, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn (u. a.) deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(i) Anwenderperspektive

Seitens einer öffentlichen Stelle wird kritisiert, § 34 Absatz 2 LDSG stehe im Widerspruch zu § 6 Absatz 2 LArchG, sofern sich eine verlangte Löschung nicht ausschließlich auf unzulässig erhobene Daten bezieht. Es wird daher vorgeschlagen, in § 34 Absatz 2 LDSG ausdrücklich auf die Regelung zur Löschung von Daten in § 6 LDSG zu verweisen oder folgenden Satz zu ergänzen: „Sofern nicht bereits die Erhebung der Daten unzulässig war, sind diese vor einer Löschung dem zuständigen Archiv zur Übernahme anzubieten und bei festgestellter Archivwürdigkeit zu übergeben,“

Bewertung:

Die Landesregierung sieht kein Erfordernis einer Ergänzung, die nur klarstellenden Charakter hätte.

Das Verlangen der betroffenen Person löst eine Einzelfallprüfung über die Erforderlichkeit der weiteren Speicherung aus. Hat diese Prüfung zum Ergebnis, dass die Daten zu löschen sind, greift § 6 Absatz 2 LArchG, wonach Unterlagen, die nach einer Rechtsvorschrift zu löschen sind zuvor dem zuständigen Archiv anzubieten sind. Es gilt insoweit nichts anderes, als bei einer „regulären“ Löschung, die nicht auf einen Antrag der betroffenen Person zurückzuführen ist, sondern auf einen Wegfall des

verfolgten Zwecks oder den Ablauf von Aufbewahrungsfristen. Soweit bereichsspezifisches Datenschutzrecht, das nach dem Grundsatz der Spezialität vorrangig vor dem LDSG Anwendung findet, ausdrücklich auf die Verpflichtung zur Anbietung vor Löschung (so § 196 Absatz 4 LVwG) oder Sperrung (§ 60 Absatz 4 JVollzDSG SH) hinweisen, hat dies rein deklaratorischen Charakter. Eine entsprechende Ergänzung von § 34 Absatz 2 LDSG ist nicht zwingend geboten.

(ii) Perspektive der Aufsichtsbehörde

Das ULD verweist hierzu erneut auf die Stellungnahme der DSK zum gleichlautenden § 58 BDSG. Danach solle die in § 58 Absatz 1 Satz 5 BDSG (wortgleich zu § 34 Absatz 1 Satz 5 LDSG) enthaltene Einschränkung „wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist“ gestrichen werden. Die Regelung bürge die Gefahr, dass ein Antrag einer betroffenen Person auf Vervollständigung von Daten aus Gründen des Verwaltungsaufwands abgelehnt werde. Der Aufwand sei jedoch kein Kriterium nach der JI-Richtlinie, um Betroffenenrechte einzuschränken.

Bewertung:

Die Kritik wird nicht geteilt. An der Regelung gilt es festzuhalten, weil das Verlangen einer betroffenen Person sonst dazu führen kann, dass personenbezogene Daten, die nicht relevant sind, unnötigerweise trotzdem verarbeitet und in Dateisystemen aufgenommen werden. Dies widerspräche den Datenschutzgrundsätzen der Datenminimierung und der Erforderlichkeit.

IV. Aufsichtsbehörde

Des Weiteren wurden Fragen zur Aufsichtsbehörde gestellt. Die Frage nach Aufgaben und Befugnissen wurden an alle befragten Rechtsanwender gerichtet. Die speziellen Fragen zur Ausgestaltung der Aufsichtsbehörde, insbesondere ihre Rechtsform und das Amtsverhältnis der oder des LfDI, wurden wegen der nur dort bestehenden Betroffenheit lediglich an das ULD selbst und – wegen der dortigen Zuständigkeit für grundsätzliche Personalangelegenheiten sowie das öffentliche Dienstrecht – die Staatskanzlei adressiert.

1. Befugnisse

a) § 17 LDSG

§ 17 LDSG regelt die Aufgaben und Befugnisse der oder des Landesbeauftragten für Datenschutz als Aufsichtsbehörde im Sinne der DSGVO.

Soweit eine Stellungnahme kritisiert, dass die Aufsichtsbehörde insgesamt mehr Befugnisse haben sollte, sei zunächst angemerkt, dass sich diese grundsätzlich unmittelbar aus Artikel 58 der DSGVO ergeben.

Das ULD kritisiert indes im Speziellen, es sei – anders als von der DSGVO vorgegeben – aufgrund landesrechtlicher Besonderheiten gegenüber öffentlichen Stellen nicht vollständig gewährleistet, dass die Aufsichtsbehörde „wirksame Befugnisse“ im Sinne des Artikel 58 erhalten habe, damit sie „die einheitliche Überwachung und Durchsetzung“ der DSGVO sicherstellen kann (Erwägungsgrund 129). Denn zwar sei nach Artikel 58 Absatz 2 DSGVO der Erlass von Anordnungen und Verboten auch gegenüber öffentlichen Stellen möglich. Gegen solche Verwaltungsakte könnten sich die Adressaten auch nach Artikel 78 Absatz 1 DSGVO i.V.m. § 20 BDSG vor dem Verwaltungsgericht zur Wehr setzen. Unterlasse es eine öffentliche Stelle allerdings, einer Anordnung nachzukommen, so könne diese derzeit nicht vollstreckt werden. Nach § 234 LVwG sei der Vollzug gegen Träger der öffentlichen Verwaltung nur möglich, soweit er durch Rechtsvorschrift ausdrücklich zugelassen sei. An einer solchen Rechtsvorschrift fehle es. Lege eine öffentliche Stelle als Adressatin einer Maßnahme nach Artikel 58 Absatz 2 DSGVO keine Rechtsmittel ein und komme sie gleichzeitig der Anordnung nicht nach, so entstünde eine dauerhaft rechtswidrige Situation, die nicht aufgelöst werden könne.

Zur Lösung schlägt das ULD vor, der Aufsichtsbehörde die Möglichkeit einer Feststellungsklage einzuräumen, um die Prüfung der Rechtmäßigkeit seiner Anordnungen gegenüber öffentlichen Stellen selbst vor das Verwaltungsgericht zu tragen, 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, könne es gegebenenfalls selbst die Vollstreckung nach § 172 VwGO vornehmen.

Bewertung:

Die Rechtslage wird im Wesentlichen zutreffend dargestellt. Die vom ULD geschilderte Situation ist indes nach Kenntnis der Landesregierung in der Praxis noch nie eingetreten. Die Landesregierung hat daher keinen Grund, daran zu zweifeln, dass öffentliche Stellen sich entsprechend des Rechtsstaatsprinzips (Artikel 20 Absatz 3 GG, Artikel 52 Absatz 3 Landesverfassung) an Gesetz und Recht halten und daher aufsichtsbehördliche Anordnungen entweder direkt befolgen oder auf dem dafür vorgesehenen Verwaltungsrechtsweg gerichtlich überprüfen lassen und sich dann an das Urteil halten.

Zur konkret angeregten Abhilfe durch Einräumung der Möglichkeit zur Erhebung einer Feststellungsklage ist einzuwenden, dass ein solches Verfahren dem Grundgedanken des deutschen Rechtsschutzsystems widerspräche, wonach es nicht die Exekutive ist, die die eigenen Entscheidungen gerichtlich überprüfen lassen kann. Vielmehr ist es Sache der Adressaten von Verwaltungsakten, gegen diese vorzugehen, wenn sie diese für rechtswidrig halten. Da ein praktischer Bedarf nicht ersichtlich ist, ist es nach Auffassung der Landesregierung nicht angezeigt, allein im Datenschutzrecht davon abzuweichen (so auch das BMI, Evaluierungsbericht zum BDSG, Ziff. 5.8.2.6).

Auch kann mittels einer Feststellungsklage erstrittenes verwaltungsgerichtliches Feststellungsurteil in der Hauptsache mangels vollstreckungsfähigen Inhalts ohnehin nicht vollstreckt werden (*Kraft*, in: Eyermann, VwGO, 15. Aufl. 2019, § 168 Rn. 3; *Porz*, in: Fehling/Kastner/Störmer, Verwaltungsrecht, 5. Aufl. 2021, § 168 Rn. 3). Dem Feststellungsurteil wohnt kein Vollstreckungsdruck inne (vgl. BVerwGE 36, 179 = NJW 1971, 1284). Es kann lediglich wegen der Kosten vorläufig vollstreckt werden (vgl. *Bamberger*, in: Wysk, VwGO, 3. Aufl. 2020, § 167 Rn. 13; *Porz*, in: Fehling/Kastner/Störmer, Verwaltungsrecht, 5. Aufl. 2021, § 168 Rn. 3).

Die angeregte Änderung sollte daher nicht aufgegriffen werden.

b) Auskunfts- und Informationspflichten der Aufsichtsbehörde ggü. Betroffenen

Eine Stellungnahme thematisiert die gegenüber der datenschutzrechtlichen Aufsichtsbehörde bestehenden Auskunfts- und Informationspflichten. Diese seien hinsichtlich der Strafverfolgungsbehörden in Inhalt und Umfang nicht in hinreichendem

Maße normiert. Insbesondere der Umstand, dass die Preisgabe von Informationen aus (laufenden) Ermittlungsverfahren zur Konsequenz habe, dass die Strafverfolgungsbehörden keinen weiteren Einfluss darauf nehmen können, ob und in welchem Umfang die Aufsichtsbehörde dem Betroffenen gegenüber im Rahmen der datenschutzrechtlichen Bescheidung Verfahrensinhalte offenbart, finde in den bestehenden Regelungen keine Berücksichtigung. Eine solche Offenlegung könne indes weitreichende Folgen für das Ermittlungsverfahren haben und im Einzelfall sogar eine erhebliche Gefährdung des Untersuchungszwecks nach sich ziehen.

Bewertung:

Aus Sicht der Landesregierung lässt sich etwaigen Zielkonflikten zwischen der Notwendigen Sicherung des Untersuchungszwecks laufender Ermittlungen sowie den Rechten Betroffener im Zusammenhang mit Auskunfts- und Informationspflichten der Aufsichtsbehörde auf dem Boden der geltenden Regelungen ausreichend Rechnung tragen. Es ist insoweit zunächst auf die Verpflichtung der oder des Landesbeauftragten zur Verschwiegenheit über amtlich bekanntgewordene Angelegenheiten aus § 7 Absatz 3 Errichtungsgesetz ULD zu verweisen.

Nach § 9 Absatz 3 LDSG ist in den Fällen, in denen das Auskunftsrecht der Betroffenen aus Artikel 15 DSGVO eingeschränkt ist, die Auskunft auf Antrag dem ULD zu erteilen. Sogar, wenn die zuständige oberste Landesbehörde feststellt, dass durch die Offenlegung die Sicherheit des Bundes oder eines Landes gefährdet würde, ist die Auskunft der oder dem Landesbeauftragten oder einer von ihr oder ihm besonders damit beauftragten Person zu erteilen. Nach § 9 Absatz 3 Satz 5 LDSG darf die Mitteilung der oder des Landesbeauftragten an die betroffene Person keine Rückschlüsse auf die Inhalte zulassen.

Sollten gegenüber dem ULD Auskunftsansprüche nach dem IZG-SH geltend macht werden, wird dieses den Schutz entgegenstehender öffentlicher Interessen zu berücksichtigen haben, worunter u.a. auch die Durchführung eines laufenden Gerichtsverfahrens und die Durchführung strafrechtlicher oder ordnungswidrigkeitenrechtlicher Ermittlungen fallen (§ 9 Absatz 1 Nr. 4 IZG-SH).

Im Hinblick auf diese Grundentscheidungen des Gesetzgebers bestehen im Hinblick auf die Behandlung von Informationen durch die oder den LfDI keine Bedenken. Es sind auch seit Inkrafttreten des LDSG keine Probleme bekanntgeworden.

Einzuräumen ist, dass die Vorgabe des § 9 Absatz 3 Satz 5 LDSG de lege lata nur für den dortigen Fall des Auskunftsantrags nach Artikel 15 DSGVO in dem dort spezifisch geregelten Verfahren gilt. Die Landesregierung wird prüfen, ob es sich nicht vielmehr um einen allgemeinen Grundsatz handelt, der auf alle Fälle – auch anlassbezogene Prüfungen aufgrund von Betroffenenrügen – übertragen werden sollte, sodass auch § 64 LDSG abgedeckt ist.

c) § 64 LDSG

§ 64 LDSG regelt die Befugnisse der oder des Landesbeauftragten für Datenschutz bei der Verarbeitung personenbezogener Daten durch die in § 20 genannten Stellen, also im Anwendungsbereich der JI-Richtlinie.

(i) Perspektive der Aufsichtsbehörde

Aus Sicht des ULD wäre eine Klarstellung der nach Artikel 47 Absatz 1 JI- Richtlinie erforderlichen Untersuchungsbefugnisse wünschenswert. Im Gegensatz zu Artikel 58 DSGVO, der Untersuchungs- und Anordnungsbefugnisse klar voneinander trenne und ausdifferenziert regele, sei § 64 LDSG systematisch unglücklich aufgebaut. Eine ausdrückliche Regelung der Untersuchungsbefugnisse fehle. § 64 LDSG beschränke sich auf die Verpflichtungen der Verantwortlichen, der und ihren Beauftragten Zugang zu Gebäuden, Anlagen und Daten zu gewähren und alle Informationen bereitzustellen. Es verwundere, dass dieser Verpflichtung keine ausdrückliche Befugnis der Landesbeauftragten gegenüberstehe, Zugang oder Auskünfte zu verlangen. In systematischer Hinsicht sei nicht nachvollziehbar, warum in § 64 LDSG für den Bereich der JI-Richtlinie zunächst die Abhilfebefugnisse und erst danach die Untersuchungen der Landesbeauftragten geregelt werden. Zur Klarstellung sollten daher ausdrückliche Untersuchungsbefugnisse nach dem Vorbild des Artikel 58 Absatz 1 DSGVO geregelt werden und diese den Abhilfebefugnissen und den Mitwirkungspflichten der Verantwortlichen vorangestellt werden.

Die Abhilfebefugnisse der Landesbeauftragten blieben hinter denen der DSGVO zurück. Vor allem seien in § 64 LDSG nicht sämtliche in Artikel 47 Absatz 2 JI- Richtlinie genannten Abhilfebefugnisse umgesetzt. So soll in Artikel 47 Absatz 2 Buchst. b

JI- Richtlinie genannte Befugnis, die Berichtigung, Löschung oder Einschränkung der Verarbeitung anzuordnen, nicht ausdrücklich in § 64 LDSG wiedergegeben sein. Zudem fehle die Befugnis nach Artikel 47 Absatz 2 Buchst. c JI- Richtlinie, eine vorübergehende oder endgültige Beschränkung der Verarbeitung vorzusehen. In der aufsichtsbehördlichen Praxis habe sich das Fehlen dieser Befugnisse bislang nicht ausgewirkt. Bislang habe man Beschwerden – z. B. zu der Löschung von Datensätzen, für die die Erforderlichkeit einer weitergehenden Aufbewahrung nicht erkennbar war – im Einvernehmen mit den Verantwortlichen lösen können. Ob die Regelung der Abhilfebefugnisse im LDSG europarechtskonform ist, sei hingegen zweifelhaft. Hier bestehe ein Risiko einer nicht ausreichenden Umsetzung von Europarecht. Die Beurteilung dieser Frage obliege der Europäischen Kommission, die eine Evaluierung der Umsetzung der JI-Richtlinie in den Mitgliedstaaten bereits eingeleitet habe, und dem Europäischen Gerichtshof.

Letztlich fehle im LDSG die Befugnis nach Artikel 47 Absatz 5 JI-Richtlinie, „Verstöße gegen nach dieser Richtlinie erlassene Vorschriften den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die nach dieser Richtlinie erlassenen Vorschriften durchzusetzen“.

Bewertung:

Die Ausgestaltung des § 64 LDSG erfolgte bei Novellierung des LDSG in Anlehnung an § 16 Absatz 2 BDSG. Bereits im Zuge des Gesetzgebungsverfahrens zum LDSG n. F. hat sich das ULD in gleicher Weise geäußert (vgl. u. a. die Stellungnahmen des ULD vom 01.12.2017 im Rahmen der Verbandsanhörung sowie vom 12.03.2018 im Rahmen der schriftlichen Anhörung des IuR-Ausschusses).

Die Landesregierung war seinerzeit und ist nach wie vor der Auffassung, dass Artikel 47 JI-Richtlinie in Absatz 2 Befugnisse – entgegen der Regelung in Artikel 58 DSGVO – ausdrücklich „beispielhaft“ aufzählt und dem Gesetzgeber somit ermöglicht, entgegen der starren Regelung in der DSGVO eine Abweichung für den Anwendungsbereich der Richtlinie zu normieren. Es handelt sich gerade nicht um einen Mindestkatalog.

Durch den Gleichlauf mit § 16 BDSG ist gewährleistet, dass die Befugnisse für die oder den LfD gegenüber allen öffentlichen Stellen, egal ob die des Bundes oder des Landes, gleich sind, wenn sie personenbezogene Daten im Anwendungsbereich der

JI-Richtlinie verarbeiten. Das gilt insbesondere auch für die Befugnis nach Artikel 47 Absatz 5 JI-Richtlinie.

In der Zeit seit Inkrafttreten des neuen LDSG im Mai 2018 sind keine Fälle bekanntgeworden, in denen es der Aufsichtsbehörde an wirksamen Befugnissen gemangelt hätte, um datenschutzrechtliche Missstände im Bereich der Strafverfolgungsbehörden abzustellen. Aus Sicht der Landesregierung bedarf es daher keiner Erweiterung der Abhilfebefugnisse in § 64 LDSG. Auch wäre gerade aus polizeilicher Sicht nicht vertretbar, wenn es in letzter Konsequenz zu einem Verbot des Umganges mit personenbezogenen Daten im Rahmen der Verbrechens- und Terrorbekämpfung geben könnte.

Gleichwohl ist zu konstatieren, dass die Europäische Kommission diese Argumentation nicht teilt. Sie ist der Auffassung, dass Deutschland gegen seine Verpflichtungen nach Artikel 47 Absatz 2 JI-Richtlinie verstoßen habe, da es versäumt worden sei, die Datenschutzaufsichtsbehörden mit wirksamen Abhilfebefugnissen auszustatten. Die Kommission hat daher ein Vertragsverletzungsverfahren gemäß Artikel 258 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) eingeleitet. Im Mahnschreiben vom 19. Mai 2022 wird dargelegt, dass es in Deutschland sowohl auf bundesgesetzlicher Ebene als auch in 14 Bundesländern – darunter Schleswig-Holstein – an wirksamen und gleichwertigen Abhilfebefugnissen für die Datenschutzaufsichtsbehörden mangele. Die Überwachung und Durchsetzung der nach der JI-Richtlinie erlassenen Vorschriften könne nicht gewährleistet werden, wenn die Datenschutzaufsichtsbehörden nicht über wirksame Befugnisse verfügen. Die Datenschutzaufsichtsbehörden müssten in der Lage sein, konkrete Maßnahmen zur Beseitigung von Verstößen gegen die nationalen Gesetze zur Umsetzung der JI-Richtlinie rechtsverbindlich anzuordnen. Die Mitgliedstaaten müssen daher vorsehen, dass die Datenschutzaufsichtsbehörden nicht nur befugt sind, Warnungen gemäß Artikel 47 Absatz 2 Buchstabe a der Richtlinie auszusprechen, die sich nur auf die beabsichtigte Verarbeitung beziehen, oder eine Art Stellungnahme oder Beschwerde bezüglich der Rechtmäßigkeit einer Verarbeitung ohne bindende oder durchsetzbare Wirkung abgeben können.

Aus Sicht der Landesregierung ist an der vorstehend dargestellten Argumentation festzuhalten. Sollte die KOM jedoch bei ihrer Auffassung bleiben und ggf. der zur Letztentscheidung berufene EuGH einen Änderungsbedarf des nationalen Rechts

feststellen, ist eine Anpassung des Landesrechts angezeigt. Diese beträfe dann in gleicher Weise das BDSG, so dass die Entwicklung der Bundesgesetzgebung zu beachten sein wird.

(ii) Anwenderperspektive

Es wird die Frage aufgeworfen, warum in § 64 Absatz 3 Nr. 1 nicht analog zu § 18 Absatz 1 Nr. 2 zur Klarstellung auf die Einschränkung des Grundrechts der Unverletzlichkeit der Wohnung nach Artikel 13 Absatz 1 GG hingewiesen werde. Erfahrungsgemäß würden inzwischen auch – spätestens seit der Corona-Pandemie – Verarbeitungen, die die JI-Richtlinie unterliegen an mobilen Arbeitsplätzen oder im Home-Office durchgeführt.

Bewertung:

§ 18 Absatz 1 Nr. 2 LDSG bezieht sich nicht auf Privatwohnungen der im Homeoffice tätigen Beschäftigten. Das Grundrecht der Unverletzlichkeit der Wohnung nach Artikel 13 Absatz 1 GG wird nur im Hinblick auf ein Betretungsrecht der Geschäftsräume (privater) Auftragsverarbeiter eingeschränkt, wie sich aus der Gesetzesbegründung ergibt (LT-Drucksache 19/429, S. 148).

Die Landesregierung nimmt diese Rückmeldung zum Anlass, darauf hinzuweisen, dass eine Bearbeitung von Vorgängen, welche dem Anwendungsbereich der JI-Richtlinie zuzurechnen sind (insbesondere Strafanzeigen, aber auch Ordnungswidrigkeitenverfahren), außerhalb von Dienststellen besondere Anforderungen an die Einhaltung des Datenschutzes stellt.

2. Rechtsform der Aufsichtsbehörde

Hinsichtlich der Rechtsform des ULD als rechtsfähige Anstalt des öffentlichen Rechts, auf die die §§ 50-52 LVwG nicht anzuwenden sind, merkt das ULD an, diese Rechtsform sei bislang in keinem anderen Bundesland gewählt worden. Vielmehr seien, größtenteils als Reaktion auf die Entscheidung des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsicht (Rechtssache C-518/07), die Datenschutzaufsichtsbehörden im Bund und in mehreren Ländern als oberste Bundes-

oder Landesbehörden ausgestaltet worden. Die Rechtsform einer obersten Landesbehörde entspreche am ehesten den europarechtlichen Vorgaben und sollte daher auch in Schleswig-Holstein angestrebt werden.

Bewertung:

Wenngleich die Situation zutreffend dargestellt wird, werden die daraus gezogenen Schlüsse nicht geteilt.

Richtig ist, dass die völlige Unabhängigkeit und Weisungsfreiheit der Aufsichtsbehörden aufgrund unionsrechtlicher Gerichtsentscheidungen und auch durch die DSGVO selbst zwingend unionsrechtlich vorgegeben sind. Die Wahl der Rechtsform ist es hingegen nicht. Dass die genannten Ziele nicht auch in der vorliegenden Rechtsform der Anstalt öffentlichen Rechts erreicht werden können, ist nicht dargetan und auch sonst nicht ersichtlich. Die Ausgestaltung des ULD als rechtsfähige Anstalt des öffentlichen Rechts steht mit unionsrechtlichen Vorgaben im Einklang, da durch die landesrechtlichen Anpassungen im Errichtungsgesetz ULD strukturell ein Fehlen jeglicher Aufsicht und Weisungsgebundenheit gewährleistet wird.

Mit den Rundfunkanstalten gibt es andere Anstalten des öffentlichen Rechtes, die unabhängige (Informations-)Aufgaben wahrnehmen, nicht jedoch der mittelbaren Staatsverwaltung zugerechnet werden und dem Gebot der Staatsfreiheit unterliegen (Bethge-Maunz/Schmidt-Bleibtreu, BVerfGG, § 90, 58. EL, Rn. 150 – beck-online). Wegen der im Bereich Presse besonders kritisch zu bewertenden Gefahren durch staatliche Weisungen und Aufsicht besteht hier hinsichtlich der Anforderungen an die Unabhängigkeit eine große Nähe zum ULD. So hat das BVerfG festgestellt, dass der Rundfunk weder den staatlichen Stellen (und erst recht nicht den politischen Parteien) noch einer gesellschaftlichen Gruppierung ausgeliefert werden darf (vgl. BVerfGE 12, 205, 250ff; 31, 314, 325ff.).

Auch die Form als oberste Landes- oder Bundesbehörde wäre nicht vollkommen idealtypisch. So führt der Gesetzesentwurf (BT-Ds. 18/2848, S. 16) zur Ausgestaltung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aus: „Der BfDI ist oberste Bundesbehörde, aber kein Ministerium und nicht Teil der Bundesregierung. Ähnlich wie der Bundesrechnungshof und der Vorstand der Deutschen Bundesbank hat sie eine besondere Stellung, auch wenn eine Verankerung im Grundgesetz nicht notwendig ist. Die Behörde ist unabhängig. Sie ist in keine Struktur eingegliedert, die eine Aufsicht der Exekutive ermöglichen könnte. Die Kontrolle

erfolgt ausschließlich durch die Gerichte und das Parlament“. Auch hier ist eine Anpassung an das „Grundmodell“ nötig, da oberste Bundes-/ Landesbehörden in der Regel Regierungs- und Verwaltungsinstanzen sind, bei denen eine enge Verknüpfung zwischen diesen Aufgaben besteht (Maurer, Allgemeines Verwaltungsrecht, 18. Aufl., § 22, Rn. 19) – und daher politische Einflussnahme strukturell gegeben ist, welche den unionsrechtlichen Vorgaben zur Aufsichtsbehörde entgegensteht

Letztendlich kann es aufgrund dieser Erwägungen keine eindeutige Antwort geben, welches die „geeignetere“ Rechtsform darstellt. Diesbezügliche Probleme sind in der Zeit seit 2018 indes nicht bekannt geworden. Aus Sicht der Landesregierung besteht daher kein Änderungsbedarf. Es spricht allerdings auch nichts gegen die Änderung der Rechtsform in eine oberste Landesbehörde, wenn der Gesetzgeber sich dazu entschließen sollte.

3. Amtsverhältnis

Im Sommer 2020 zeigte sich eine unvorhergesehene Lücke im Zusammenspiel der Regelungen zum Amtsverhältnis der oder des Landesbeauftragten und ihrer oder seiner Stellvertretung. Ein Konkurrent um den Posten der oder des Landesbeauftragten für Datenschutz hatte das Verwaltungsgericht angerufen, um die Ernennung der vom Landtag nach Ablauf der Amtszeit wiedergewählten Amtsinhaberin durch den Ministerpräsidenten zu verhindern.

Nach § 6 Absatz 2 Satz 4 Errichtungsgesetz ULD ist die oder der Landesbeauftragte nach Ablauf der Amtszeit berechtigt, die Geschäfte bis zu Ernennung einer Nachfolgerin oder eines Nachfolgers für die Dauer von höchstens sechs Monaten weiterzuführen. Die Stellvertreterin oder der Stellvertreter führt die Geschäfte nach § 9 Absatz 2 Satz 3 Errichtungsgesetz ULD höchstens sechs Monate nach Ende der Amtszeit der Landesbeauftragten oder des Landesbeauftragten, wenn diese oder dieser nicht gemäß § 6 Absatz 2 Satz 4 die Geschäfte weiterführt.

Bewertung:

Es sollte vorsorglich für die Zukunft eine entsprechende Gesetzesänderung vorgenommen werden. Zwar hat das Schleswig-Holsteinische Verwaltungsgericht im einst-

weiligen Rechtsschutzverfahren entschieden, dass für Konkurrentenklagen bei Ämtern, die durch demokratische Wahlen der Wahlbürger oder durch eine Wahl von von diesen gewählten Wahlkörpern besetzt werden, aus verfassungsrechtlichen Gründen kein Raum besteht. Es sind jedoch auch andere Verhinderungsfälle denkbar, die länger als die gesetzliche Frist andauern und in denen eine Führung der Geschäfte des ULD nicht möglich gewesen wäre.

Zur Lösung bestehen zwei Optionen: Denkbar wäre zum einen die Streichung der Höchstfrist in § 6 Absatz 2 Satz 4, sodass die oder der Landesbeauftragte nach Ablauf der Amtszeit die Geschäfte zeitlich unbegrenzt weiterführen kann. Für den Fall, dass die oder der amtierende Landesbeauftragte die Zeit bis zum Eintritt der Nachfolge zu überbrücken bereit ist, wäre eine Regelung vorzusehen, ob das Amtsverhältnis für diesen Zeitraum weiter aufrechterhalten wird.

Zum anderen könnte die Höchstfrist für die Fortführung der Geschäfte durch die oder den Stellvertreter(in) in § 9 Absatz 2 Errichtungsgesetz ULD gestrichen werden, sodass sie oder er die Geschäftsführung unabhängig vom Zeitablauf bis zur Ernennung einer oder eines neuen Landesbeauftragten wahrnehmen kann. Die Regelung in § 6 Absatz 2 Satz 4 könnte unverändert bleiben. Diese Lösung hätte indes den Nachteil, dass die bisherige Amtsinhaberin oder der Amtsinhaber für die Dauer des Konkurrentenstreits in einem unklaren „Schwebezustand“ gehalten würde. Auch hier wäre zu regeln, ob das Amtsverhältnis (vorübergehend) endet und ob das Verbot mit dem Amt nicht zu vereinbarender entgeltlichen Tätigkeiten aus § 8 Absatz 1 Errichtungsgesetz ULD ausgesetzt wird. Andernfalls würde die oder der wartende bisherige Landesbeauftragte zu einem „unbezahlten Urlaub“ gezwungen, der eine Wiederwahl ggf. deutlich unattraktiver machte. Zudem wäre eine Regelung für den Fall vorzusehen, dass die oder der amtierende Landesbeauftragte, d.h. die bisherige Stellvertretung, während der Zeit der kommissarischen Amtsführung ebenfalls das ULD verlässt. Denn die Stellvertreterin oder der Stellvertreter wird durch die Landesbeauftragte oder den Landesbeauftragten bestellt (§ 9 Absatz 2 Satz 1 Errichtungsgesetz ULD), die oder zu dem fraglichen Zeitpunkt nicht vorhanden wäre. Es wäre daher präventiv eine weitere Stellvertretung zu bestellen, für den Fall, dass die Stellvertreterin oder der Stellvertreter die Führung der Geschäfte übernimmt.

V. Allgemein

Abschließend wurden den Rechtsanwendern drei offene Fragen gestellt, um Erfahrungen abzufragen, die nicht den voranstehenden konkreten Punkten zugeordnet werden können. Hierzu ist eine Vielzahl verschiedener Anmerkungen eingegangen, die im Folgenden knapp dargestellt und bewertet werden.

1. Wie bewerten Sie das LDSG insgesamt in Bezug auf die Sachgerechtheit, Praktikabilität und Normenklarheit der Bestimmungen?

a) Bezugnahme auf zugrundeliegende Vorschriften

Nach § 1 LDSG ergänze das LDSG die EU-Regelungen. Hilfreich sei es, wenn in den einzelnen Vorschriften des LDSG konsequent aufgenommen würde, welche konkreten Regelungen der DSGVO ergänzt werden.

Bewertung:

Ein solches Vorgehen, bei dem auf die jeweiligen Artikel der DSGVO verwiesen wird, wird verschiedentlich im Datenschutzrecht anderer Länder praktiziert, so im Bayerischem Datenschutzgesetz. Auch der Schleswig-Holsteinische Landesgesetzgeber ist in anderen Landesgesetzen bereits so vorgegangen und nimmt etwa in den Paragraphenüberschriften des Landesbeamtengesetzes teilweise Bezug auf die jeweiligen Regelungen des Beamtenstatusgesetzes.

Die angeregte Klarstellung zur Vereinfachung für die Praxis wäre daher nicht ganz unüblich. Sie erscheint allerdings auch nicht zwingend erforderlich, da die Vorschriften des LDSG weitestgehend bereits eingangs des Normtextes auf die jeweilige Vorschrift der DSGVO Bezug nehmen (bspw. § 8 Absatz 1: „Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 oder Artikel 14 Absatz 1, 2 und 4 [DSGVO] besteht ergänzend zu den in Artikel 13 Absatz 4 oder Artikel 14 Absatz 5 [DSGVO] genannten Ausnahmen nicht, wenn…“; ähnlich in §§ 9, 10, 11, 12), sodass keine Unklarheiten aufkommen sollten.

b) Vereinheitlichung von Begrifflichkeiten

Um einen Gleichlauf mit den Begrifflichkeiten der DSGVO zu erreichen, sollte in §§ 3 und 4 besser von „Rechtmäßigkeit“ statt „Zulässigkeit“ gesprochen werden.

Bewertung:

Der Anregung kann nicht gefolgt werden. Die Aufgabenübertragung bzw. die Zulässigkeit der Zweckänderung allein machen die Verarbeitung nicht rechtmäßig. Es handelt sich um erforderliche, aber nicht hinreichende Bedingungen. Auch bei Vorliegen einer übertragenen Aufgabe oder zulässigen Änderung des Verarbeitungszweckes können Verstöße gegen andere zwingende Vorgaben der DSGVO oder des LDSG vorliegen, die die Verarbeitung rechtswidrig machen.

c) Funktion und Bedeutung von § 3 LDSG

Nach den Erfahrungen eines Rechtsanwenders ergäben sich im Kontext des § 3 LDSG Verständnisprobleme. Denn nach Artikel 6 Absatz 1 Buchst. e, Absatz 3 DSGVO i.V.m. dem einschlägigen Landes- oder Bundesrecht seien die grundsätzlichen Verarbeitungstätigkeiten der öffentlichen Stellen auf spezifische Rechtsgrundlagen gestützt. Soll also die Verarbeitung zur Erfüllung einer öffentlichen Aufgabe erforderlich sein, müsse im ersten Schritt die Rechtsgrundlage aus dem Landes- oder Bundesrecht ermittelt werden. Fraglich sei in Bezug auf Artikel 6 Absatz 1 Buchst. e DSGVO, dem die Norm im Wesentlichen entspreche, der eigenständige Regelungsgehalt von § 3 LDSG. Es könnte einiges für einen Verstoß gegen das europarechtliche Normwiederholungsverbot sprechen, was zur Unwirksamkeit des § 3 LDSG führen würde.

Von anderer Stelle wurde zurückgemeldet, § 3 LDSG sei aus Praxissicht erforderlich und sollte daher beibehalten werden, da es nicht immer fachrechtliche Regelungen gäbe, die die Zuständigkeit begründen, und damit nur die Einwilligung für die Rechtmäßigkeit der Verarbeitung bliebe. Eine Einwilligung der betroffenen Person nach Artikel 6 Absatz 1 Buchst. a DSGVO komme allerdings nur ausnahmsweise in Betracht, weil die nach Artikel 4 Ziff. 11 und Artikel 7 Absatz 4 DSGVO erforderliche Freiwilligkeit in der Regel gegenüber Behörden nicht gegeben sei (siehe auch Erwägungsgrund 43).

Bewertung:

Die Landesregierung teil die letztgenannte Auffassung. § 3 LDSG setzt den Regelungsgehalt von Artikel 6 Absatz 1 Buchst. e DSGVO im Anwendungsbereich des LDSG um. Dies ist aufgrund von Artikel 6 Absatz 3 DSGVO erforderlich, da die Rechtsgrundlagen für die in Artikel 6 Absatz 1 Buchst. e DSGVO genannten Verarbeitungen durch das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt werden. Artikel 6 Absatz 1 Buchst. e DSGVO unmittelbar ist hingegen keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen. Die Vorschrift des § 3 LDSG wurde vor diesem Hintergrund als nachrangige allgemeine Rechtsgrundlage geschaffen. Dies gilt insbesondere im Hinblick auf Datenverarbeitungen, für die keine spezialgesetzliche Datenverarbeitungsnorm existiert und für die es auch nicht angezeigt erscheint, eine solche zu schaffen. Aber auch als Auffangnorm für etwaige Lücken im Fachrecht ist § 3 Absatz 1 LDSG unverzichtbar und kann nicht gestrichen werden. Soweit bereichsspezifisches Recht existiert, geht dieses als spezieller vor.

d) § 3 Absatz 2 LDSG

§ 3 Absatz 2 LDSG treffe eine Regelung zu dem „Zweck“ der Verarbeitung. Es sei nicht klar, ob die dort aufgenommenen Zwecke Absatz 1 der Vorschrift ergänzen sollen. Die Regelungsinhalte des § 3 Absatz 2 und § 4 LDSG, die jeweils Regelungen zum Zweck der Verarbeitung personenbezogener Daten treffen, sollten in einer Vorschrift behandelt werden.

Bewertung:

Nach dem Verständnis der Landesregierung ist die Regelungssystematik genau umgekehrt: § 3 Absatz 2 definiert die Reichweite der eigentlichen Aufgabe, indem er die dort genannten Zwecke im Wege einer gesetzlichen Fiktion noch dem ursprünglichen Zweck im Sinne des Absatz 1 zurechnet. In den dort beschriebenen Fällen liegt gerade keine Zweckänderung vor, die Gegenstand von § 4 LDSG ist. § 3 Absatz 2 ist daher systematisch „näher“ an § 3 Absatz 1. Die Regelung erscheint daher sachgerecht.

e) Verteilung der Verantwortlichkeiten durch § 5 LDSG

§ 5 LDSG sollte klarer formuliert werden. Gemäß § 5 Absatz 1 trage die übermittelnde Stelle die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten. Aus dieser Formulierung werde nicht hinreichend deutlich, was darunter zu verstehen sei. So sei fraglich, ob die übermittelnde Stelle (unter Bezugnahme auf Absatz 2) an dieser Stelle prüfen müsse, ob die ersuchende Stelle die Daten rechtmäßig verarbeitet. Unter Zugrundelegung dieses Verständnisses sollte § 5 Absatz 1 deutlicher formuliert werden. Auch § 5 Absatz 2 sei aus sich heraus nicht verständlich.

Bewertung:

Die Einwände können nicht nachvollzogen werden. Da die Übermittlung als Unterfall der Verarbeitung bereits von den Regelungen der DSGVO umfasst ist, enthält das LDSG (abgesehen vom Sonderfall in Absatz 4) hierfür keine eigene Rechtsgrundlage mehr, sondern regelt die datenschutzrechtlichen Pflichten der Beteiligten. Nach Absatz 1 ist der Regelfall, dass die übermittelnde Stelle die Verantwortung für die *Zulässigkeit der Übermittlung* personenbezogener Daten trägt. Normiert wird damit ausdrücklich nur die Übermittlung, nicht die weitere Verarbeitung bei der ersuchenden öffentlichen Stelle. Für die dortige Verarbeitung ist der Empfänger als eigenständiger Verantwortlicher im Sinne des Artikel 4 Nr. 7 DSGVO selbst verantwortlich. Die übermittelnde Stelle könnte die Bewertung der Rechtmäßigkeit der Verarbeitung in der Praxis auch gar nicht leisten, da hierzu bspw. die Datenschutzdokumentation und deren praktische Umsetzung zu prüfen wäre. Es bleibt damit jedenfalls eine öffentliche Stelle für die Verarbeitung von Daten, die von der öffentlichen Hand erhoben wurden, verantwortlich. Bei der Abgabe von Daten von der öffentlichen Hand an Private ist hingegen eine vertiefte Kontrolle angezeigt.

f) Freigabe und Testung automatisierter Verfahren nach § 7 LDSG

Die Reglung des § 7 Absatz 1 LDSG sei nicht stimmig und führe in der Praxis zu Missverständnissen, weil nur zwei (Test und Freigabe) von zahlreichen technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO herausgestellt werden.

Bewertung:

Die Missverständnisse können nicht nachvollzogen werden. Die Vorschrift regelt, dass automatisierte Verfahren vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen hinsichtlich einer wirksamen Umsetzung von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung von dem Verantwortlichen oder einer von ihm beauftragten Person freizugeben sind; das Testverfahren ist zu dokumentieren. Normiert ist damit lediglich das Prozedere bei der Inbetriebnahme bzw. nach gewichtigen Änderungen. Hierzu ist ein Test durchzuführen, der zu dokumentieren ist. Gegenstand der Prüfung ist die wirksame Umsetzung aller erforderlichen technischen und organisatorischen Maßnahmen im Sinne des Artikels 32 DSGVO. Diese müssen selbstredend während der gesamten Nutzung des automatisierten Verfahrens eingehalten werden. Am Ende steht eine förmliche Freigabeentscheidung des Verantwortlichen.

Aus den Vorgaben zum Ablauf der Inbetriebnahme (Testung mit anschließender Freigabe) ist nichts für die jeweils festzusetzenden technischen und organisatorischen Maßnahmen abzuleiten, insbesondere werden diese nicht beschränkt.

g) Verordnung zu Sicherheitskonzepten und Freigabe automatisierter Verfahren

Es wird kritisiert, dass die Landesregierung von den Verordnungsermächtigungen in § 7 Absatz 2 bzw. § 40 Absatz 5 LDSG bislang keinen Gebrauch gemacht hat. Danach regelt die Landesregierung durch Verordnung die Anforderungen an das Sicherheitskonzept sowie die Freigabe automatisierter Verfahren und weitere Einzelheiten einer ordnungsgemäßen Datenverarbeitung durch die öffentlichen Stellen. Die bisherige Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung, DSVO) vom 05.12.2013 ist am 31.12.2018 außer Kraft getreten.

Bewertung:

Die Landesregierung sieht für eine derartige Verordnung derzeit grundsätzlich keinen Bedarf. Das ULD hat „Hinweise zur Dokumentation einer ordnungsgemäßen Verarbeitung personenbezogener Daten“ erarbeitet und auf seinem Internetauftritt veröffentlicht, die demselben Zweck dienen.

Sie ermöglichen es, dass Verantwortliche ihre Verpflichtungen nach Artikel 5 Absatz 1 DSGVO und § 22 LDSG (Grundsätze für die Verarbeitung personenbezogener Daten) erfüllen und gemäß Artikel 5 Absatz 2 DSGVO (Nachweispflicht) einen Nachweis darüber führen. Soweit die Verantwortlichen im Hinblick auf die Konzeption und Durchführung der Verarbeitung und der Wahl technisch-organisatorischer Maßnahmen gemäß Artikel 24, 25 und 32 DSGVO bzw. §§ 40, 47 LDSG einen Gestaltungsspielraum haben, wie sie die Grundsätze für die Verarbeitung personenbezogener Daten erfüllen und dabei Risiken für die Rechte und Freiheiten natürlicher Personen eindämmen, bleibt dieser gewährleistet.

Zwar sind die Hinweise nicht unmittelbar für die Verantwortlichen bindend, wie es eine Landesverordnung wäre. Allerdings handelt es sich um die Prüfungsmaßstäbe der zuständigen Aufsichtsbehörde. Insoweit sollten die Verantwortlichen diese Kriterien ihren Verarbeitungsvorgängen zugrunde legen.

Gleichwohl teilt das ULD mit, dass in der aufsichtlichen Praxis durchaus Fälle aufgetreten sind, in denen Verantwortliche gleichwohl die Anwendung der in den Hinweisen niedergelegten Vorgaben verweigern und bereits die Legitimation des ULD zu solchen Vorgaben bestreiten. Dies ist aus Sicht der Landesregierung nicht nachvollziehbar. Das ULD hat als Aufsichtsbehörde im Sinne des Artikel 51 Absatz 1 DSGVO (vgl. § 17 LDSG) aus der DSGVO umfassende Befugnisse, um auf von ihr für rechtswidrig erachtete Verarbeitungen einzuwirken. Im Sinne der Transparenz ist es zu begrüßen, wenn die von der Aufsichtsbehörde angelegten Maßstäbe nicht erst bei der Einzelfallprüfung angewandt, sondern bereits vorab allgemein publiziert werden, damit Verantwortliche ihre Verarbeitungsvorgänge danach ausrichten können.

Eine Landesverordnung wäre zwar geeignet, diese Unsicherheit zu beseitigen, da hierdurch verbindliches Recht geschaffen würde. Sie gälte jedoch nur für die Verarbeitung durch öffentliche Stellen (vgl. § 7 Absatz 2 Satz 1 LDSG), während die vom ULD veröffentlichten Hinweise einen einheitlichen Maßstab auch für Private darstellen.

Letztlich brächte es auch keinen Zuwachs an Rechtssicherheit, wenn die Landesregierung in einer Verordnung verbindlichen Vorgaben machte, die unabhängige Aufsichtsbehörde diese aber ggf. für unzureichend erachtet und auf Grundlage der eigenen Rechtsauffassung Maßnahmen gegen die Verantwortlichen trifft. Auch sieht das

Zentrale IT-Management der Landesregierung (Abt. 3 des MELUND) keinen fachlichen Bedarf für abweichende eigene Regelungen.

Die Landesregierung wird daher prüfen, ob von der Ermächtigung zum Erlass einer Verordnung Gebrauch gemacht werden soll.

h) Verschwiegenheit von Datenschutzbeauftragten öffentlicher Stellen

Das ULD weist darauf hin, dass die Bestimmungen für Datenschutzbeauftragte öffentlicher Stellen lückenhaft seien. So bestehe im Anwendungsbereich der DSGVO für Datenschutzbeauftragte bisher keine Verschwiegenheitsverpflichtung. Es wird empfohlen, auf Grundlage der Öffnungsklausel in Artikel 38 Absatz 5 DSGVO eine entsprechende Bestimmung in das LDSG aufzunehmen, zumal die Verschwiegenheit für Datenschutzbeauftragte im Anwendungsbereich der JI-Richtlinie in § 59 Absatz 4 LDSG umgesetzt wurde. Für eine unterschiedliche Behandlung der Datenschutzbeauftragten danach, ob die jeweilige öffentliche Stelle Aufgaben nach der DSGVO oder in Umsetzung der JI-Richtlinie wahrgenommen werden, bestünden keine maßgeblichen Gründe. Es wird daher empfohlen, auch hinsichtlich eines Zeugnisverweigerungsrechts und bezüglich eines Beschlagnahmeverbots in Anlehnung an den Wortlaut von § 59 Absatz 5 LDSG eine einheitliche bzw. vergleichbare Regelung zu schaffen.

Bewertung:

Der Hinweis ist zutreffend. Der Anregung sollte gefolgt und eine entsprechende Regelung für den DSGVO-Bereich geschaffen werden. Der geeignete Regelungsstandort innerhalb des LDSG wäre noch zu prüfen.

2. Bestehen in Ihrer datenschutzrechtlichen Praxis Schwierigkeiten mit der Auslegung und Anwendung des LDSG? Wenn ja, welche Schwierigkeiten sind das und auf welche Regelungen des LDSG beziehen sie sich?

a) Funktionsträgerdaten

Eine Rückmeldung äußert Bedarf für eine klarstellende Regelung zum Umgang mit Funktionsträgerdaten. So habe § 21 LDSG a.F. die Zulässigkeit der Veröffentlichung

von Funktionsträgerdaten unter bestimmten Voraussetzungen geregelt, nämlich wenn es sich um Daten von Mandatsträgern oder öffentlich tätigen Personen im Rahmen des Dienst- oder Arbeitsverhältnisses handelt und die schutzwürdigen Belange der Betroffenen an der Geheimhaltung das Veröffentlichungsinteresse nicht überwiegen. In der aktuellen Fassung des LDSG fehle eine entsprechende Regelung.

Bewertung:

Tatsächlich besteht ein großes praktisches Interesse an der Frage. Fast alle öffentliche Stellen veröffentlichen Geschäftsverteilungs- und Organisationspläne, die jedenfalls bis zu einer bestimmten Hierarchieebene personenbezogene Daten von Mitarbeitenden enthalten. Das Bundesverwaltungsgericht hat insoweit zu der Rechtslage vor Inkrafttreten der DSGVO auch entschieden, dass eine Behörde mit Publikumsverkehr grundsätzlich befugt ist, dienstliche Kontaktdaten ihrer Bediensteten zu veröffentlichen, und diese keinen Anspruch darauf haben, von der Möglichkeit der Kontaktaufnahme abgeschirmt zu werden (vgl. BVerwG, Beschluss vom 12. März 2008 - 2 B 131.07 -). Unter Geltung der DSGVO, die für die Rechtmäßigkeit der Verarbeitung eine konkrete Rechtsgrundlage voraussetzt, reicht dies nicht mehr aus.

Nicht-öffentliche Stellen können eine entsprechende Veröffentlichung von Namen, Aufgabengebiet und persönlicher Erreichbarkeit ggf. unter dem Aspekt der Transparenz, Kundenfreundlichkeit oder Öffentlichkeitsarbeit auf den Erlaubnistatbestand der berechtigten Interessen nach Artikel 6 Absatz 1 Buchst. f DSGVO stützen. Diese Möglichkeit besteht für Behörden in Erfüllung ihrer Aufgaben nicht (vgl. Artikel 6 Absatz 1 Unterabsatz 2). Zwar können diese die Veröffentlichung mit Einwilligung der betroffenen Personen nach Artikel 6 Absatz 1 Buchst. a DSGVO vornehmen. Dieses Vorgehen ist indes nicht praktikabel, da die Einwilligung jederzeit ohne Angaben von Gründen widerruflich ist, Artikel 7 Absatz 3 Satz 1 DSGVO. Zu erwägen wäre ferner, ob die Veröffentlichung auf Artikel 6 Absatz 1 Buchst. e DSGVO in Verbindung mit § 3 LDSG gestützt werden kann, wenn sie als Teil der Aufgabenwahrnehmung anzusehen ist.

Denkbar wäre auch eine spezielle Regelung, die nicht zwingend gesetzlich sein muss. Artikel 88 DSGVO ermächtigt die Mitgliedsstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener

Beschäftigtendaten im Beschäftigungskontext zu regeln, sofern dabei der berechtigten Interessen und der Grundrechte der betroffenen Person gewahrt bleiben.

Die Landesregierung wird das weitere Vorgehen prüfen.

b) Technische Fachbegriffe

Die in § 12 Absatz 3 Nr. 6 LDSG und § 40 Absatz 2 Nr. 1 LDSG verwendeten Begriffe der „Fähigkeit“ bzw. „Belastbarkeit“ der Systeme und Dienste seien nicht legaldefiniert. Es wird die Frage aufgeworfen, wie sich diese von dem in den jeweiligen Normen ebenfalls enthaltenen Begriff der „Verfügbarkeit“ der Systeme und Dienste unterscheiden.

Bewertung:

§ 12 Absatz 3 Satz 1 und 2 setzt das Erfordernis aus Artikel 9 Absatz 2 Buchst. b, g und i DSGVO um, „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ bzw. „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorzusehen.

Es handelt sich bei den dort – als nicht abschließende Regelbeispiele, wie sich aus dem Wort „insbesondere“ ergibt – beschriebenen Eigenschaften der eingesetzten Systeme und Dienste um technische und organisatorische Maßnahmen, die in der DSGVO selbst genannt sind, Artikel 32 Absatz 1 Buchst. b) und c), und die im IT-Bereich verbreitet sind. Eine Legaldefinition scheint daher nicht erforderlich. So ist die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können (Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium Edition 2021, Glossar). „Belastbarkeit“ von Systemen und Diensten ist zwar kein klassisches Ziel der IT-Sicherheit. In der englischsprachlichen Originalfassung der DSGVO wird der Begriff „resilience“ verwendet, der in der deutschen Literatur der Informatik regelmäßig mit „Widerstandsfähigkeit“ oder „Ausfallsicherheit“ übersetzt wird (Kühling/Buchner/Jandt, DS-GVO, 3. Aufl. 2020, Art. 32 Rn. 26 mit weiteren Nachweisen).

c) Abgabe an Archive

In der Zusammenarbeit mit Behörden, die gemäß § 6 Absatz 1 Landesarchivgesetz ihre nicht mehr benötigten Unterlagen dem Landesarchiv zur Übernahme anbieten müssen, komme häufig eine Verunsicherung hinsichtlich der Übergabe von (zum Teil sehr sensiblen) personenbezogenen Daten an ein Archiv zum Ausdruck. Es wird daher angeregt, die bereits in anderen Normen (wie z.B. § 91 Absatz 4 LBG) sehr deutlich beschriebene Funktion der Archivierung als Löschungssurrogat auch im LDSG noch deutlicher zu benennen. Dazu böte sich insbesondere § 6 LDSG an.

Bewertung:

Nach Auffassung der Landesregierung handelt es sich bei den geschilderten Vorbehalten der anbietungspflichtigen Stellen vornehmlich um ein Praxisproblem, dass sich durch eine Gesetzesänderung nicht lösen lässt.

§ 6 LDSG regelt insoweit nur das Verfahren. Danach sind öffentliche Stellen vor der Löschung personenbezogener Daten – die in der Regel zu erfolgen hat, sobald sie zur Erreichung des verfolgten Zwecks nicht mehr erforderlich sind – die Unterlagen dem Landesarchiv anzubieten sind. Die Norm unterstützt die Vorgaben aus § 6 Absatz 1 LArchG, wonach die betroffenen Stellen dem Landesarchiv alle Unterlagen, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen, unverzüglich zur Übernahme anzubieten haben.

Denn in dem Moment, in dem die personenbezogenen Unterlagen von den öffentlichen Stellen zur Erfüllung ihrer Aufgaben nicht mehr benötigt werden, sind – gewissermaßen gleichzeitig – erstens die personenbezogenen Daten nach Artikel 5 Absatz 1 Buchst. d), Artikel 17 Absatz 1 Buchst. a) DSGVO zu löschen und zweitens die Unterlagen nach § 6 Absatz 1 LArchG dem Landesarchiv anzubieten.

§ 6 LDSG entzerrt insoweit das Verfahren und regelt, dass die datenschutzrechtlich gebotene Löschung erst dann erfolgen darf, wenn das Landesarchiv über eine Übernahme entschieden hat. So wird gesichert, dass keine archivwürdigen Daten verloren gehen und das Archiv seine gesetzlichen Aufgaben erfüllen kann. Es ist nicht erkennbar, inwieweit eine weitergehende Bekräftigung, dass die Unterlagen inklusive personenbezogener Daten anzubieten sind, noch klarstellend helfen könnte.

d) § 22 LDSG

In § 22 LDSG werden allgemeine Grundsätze für die Verarbeitung personenbezogener Daten im Anwendungsbereich der JI-Richtlinie geregelt, die den Grundsätzen aus Artikel 5 Absatz 1 DSGVO entsprechen.

Sowohl im Hinblick auf die Umsetzung der JI-Richtlinie als auch in der Anwendung des Datenschutzrechts in der Praxis gestalte sich die in § 22 LDSG getroffene Regelung allgemeiner Grundsätze für die Verarbeitung personenbezogener Daten nach Ansicht des ULD problematisch.

So sei Artikel 4 Absatz 4 JI-Richtlinie, der die Rechenschaftspflicht des Verantwortlichen bekräftige, dort nicht umgesetzt. Die Parallelvorschrift des Artikel 5 Absatz 2 DSGVO spiele in der Praxis eine wichtige Rolle. Zur Verdeutlichung der Pflichten der Verantwortlichen sollte die Regelung des Artikel 4 Absatz 4 JI-Richtlinie in den 3. Abschnitt des LDSG aufgenommen werden, regt das ULD an. Es handele sich zwar nur um eine deklaratorische Regelung. Die Erfahrung in der Praxis habe jedoch gezeigt, dass gerade die Pflicht, die Einhaltung der Vorgaben nachzuweisen, nicht allen Verantwortlichen klar sei. Einige Verantwortliche gingen davon aus, dass die Datenschutzaufsichtsbehörde das Vorliegen von Verstößen gegen Datenschutzvorschriften positiv nachweisen müsse. Im Regelfall sei es jedoch umgekehrt: Der Verantwortliche müsse gegenüber der Aufsichtsbehörde die Einhaltung der Vorgaben des Datenschutzrechts nachweisen. Gelingt dies nicht, müsse die Aufsichtsbehörde davon ausgehen, dass das Datenschutzrecht nicht eingehalten sei und daraufhin prüfen, ob Maßnahmen erforderlich sind, um die Verarbeitung in Einklang mit den datenschutzrechtlichen Vorgaben zu bringen.

Bewertung:

Es ergibt sich bereits aus höherrangigen Grundsätzen, dass sich die handelnden Behörden rechtskonform zu verhalten haben. Der Landesregierung ist auch kein Fall bekannt, in dem eine verantwortliche Stelle dem vom ULD geschilderten Missverständnis unterlegen wäre und irrigerweise seine Rechenschaftspflicht für eine ordnungsgemäße Verarbeitung verkannt hätte. Insbesondere wird durch das Fehlen der vom ULD angeregten Regelung keine „Beweislast“ der Aufsichtsbehörde begründet. Die Landesregierung kann daher kein dringendes Bedürfnis für eine rein deklaratorische Ergänzung erkennen.

3. Gibt es aus Ihrer Sicht Anpassungsbedarfe in Fachgesetzen, die aus dem Zusammenspiel von LDSG und bereichsspezifischem Datenschutzrecht herrühren? Wenn ja, welche?

a) Einwilligung als Rechtsgrundlage der Verarbeitung

In den zur Umsetzung der JI-Richtlinie erlassenen Fachgesetzen sei oftmals die Einwilligung als alleinige Rechtsgrundlage für die Verarbeitung personenbezogener Daten vorgesehen. Hierzu habe das ULD jeweils darauf hingewiesen, dass die Einwilligung als alleinige Rechtsgrundlage in der JI-Richtlinie nicht vorgesehen sei. Die in den Erwägungsgründen 35 und 37 der Richtlinie als „Einwilligung“ bezeichnete Beteiligung der betroffenen Person sei weniger als Einwilligung im datenschutzrechtlichen Sinne zu verstehen, sondern als Einbindung der betroffenen Person in den Prozess der Datenverarbeitung (siehe auch oben zu § 27 LDSG). Im Grundsatz sei die Kombination aus gesetzlicher Grundlage und Einwilligung der betroffenen Person auch sinnvoll. Sie gewährleiste, dass die betroffene Person an der Datenverarbeitung mitwirken kann, und verhindere, dass Daten zu ihrer Person ohne ihr Wissen und Wollen verarbeitet werden. Um eine Einwilligung im Sinne des Datenschutzrechts handele es sich dabei indes nicht. Deren Anforderungen seien in § 27 LDSG festgelegt. Die Einwilligung sei nach § 27 Absatz 4 LDSG nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruhe. Dies sei im Bereich der Strafverfolgung und der Gefahrenabwehr kaum möglich; insbesondere stehe das „Ob“ der Verarbeitung in diesem Bereich in der Regel nicht zur Disposition der betroffenen Person. Man habe daher im Gesetzgebungsverfahren zum LDSG angeregt, in § 27 LDSG keine Einwilligung im datenschutzrechtlichen Sinne vorzusehen, sondern vielmehr eine „Zustimmung“ der betroffenen Person. Diese Grundfrage könne nicht in den Fachgesetzen, sondern nur im LDSG gelöst werden. Es komme insbesondere nicht in Frage, den Begriff der Einwilligung in den Fachgesetzen durch den Begriff der Zustimmung zu ersetzen. Denn für die Zustimmung seien keine Anforderungen gesetzlich definiert.

Bewertung:

Die Frage der unterschiedlichen Begrifflichkeiten „Einwilligung“ und „Zustimmung“ wurden nach Auffassung der Landesregierung im Gesetzgebungsverfahren zum LDSG mehrfach und hinreichend gewürdigt.

Das LSDG, mit dem die landesgesetzliche Umsetzung der JI-Richtlinie erfolgt, nutzt insoweit die identische Formulierung wie der europäische Gesetzgeber. Es handelt sich um eine unionsrechtliche Begriffsschöpfung, die in wörtlicher Übersetzung (im Original: „consent“) in nationales Recht übernommen wurde. Dagegen könnte die Verwendung von Begriffen, die von den umzusetzenden unionsrechtlichen Vorgaben abweichen, die Gefahr von Auslegungsschwierigkeiten bzw. Schwierigkeiten der Übertragung eventueller Rechtsprechung europäischer Gerichte zu der fraglichen Formulierung bergen.

Zurückgegriffen werden kann auch auf die nationale Verwendung des Rechtsbegriffs, um die Unterschiede zwischen den Begrifflichkeiten „Einwilligung“ und „Zustimmung“ im rechtlichen Sinne zu klären. Hilfreich kann hier eine Ableitung aus dem Bürgerlichen Gesetzbuch sein. Lt. §§ 183 und 184 BGB handelt es sich bei der vorherigen Zustimmung um eine Einwilligung (vgl. § 183 BGB) und bei der nachträglichen Zustimmung um eine Genehmigung (vgl. § 184 BGB). Insofern ist die „Zustimmung“ als Oberbegriff anzusehen und weitergehender als die Einwilligung. Sie kann daher entgegen dem Vorschlag des ULD nicht synonym verwendet werden, sondern müsste demzufolge sprachlich wieder eingeschränkt werden, um dem in der Richtlinie zugrunde gelegten Gehalt zutreffend zum Ausdruck zu bringen.

Nach Auffassung der Landesregierung gilt es daher, an der Begrifflichkeit „Einwilligung“ festzuhalten.

b) Terminologie in Fachgesetzen

Das ULD weist darauf hin, dass die Terminologie in den Fachgesetzen oftmals noch nicht an das neue Datenschutzrecht angepasst sei. In vielen Fachgesetzen würden noch die Begrifflichkeiten aus dem früheren LDSG verwendet, die mittlerweile jedoch im LDSG nicht mehr enthalten und somit nicht mehr legaldefiniert sind. Dies betreffe insbesondere den Begriff der Verarbeitung. An dessen Stelle würden auch in neuen Fachgesetzen noch häufig die Begriffe „Erheben“, „Speichern“, „Nutzen“ und „Übermitteln“ verwendet. Dieses Problem könne nur in den Fachgesetzen gelöst werden, indem dort die Terminologie aus dem allgemeinen nationalen und europäischen Datenschutzrecht verwendet wird. Für das LDSG ergebe sich kein Änderungsbedarf.

Bewertung:

Der Hinweis ist teilweise zutreffend. Es wurden noch nicht alle Fachgesetze an das neue Datenschutzrecht angepasst. Hierauf wurde dann verzichtet, wenn es sich einzig um die Änderung der Terminologie handeln würde. Bei einer etwaig anstehenden materiellen Gesetzesänderung würde in diesen Fällen auch die zwischenzeitlich auseinanderfallenden Begrifflichkeiten korrigiert. Soweit das ULD die Verwendung in Gesetzen anspricht, die seit Inkrafttreten des neuen LDSG überhaupt oder auch gerade in den Vorschriften zur Verarbeitung personenbezogener Daten geändert wurden, ist die Frage im Gesetzgebungsverfahren berücksichtigt worden. In diesen Fällen werden die einzelnen Verarbeitungsschritte nur noch dann verwendet, wenn bewusst auf sie abgestellt wird. Also wenn nicht jegliche Form der Verarbeitung im Sinne des Artikels 4 Nr. 2 DSGVO bzw. § 21 Nr. 2 LDSG gemeint ist, sondern ausdrücklich nur das genannte Erheben, Speichern usw.