Landtag von Baden-Württemberg **Drucksache 17 / 7596**

17. Wahlperiode **8.10.2024**

Mitteilung

der Landesregierung

Bericht der Landesregierung zu einem Beschluss des Landtags; hier: Evaluationsbericht zum Landesdatenschutzgesetz

Landtagsbeschluss

Der Landtag hat am 6. Juni 2018 das Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 verabschiedet. Artikel 20 sieht darin vor (vgl. Gesetzesbeschluss Drucksache 16/4203):

„Die Auswirkungen von Artikel 1 dieses Gesetzes werden nach einem Erfahrungszeitraum von zwei Jahren durch die Landesregierung unter Mitwirkung der oder des Landesbeauftragten für den Datenschutz, der kommunalen Landesverbände und gegebenenfalls weiterer sachverständiger Personen überprüft. Die Landesregierung unterrichtet den Landtag über das Ergebnis der Überprüfung.“

Bericht

Mit Schreiben vom 8. Oktober 2024, Az.: STM14-055-1/4/16, berichtet das Staatsministerium wie folgt:

Bezugnehmend auf Artikel 20 des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 vom 12. Juni 2018 (GBl. S. 173, 192) darf ich Ihnen anliegend den Evaluierungsbericht zum Landesdatenschutzgesetz nebst Anlagen übersenden.

Eingegangen: 8.10.2024 / Ausgegeben: 6.11.2024

Anlage 1

Baden-Württemberg
MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN

Evaluierung des Landesdatenschutzgesetzes vom 12. Juni 2018

Abschlussbericht zu der Überprüfung der Auswirkungen

des Landesdatenschutzgesetzes

unter Mitwirkung

des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

und der kommunalen Landesverbände

Stand: Juli 2024

Inhalt

Abkürzungsverzeichnis

AGVwGO	Gesetz zur Ausführung der Verwaltungsgerichtsordnung
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BITBW	Landesoberbehörde IT Baden-Württemberg
BITBWG	Gesetz zur Errichtung der Landesoberbehörde IT Baden-Württemberg – Errichtungsgesetz BITBW
1. BMeldDÜV	Verordnung zur Durchführung von regelmäßigen Datenübermittlungen zwischen Meldebehörden
2. BMeldDÜV	Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden an Behörden oder sonstige öffentliche Stellen des Bundes
BMG	Bundesmeldegesetz
BVerfG	Bundesverfassungsgericht
BVerGE	Entscheidungen der amtlichen Sammlung des Bundesverfassungsgerichts
DSFA	Datenschutz-Folgenabschätzung
DSGVO	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)
EHDS-VO	Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten
EuGH	Europäischer Gerichtshof
f.	Folgende Seite
ff.	Folgende Seiten
GDNG	Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens – Gesundheitsdatennutzungsgesetz

GRCh	Charta der Grundrechte der Europäischen Union
HTTPS	Hypertext Transfer Protocol Secure
ITEG	Gesetz über die Möglichkeit des Einsatzes von datengetriebenen Informationstechnologien bei öffentlich-rechtlicher Verwaltungstätigkeit – IT-Einsatz-Gesetz
JI-Richtlinie	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
KAG	Kommunalabgabengesetz
KI	Künstliche Intelligenz
KI-Verordnung	Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)
KlimaG BW	Klimaschutz- und Klimawandelanpassungsgesetz Baden-Württemberg
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
LDSG	Landesdatenschutzgesetz
LDSG a. F.	Landesdatenschutzgesetz alter Fassung
LDSG-JB	Gesetz zum Schutz personenbezogener Daten bei der Verarbeitung durch die Justizbehörden des Landes zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ahndung von Ordnungswidrigkeiten oder zum Zwecke der Strafvollstreckung sowie durch die Behörden des Landes zum Zwecke der Ahndung von Ordnungswidrigkeiten – Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden
LfDI	Landesbeauftragter für den Datenschutz und die Informationsfreiheit

LHG	Gesetz über die Hochschulen in Baden-Württemberg – Landeshochschulgesetz
LIFG	Gesetz zur Regelung des Zugangs zu Informationen in Baden-Württemberg – Landesinformationsfreiheitsgesetz
LKHG	Landeskrankenhausgesetz Baden-Württemberg
LKrebsRG	Gesetz über die Krebsregistrierung in Baden-Württemberg – Landeskrebsregistergesetz
LT-Drs.	Landtagsdrucksache
LStatG	Landesstatistikgesetz
LVwVfG	Verwaltungsverfahrensgesetz für Baden-Württemberg - Landesverwaltungsverfahrensgesetz
MStV	Medienstaatsvertrag
ÖGDG	Gesetz über den öffentlichen Gesundheitsdienst – Gesundheitsdienstgesetz
openJur	Freie juristische Fachdatenbank
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen – Onlinezugangsgesetz
PolG	Polizeigesetz
RegMoG	Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze – Registermodernisierungsgesetz
SGB VIII	Sozialgesetzbuch (SGB) - Achtes Buch (VIII) - Kinder- und Jugendhilfe
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz
SSL	Secure Sockets Layer
SWR	Südwestrundfunk
TB	Tätigkeitsbericht
TDDDG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten – Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz

TLS	Transport Layer Security
TOM	Technische und organisatorische Maßnahmen
TTDSG	Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien
VwVfG	Verwaltungsverfahrensgesetz

A. Grundlagen

I. Einleitung

Am 21. Juni 2018 ist das neue Landesdatenschutzgesetz (LDSG) in Kraft getreten. Es wurde als Artikel 1 des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 vom 12. Juni 2018 (GBl. S. 173) verkündet.

In diesem Gesetz wurde eine Evaluierung des LDSG wie folgt vorgesehen:

„Überprüfung der Auswirkungen des Gesetzes

Die Auswirkungen von Artikel 1 dieses Gesetzes werden nach einem Erfahrungszeitraum von zwei Jahren durch die Landesregierung unter Mitwirkung der oder des Landesbeauftragten für den Datenschutz, der kommunalen Landesverbände und gegebenenfalls weiterer sachverständiger Personen überprüft. Die Landesregierung unterrichtet den Landtag über das Ergebnis der Überprüfung.“

Die Landesregierung berichtet im Folgenden über die Durchführung und das Ergebnis der Evaluierung.

II. Zielsetzung

Mit dem Landesdatenschutzgesetz vom 12. Juni 2018 hat der Landesgesetzgeber das allgemeine Datenschutzrecht an die seit dem 25. Mai 2018 geltende Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, im folgenden DSGVO)[1] angepasst. Da die DSGVO unmittelbar geltendes Recht darstellt, hatte der Landesgesetzgeber nur die Befugnis zu eigenen Regelungen, soweit die DSGVO hierfür Öffnungsklauseln oder Regelungsaufträge enthält. Ziel des LDSG war es mithin, im Anwendungsbereich der DSGVO ergänzende und konkretisierende Regelungen zur DSGVO zu treffen, die im Rahmen der in der DSGVO normierten Spezifizierungsermächtigungen zulässig sind. Dabei sollte der bestehende Gestaltungsspielraum genutzt werden. Die ergänzenden Regelungen sollten der öffentlichen Verwaltung und anderen öffentlichen Stellen ausreichenden Spielraum für die Erfüllung ihrer Aufgaben im öffentlichen Interesse geben und dabei die schutzwürdigen Interessen der betroffenen Personen wahren.

Des Weiteren waren Regelungen für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, zu treffen.

Die Evaluierung dient dazu, festzustellen, ob sich die Regelungen des LDSG entsprechend der beschriebenen Zielsetzung bewährt haben. Es war also festzustellen, ob der Regelungs- und damit Gestaltungsspielraum der DSGVO durch den Landesgesetzgeber im Hinblick auf Zweckmäßigkeit und Praktikabilität sinnvoll ausgenutzt wurde. Dabei waren zum einen die praktischen Bedürfnisse der öffentlichen Stellen zur Verarbeitung personenbezogener Daten, zum anderen die schutzwürdigen Interessen der betroffenen Personen zu berücksichtigen.

Als ein weiterer Gesichtspunkt der Evaluierung wurde die Normenklarheit untersucht.

[1] 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) (ABl. L 119 vom 4.5.2016, S. 1, zuletzt ber. ABl. L 74 vom 4.3.2021, S. 35).

III. Vorgehensweise

Das Innenministerium hat als zuständiges Ministerium für das allgemeine Datenschutzrecht die Ressorts einschließlich dem nachgeordneten Bereich, den Rechnungshof und den Landtag um ihre Bewertung des LDSG gebeten.

Daneben erhielt der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) entsprechend dem Evaluierungsauftrag Gelegenheit zur Stellungnahme. Einbezogen wurde als weitere Aufsichtsbehörde der Rundfunkbeauftragte für den Datenschutz beim SWR.

Die kommunalen Landesverbände wurden ebenfalls entsprechend dem Evaluierungsauftrag beteiligt. Der Gemeindetag und der Landkreistag haben eine gemeinsame Stellungnahme abgegeben. Die Stellungnahme vom 29. Oktober 2021 ist als Anlage beigefügt.

Der LfDI hat an der Evaluierung mitgewirkt. Seine erste Stellungnahme, in der er Vorschläge zur Änderung des LDSG vorlegte, stammt vom 6. November 2020. Im weiteren Verlauf wurden ihm im November 2021 alle eingegangenen Stellungnahmen vorgelegt. Am 13. Februar 2024 erfolgte die Bewertung des LfDI bezüglich der vorgelegten Stellungnahmen. Dabei bezog der LfDI seine erste Stellungnahme ein und überprüfte seine Positionen. Beide Stellungnahmen des LfDI sind als Anlage beigefügt.

Der damalige Rundfunkbeauftragte für den Datenschutz beim SWR, Herr Prof. Dr. Armin Herb, legte seine Stellungnahme am 30. Oktober 2020 vor.

Die Stellungnahmen des Landtags und des Rechnungshofs gingen im November 2020 ein.

Da das LDSG nur das Datenschutzrecht der öffentlichen Stellen normiert, wurde die Wirtschaft nicht an der Evaluierung beteiligt. Im Rahmen der Überprüfung der Forschungsregelung fanden die Anliegen des Forums Gesundheitsstandort Baden-Württemberg einschließlich deren Sprecherinnen und Sprecher Eingang in die Evaluierung.

Die Personal- und Interessenvertretungen der Beschäftigten wurden beteiligt. Sie haben keine Stellungnahme abgegeben.

Aus den eingegangenen Stellungnahmen konnten die Themenbereiche identifiziert werden, die der Überprüfung unterzogen wurden. Eine Überprüfung sämtlicher Vorschriften des LDSG wurde nicht als zielführend angesehen.

11

Der Evaluierungsbericht stellt die Anregungen, Vorschläge und die Kritik aus den eingegangenen Stellungnahmen dar und setzt sich mit ihnen unter Berücksichtigung der Stellungnahme des LfDI auseinander. Es werden schließlich Änderungs- und Ergänzungsvorschläge unterbreitet.

B. Rechtliche Ausgangslage

Mit der DSGVO hat der europäische Gesetzgeber die Mitgliedstaaten, infolgedessen auch das Land Baden-Württemberg, vor die Aufgabe gestellt, das bis dato geltende allgemeine Datenschutzrecht, geregelt im LDSG für die öffentlichen Stellen, an die neue Rechtslage anzupassen. Als Verordnung beansprucht die DSGVO unmittelbare Geltung in allen Mitgliedstaaten. Die wesentlichen datenschutzrechtlichen Anforderungen ergeben sich aus der DSGVO. Die Regelungen der DSGVO durften aus europarechtlichen Gründen nicht in das LDSG übernommen werden.

Im Folgenden wird der dem Landesgesetzgeber infolge dieser europarechtlich geprägten Ausgangslage verbleibende Regelungsspielraum für das allgemeine Datenschutzrecht näher erläutert.

I. Der Anwendungsvorrang des europäischen Rechts

Die DSGVO hat die Richtlinie 95/46/EG (sog. Datenschutz-Richtlinie) abgelöst. Mit dieser war das Datenschutzrecht bereits europarechtlich geprägt. Die nationalen Gesetzgeber mussten aber, um diesem europäischen Datenschutzrecht Geltung zu verschaffen, die Richtlinie in eigenen Rechtsvorschriften umsetzen. Das LDSG alter Fassung (LDSG a. F.) hatte diese Richtlinie umfassend umgesetzt[2].

Die DSGVO beansprucht dagegen gemäß Artikel 288 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) allgemeine Geltung; sie ist „in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat“. Damit sind alle Rechte und Pflichten unmittelbar aus der DSGVO zu entnehmen. Weiter folgt hieraus ein Anwendungsvorrang der Verordnung: Widersprechende nationale Datenschutzvorschriften treten hinter die DSGVO zurück und dürfen nicht mehr angewendet werden. Des Weiteren bedarf es keiner nationalen Vorschriften mehr zur Umsetzung der DSGVO (außer dort, wo sie die DSGVO selbst vorsieht oder erlaubt). Das nationale Datenschutzrecht muss vielmehr an die Verordnung angepasst werden.

Für das vom Landesgesetzgeber zu regelnde allgemeine Datenschutzrecht, das im LDSG niedergelegt ist, bedeutet dies, dass Abweichungen des Landesgesetzgebers von der DSGVO nur zulässig sind, soweit die DSGVO dies durch sogenannte Spezifizierungsklauseln, auch Öff-

[2] Gesetz zum Schutz personenbezogener Daten (LDSG – LDSG) in der Fassung vom 18. September 2000 (GBl. S. 648), zuletzt geändert durch Gesetz vom 7. Februar 2011 (GBl. S. 43).

nungsklauseln genannt, erlaubt. Ferner, dass das LDSG lediglich ergänzende oder konkretisierende Regelungen enthalten kann, die wesentlichen Vorschriften jedoch der DSGVO selbst zu entnehmen sind.

Die Verankerung der DSGVO im europäischen Primärrecht, nämlich in Artikel 16 AEUV sowie in Artikel 7 (Achtung des Privat- und Familienlebens) und Artikel 8 (Schutz personenbezogener Daten) der Charta der Grundrechte der Grundrechte der Europäischen Union (GRCh)[3], wirkt sich auch auf das Verhältnis zum nationalen Datenschutzrecht aus. So sind mitgliedstaatliche Behörden und Gerichte von Anfang an bei der Auslegung und Anwendung der DSGVO an Artikel 7 und 8 GRCh gebunden. Kollisionen mit anderen Grundrechten nach der Grundrechtecharta, z. B. mit der Freiheit der Meinungsäußerung und Informationsfreiheit, der Forschungsfreiheit, dem Recht auf Achtung der Wohnung und der Kommunikation oder der unternehmerischen Freiheit sind auf der Ebene der Grundrechtecharta unter Beachtung des Verhältnismäßigkeitsgrundsatzes zu lösen[4].

Folgendes ist grundsätzlich voranzustellen:

1. Grundsätze der DSGVO

Die Grundsätze der DSGVO sind bei jeder Datenverarbeitung zu beachten. Die Grundsätze sind in Artikel 5 Absatz 1 DSGVO niedergelegt und werden in weiteren Vorschriften der Datenschutz-Grundvorschrift konkretisiert. Diesen Grundsätzen ist das LDSG verpflichtet. Die Vorschriften des LDSG sind daher immer im Lichte der Grundsätze nach der DSGVO auszulegen.

Die Grundsätze lauten:

- Grundsatz der Rechtmäßigkeit (Konkretisierung in Artikel 6 Absatz 1 DSGVO),
- Transparenzprinzip (Konkretisierung in Artikel 7 Absatz 2, Artikel 12 bis 15, 34 DSGVO),
- Zweckbindungsgrundsatz (Konkretisierung in Artikel 6 Absatz 4 DSGVO),
- Grundsatz der Datenminimierung (Konkretisierung in Artikel 25 DSGVO: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen),

[3] Charta der Grundrechte der Europäischen Union, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12016P/TXT&from=DE.
[4] Vgl. Erwägungsgrund 4 der DSGVO.

- Grundsatz der Richtigkeit (Konkretisierung in Artikel 16, 19 DSGVO),
- Grundsatz der Speicherbegrenzung (Konkretisierung in Artikel 17, 18 DSGVO),
- Grundsatz der Integrität und Vertraulichkeit (Konkretisierung in Artikel 32 DSGVO: Sicherheit der Verarbeitung).

Schließlich ist als allen genannten Grundsätzen übergeordnet der Grundsatz der Erforderlichkeit zu erwähnen. Dieser folgt aus dem in Artikel 8 GRCh garantierten Recht des Einzelnen auf den Schutz seiner personenbezogenen Daten und der Tragweite der garantierten Rechte gemäß Artikel 52 GRCh. Jede Verarbeitung personenbezogener Daten setzt daher die Prüfung voraus, ob es dieses Personenbezugs überhaupt bedarf.

2. Ergänzende Regelungen im LDSG

Die wesentlichen materiellen Anforderungen an die Verarbeitung personenbezogener Daten sowie deren Überwachung ergeben sich aus der DSGVO. Die hierzu im LDSG getroffenen Regelungen ergänzen und konkretisieren die DSGVO.

Dies betrifft insbesondere:

- § 3 LDSG: Die Anforderungen an die Sicherstellung des Datenschutzes folgen aus Artikel 32 DSGVO.
- §§ 4 bis 7 und §§ 12 bis 19 LDSG: Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten einschließlich der Verarbeitung zu anderen Zwecken konkretisieren Artikel 6 DSGVO.
- §§ 8 bis 11 LDSG: Die Betroffenenrechte sind in Artikel 12 bis 22 DSGVO geregelt. Das LDSG regelt nur Beschränkungen.
- §§ 20 bis 24, § 27 LDSG: Die Artikel 51 bis 54 DSGVO schreiben die Einrichtung der Aufsichtsbehörden, ihre Unabhängigkeit und ihre Organisation vor. Das LDSG regelt dementsprechend die Rechtsstellung des LfDI und des Rundfunkbeauftragten für den Datenschutz.
- § 25 LDSG: Die Aufgaben und Befugnisse der Aufsichtsbehörden sind in Artikel 57 und 58 DSGVO niedergelegt. Zusätzlich geregelt wird die Zuständigkeit des LfDI als Aufsichtsbehörde für Datenverarbeitungen nichtöffentlicher Stellen sowie außerhalb

des Anwendungsbereichs der DSGVO. Des Weiteren war ergänzend das Verfahren bei Ausübung der Befugnisse zu regeln.

- §§ 28, 29 LDSG: In Ergänzung zu Artikel 83 und 84 DSGVO wurden Regelungen zur Sanktionierung eingefügt.

3. Spezifizierungen im Rahmen der DSGVO

Der Landesgesetzgeber konnte, wie gesehen, nur eingeschränkt unter Nutzung der Spezifizierungsklauseln der DSGVO eigene Regelungen treffen.

Dementsprechend enthält das LDSG dort keine Regelungen, wo die DSGVO abschließend die Voraussetzungen geregelt hat. Abschließend in diesem Sinne sind folgende Regelungen der DSGVO:

- die Regelungen zur Datenverarbeitung aufgrund einer Einwilligung und deren Anforderungen (Artikel 6 Absatz 1 Unterabsatz 1 Buchst. a in Verbindung mit Artikel 7)
- die Regelungen zum Verzeichnis über Verarbeitungstätigkeiten (Artikel 30),
- die Regelung zur gemeinsamen Datenverarbeitung (Artikel 26),
- zur Datenübermittlung in das Ausland (Artikel 44 bis 50),
- die Bußgeldtatbestände (Artikel 83).

Sofern die Verordnung Regelungsaufträge und -ermächtigungen enthält, die die Mitgliedsstaaten für eigene Regelungen nutzen können oder müssen, hat der Landesgesetzgeber diese wie folgt genutzt:

- Im Interesse des Gemeinwohls oder zum Schutz der Interessen Einzelner werden in § 5 LDSG die Zweckbindung sowie in den §§ 8 bis 11 LDSG die Betroffenenrechte der DSGVO beschränkt. Die Berechtigung zur Beschränkung der Zweckbindung sowie der Betroffenenrechte ergibt sich aus Artikel 6 Absatz 4 und Artikel 23 Absatz 1 DSGVO, sofern es sich unter Beachtung des Wesensgehalts der Grundrechte und Grundfreiheiten um eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft handelt, die den in den Buchstaben a bis j definierten Zielen dient. Es handelt sich hierbei im Wesentlichen um die Wahrung nationaler Interessen (Buchst. a, b), den Schutz der öffentlichen Sicherheit (Buchst. c) sowie die Sicherung der Strafverfolgung (Buchst. c) und von Gemeinwohlinteressen (Buchst. e), aber auch um den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen (Buchst. i), die Ausübung von Kontroll- und Überwachungsfunktionen sowie die

Durchsetzung zivilrechtlicher Ansprüche (Buchst. j). Wie Artikel 23 Absatz 1 DSGVO ausführt, stehen die Beschränkungen unter dem Vorbehalt, dass der Wesensgehalt der Grundrechte und Grundfreiheiten geachtet und sie geeignet und verhältnismäßig sind.

- Die Vorschriften zu den Aufsichtsbehörden, §§ 20 bis 27 LDSG, enthalten die notwendigen Regelungen zur Ausfüllung der Vorgaben der DSGVO an unabhängige Aufsichtsbehörden entsprechend Artikel 51ff. DSGVO.

- Gemäß der Ermächtigung in Artikel 83 Absatz 7 DSGVO hat der Landesgesetzgeber die Verhängung von Geldbußen gegen öffentliche Stellen in § 28 LDSG ausgeschlossen. Die Strafvorschrift in § 29 LDSG stellt eine weitere von Artikel 84 DSGVO geforderte Sanktion neben den Bußgeldvorschriften des Artikels 83 DSGVO dar.

- Weitere Öffnungsklauseln enthält die DSGVO, um konkurrierenden Grundrechten oder überragenden öffentlichen Interessen Rechnung zu tragen, und zwar in Artikel 85 DSGVO zum Schutz der Freiheit der Meinungsäußerung und der Informationsfreiheit, in Artikel 86 DSGVO für den Zugang der Öffentlichkeit zu amtlichen Dokumenten, in Artikel 88 DSGVO zur Datenverarbeitung im Beschäftigungskontext, in Artikel 89 DSGVO zum Schutz der Forschungsfreiheit, (zuzüglich statistischer und öffentlicher Archivzwecke) sowie in Artikel 90 DSGVO zum Schutz von Geheimhaltungspflichten. Der Landesgesetzgeber hat diese Öffnungsklauseln in den §§ 12 bis 19 sowie in § 25 Absatz 5 LDSG entsprechend genutzt.

4. Wiederholungsverbot

Aus dem Anwendungsvorrang und dessen Zweck heraus hat der Europäische Gerichtshof für die nationale Gesetzgebung ein Wiederholungsverbot statuiert. Der Anwendungsbefehl des Unionsrechts soll nicht durch mitgliedstaatliche Regelungen verdeckt werden. Wenn ein Mitgliedstaat die Bestimmungen einer unmittelbar geltenden Verordnung in nationales Recht übernehmen würde, würde damit die Zuständigkeit des Europäischen Gerichtshofs in Frage gestellt und somit wäre eine einheitliche Anwendung der Verordnung in der EU nicht mehr gewährleistet.

Was bereits in der DSGVO geregelt ist, darf also im LDSG nicht wiederholt werden, es sei denn, dies ist notwendig, „um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen“[5].

[5] Vgl. Erwägungsgrund 8 der Datenschutz-Grundverordnung.

Der Anwender des Gesetzes ist also aufgerufen, das LDSG immer mit Bezug auf die DSGVO und in deren Kontext zu lesen und anzuwenden.

II. Vorrang des bereichsspezifischen Datenschutzrechts

In einigen Anwendungsbereichen der Landesverwaltung findet das LDSG nur eingeschränkt Anwendung, da bereichsspezifische Vorschriften bestehen, die vorrangig sind. Der Vorrang des bereichsspezifischen Datenschutzrechts ist in § 2 Absatz 3 LDSG ausdrücklich normiert. Er bezieht sich auf das Rechtsregime der DSGVO; das Datenschutzrecht der Polizeibehörden ist in Bezug auf die polizeiliche Tätigkeit der Verhütung und Verfolgung von Straftaten gesondert geregelt.

1. Rechtliche Begründung

Die Notwendigkeit bereichsspezifischer Datenschutzgesetzgebung ergibt sich aus Folgendem:

- Das Recht auf Datenschutz ist in Artikel 8 GRCh verbürgt. Artikel 52 Absatz 1 GRCh bestimmt: „Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“.

- In Ausfüllung der Grundrechtecharta bestimmt die DSGVO in Artikel 6 Absatz 3 DSGVO die Anforderungen an die Datenschutzgesetzgebung für die staatliche Rechtsanwendung. Die Rechtsgrundlagen für die Datenverarbeitung müssen danach im Unionsrecht oder im Recht der Mitgliedstaaten bestimmt werden. Ferner muss der Zweck der Verarbeitung in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Artikel 6 Absatz 1 Buchst. e DSGVO für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Das Recht der Mitgliedstaaten muss ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck dienen.

- Grundlegend ist des Weiteren die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Doppeltürmodell[6], das als Leitbild für den Datenaustausch zur staatlichen Aufgabenwahrnehmung jeweils eigene Rechtsgrundlagen für die korrespondierenden Eingriffe der Datenanforderung und der Datenübermittlung verlangt.

- Des Weiteren erfordern der Grundrechtsschutz verschiedener Tätigkeiten spezifische Datenschutzregelungen. Dies betrifft insbesondere Tätigkeiten, die sich auf die Freiheit der Wissenschaft, die Freiheit der Medien, die Meinungs- und Informationsfreiheit stützen. Die DSGVO sieht in den Artikeln 85 ff. entsprechende Privilegierungen vor.

- In einigen Regelungsbereichen hatte der europäische Gesetzgeber keine Zuständigkeit für eine Regelung durch Verordnung.

2. Bereichsspezifisches Datenschutzrecht

Im Folgenden wird ein Überblick über das bereichsspezifische Datenschutzrecht gegeben.

a) Fachgesetzliche Regelungen

Den obigen Anforderungen des Artikels 6 Absatz 2 und 3 DSGVO entsprechend finden sich datenschutzrechtliche Rechtsgrundlagen in bereichsspezifischen Gesetzen, und zwar je nach Gesetzgebungskompetenz in Bundes- oder Landesvorschriften. Zu nennen sind als bundesrechtliche Vorschriften beispielsweise die Vorschriften für die Sozialbehörden in den Sozialgesetzbüchern (z. B. SGB VIII und SGB X), für die Finanzbehörden in der Abgabenordnung, für die Meldebehörden im Bundesmeldegesetz (BMG) und den Bundesmeldedatenübermittlungsverordnungen (1. BMeldDÜV und 2. BMeldDÜV). Für den Bereich der amtlichen Statistik enthält das Bundesstatistikgesetz bereichsspezifische Datenschutznormen.

Bereichsspezifische Datenschutzvorschriften in Landesgesetzen finden sich unter anderem im Landeshochschulgesetz (LHG)[7], im Klimaschutz- und Klimawandelanpassungsgesetz Baden-Württemberg (KlimaG BW)[8], im Gesetz über den öffentlichen Gesundheitsdienst (ÖGDG)[9]

[6] Vgl. BVerfG, Beschluss des Ersten Senats vom 24. Januar 2012 - 1 BvR 1299/05 -, Rn. 1-192, abrufbar unter https://www.bverfg.de/e/rs20120124_1bvr129905.html, BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 -, Rn. 1-275, abrufbar unter https://www.bverfg.de/e/rs20200527_1bvr187313.html.
[7] Vgl. § 12 LHG.
[8] Vgl. § 33 KlimaG BW.
[9] Vgl. §§ 17, 18 ÖGDG.

im Landeskrankenhausgesetz (LKHG)[10], im Landeskrebsregistergesetz (LKrebsRG)[11], im Kommunalabgabengesetz (KAG)[12], im Landesstatistikgesetz[13] (LStatG).

b) Spezielle Regelungen für grundrechtlich geschützte Tätigkeiten

Die erwähnten grundrechtlich geschützten Bereiche sind, sofern sie nicht Eingang in das LDSG gefunden haben, bereichsspezifisch geregelt. Zu nennen sind hier auf das Land bezogen für den Medienbereich das Landespressegesetz [14] sowie das Landesmediengesetz (LMedienG)[15] ebenso wie der Medienstaatsvertrag (MStV)[16], für den Forschungsbereich neben § 13 LDSG das Landeskrebsregistergesetz[17]. Das Landesinformationsfreiheitsgesetz (LIFG) regelt im Besonderen das Verhältnis von Informationsfreiheit und Datenschutz[18].

III. Regelungen außerhalb des Anwendungsbereichs der DSGVO

Bereichsspezifisches Datenschutzrecht findet sich ferner in Rechtsgebieten, die vom sachlichen Anwendungsbereich der DSGVO und dementsprechend, wie in § 2 Absatz 1 und 5 LDSG normiert, vom Anwendungsbereich des LDSG ausgenommen sind.

- Dies betrifft zum einen den Verfassungsschutz sowie den Vollzug des Landessicherheitsüberprüfungsgesetzes.

- Auch im Bereich der Justiz ist das LDSG größtenteils nicht anwendbar. Es bestehen spezielle Vorschriften für die justizielle Tätigkeit in den jeweiligen Prozessordnungen oder im LDSG für Justiz- und Bußgeldbehörden (LDSG-JB). Gemäß § 2 Absatz 5 LDSG gilt das LDSG für die Gerichte nur für die Tätigkeit in Verwaltungsangelegenheiten.

- Der Datenschutz für die Polizei ist in Umsetzung der Richtlinie (EU) 2016/680 im Polizeigesetz (PolG) und ggf. in der Strafprozessordnung geregelt, soweit die Datenverarbeitung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit dient.

[10] Vgl. §§ 43 bis 49 LKHG.
[11] Vgl. §§ 9 bis 12 LKrebsRG.
[12] Vgl. § 3a KAG.
[13] Vgl. § 14 LStatG
[14] Vgl. § 12 Landespressegesetz.
[15] Vgl. § 49 LMedienG.
[16] Vgl. §§ 23, 113 MStV.
[17] Vgl. § 9 LKrebsRG.
[18] Vgl. § 5 LIFG.

- Das LDSG subsumiert auch in Bezug auf den Landtag nur dessen Verwaltungstätigkeit unter den Anwendungsbereich. Ob die zugrundliegende Annahme, dass die DSGVO die parlamentarische Tätigkeit des Landtags nicht erfasst, zutreffend ist, bedarf infolge neuerer Rechtsprechung der Überprüfung.

- Für die Verfolgung und Ahndung von Straftaten und Ordnungswidrigkeiten findet ebenfalls das LDSG keine Anwendung. Hier gilt das LDSG-JB sowie die vorrangigen bundesrechtlichen Vorschriften der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten.

IV. Europäisches Datenschutzrecht

Zunehmend wird das Datenschutzrecht auch durch (bereichsspezifische) europäische Gesetzgebung geprägt.

Mit der Datenverordnung[19], dem Daten-Governance-Rechtsakt[20], der KI-Verordnung[21] und weiteren Vorhaben zur Schaffung europäischer Datenräume sollen die Grundrechte und Grundfreiheiten der Bürgerinnen und Bürger und die Chancen europäischer Unternehmen gestärkt werden und der Datenzugang, insbesondere für Nutzer und Dritte geregelt werden. Alle diese Vorhaben berühren auch den Umgang mit personenbezogenen Daten und verlangen eine Weiterentwicklung des Datenschutzes.

Die Datennutzung zu ermöglichen und gleichzeitig den Datenschutz der Bürgerinnen und Bürger zu gewährleisten, ist die Herausforderung, die sich in diesem Zusammenhang stellt. Der Landesgesetzgeber ist hier gefordert, sofern eigene Regelungsspielräume bestehen, einen Ausgleich zu schaffen. Dies ist die Aufgabe eines gestaltenden Datenschutzes, für den sich das Land besonders einsetzt, bezogen insbesondere auf den Bereich der Gesundheitsdatennutzung für die Forschung wie auch im Themenfeld „Autonomes und vernetztes Fahren“ oder der Nutzung künstlicher Intelligenz (KI).

[19] Vgl. Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ%3AL_202302854.
[20] Vgl. Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R0868.
[21] Vgl. Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L_202401689.

C. Überblick zu den Rückmeldungen

I. Landesverwaltung

Am LDSG wurde aus der Landesverwaltung keine grundlegende Kritik geäußert. Es wurde bemerkt, dass mit Einführung der DSGVO das LDSG in der Verwaltungspraxis an Bedeutung verloren habe. Die Umsetzung der DSGVO habe nach deren Einführung die hauptsächliche Herausforderung dargestellt. Überwiegend bereite die Umsetzung des LDSG keine Schwierigkeiten.

Aus dem Staatsministerium wurde mitgeteilt, dass der praktische Anwendungsbereich des LDSG nur wenige Bereiche des Hauses betreffe. Hilfreich seien die Zweckänderungstatbestände, die zum Schutz des Gemeinwohls und zum Schutz Einzelner, wenn nötig, Datenverarbeitung in Gefahrenlagen erlaubten.

Im Geschäftsbereich des Kultusministeriums wird das LDSG für gut gelungen gehalten, auch insofern, als es die DSGVO an vielen Stellen präzisiere.

Für das Sozialministerium seien die §§ 4, 5, 6 sowie § 13 LDSG von besonderer Relevanz. Im Geschäftsbereich einzelner Referate gingen die Vorschriften der Sozialgesetzbücher VIII und X sowie des Gesetzes über den öffentlichen Gesundheitsdienst (ÖGDG) vor und in der Folge habe das LDSG dort nur eine eingeschränkte verwaltungspraktische Bedeutung.

Wie das Justizministerium mitteilte, sei im Bereich der Justiz die Erfahrung mit dem LDSG gering, da dieses dort überwiegend nicht anwendbar sei. Wesentlich sei dort die Abgrenzung zwischen Verwaltungstätigkeit und justiziellen Tätigkeiten zu leisten. Diese bereite in der Regel keine Schwierigkeiten.

Neben manchen Unsicherheiten in der Anwendung wird in Bezug auf einzelne Vorschriften und Themenbereiche ein Ergänzungs- oder Änderungsbedarf gesehen:

- Im Anwendungsbereich des LDSG komme es zu Kollisionen mit Vorschriften des Verwaltungsverfahrensrechts, vor allem in förmlichen Verwaltungsverfahren, wie vom Umweltministerium bemerkt wurde. Diese sollten bereinigt werden.

- Wer Öffentlichkeitsarbeit betreibe, stehe vor der Frage, ob ihm § 4 LDSG als ausreichende Rechtsgrundlage zur Verfügung steht, um personenbezogene Daten zu verarbeiten. Wegen dieser Unsicherheit wurde um Prüfung gebeten, ob spezielle Rechtsnor-

men regeln könnten, welche Formen der Öffentlichkeitsarbeit unter welchen Voraussetzungen datenschutzrechtlich zulässig seien. Dies betreffe z. B. die Erstellung von Fotografien, Videoaufnahmen oder Livestream bei Veranstaltungen, die Nutzung sozialer Netzwerke oder das Veranstaltungsmanagement.

- Im Rahmen der Beantwortung von Landtagsanfragen wird eine Regelung zur Übermittlung personenbezogener Daten angeregt.

- Die Systematik der §§ 4 bis 6 LDSG zu verstehen, im Besonderen die Übermittlungsvorschrift des § 6 LDSG im Gefüge der Vorschriften, bereitet Schwierigkeiten; Klarstellungen seien wünschenswert.

- In Bezug auf § 5 LDSG wurden aus polizeilicher Sicht Vorschläge zur Erweiterung der Zweckänderungstatbestände unterbreitet. Diese beziehen sich darauf, Ordnungswidrigkeiten ohne Beschränkung auf ihre erhebliche Bedeutung zu verfolgen, Daten für die Einleitung disziplinarrechtlicher Verfahren zu nutzen und die Anforderungen für die Übermittlung von Protokolldaten herabzusetzen.

- In Bezug auf Forschungsvorhaben (§ 13 LDSG) werden forschungsfreundlichere Regelungen für gemeinwohlorientierte Forschung gefordert, die auch die Sekundärnutzung von erhobenen Daten, die Forschung mit großen Datenmengen sowie die Kooperation mit der Privatwirtschaft erlaubten. Soweit möglich, sollte die Pseudonymisierung statt der Anonymisierung von Daten erlaubt sein. Außerdem würden einheitliche Datenschutzregelungen in den Ländern für länderübergreifende Forschung vermisst.

  Zusammenfassend lautet das Anliegen, zu untersuchen, welchen Beitrag der Landesgesetzgeber leisten könne, um Forschung mit personenbezogenen Daten zu ermöglichen, ohne den Datenschutz zu beschädigen.

- Mit dem Aufkommen des Einsatzes von KI stelle sich die Frage nach den Rechtsgrundlagen für deren Einsatz in der Verwaltung, aber auch für das vorgelagerte Training mit personenbezogenen Daten.

- Die verstärkte Inanspruchnahme des Auskunftsrechts nach der DSGVO hat zu dem Wunsch geführt, die Voraussetzungen des § 9 Absatz 2 LDSG zu konkretisieren.

- In die Vorschrift des § 15 Absatz 2 LDSG sollten, wie vom Landespolizeipräsidium angemerkt wurde, als weitere Zwecke für die Verarbeitung besonderer Kategorien personenbezogener Daten die Gesundheitsvorsorge und Arbeitsmedizin aufgenommen werden.

- Die Regelung in § 15 Absatz 6 LDSG zur Datenverarbeitung biometrischer Daten in Dienst- und Arbeitsverhältnissen veranlasste das Wissenschaftsministerium zur Nachfrage nach der Reichweite des Verbots und seine Berechtigung, insbesondere in Bezug auf den Abschluss von Betriebsvereinbarungen zum Zutritt zu Hochschulgebäuden.

- Nach Auffassung des Kultus- und Wissenschaftsministerium sollte die Vorschrift des § 16 LDSG auch auf Auszeichnungen an Schulen und Hochschulen erstreckt werden.

- In Bezug auf die Videoüberwachung wird es aus polizeilicher Sicht als belastend angesehen, in jedem Einzelfall im Rahmen der Verhältnismäßigkeitsprüfung mildere Maßnahmen prüfen zu müssen, obwohl diese meistens nicht praktikabel seien. Hier sollte über Erleichterungen nachgedacht werden. Ebenfalls in Bezug auf die Videoüberwachung wurde vorgebracht, dass die Speicherfrist zur Überprüfung der erhobenen Daten vielfach über das erforderliche Maß hinaus ausgedehnt werde. Hier könnte eine Klarstellung hilfreich sein.

- Mehrfach wurde ein Bedarf für die Regelung einer Videoüberwachung in nicht öffentlich zugänglichen Bereichen festgestellt.

- Angesprochen wurden Regelungen zur Zusammenarbeit des LfDI mit anderen Aufsichtsbehörden, insbesondere mit dem Rundfunkbeauftragten für den Datenschutz, um die einheitliche Anwendung der Vorschriften über den Datenschutz zu gewährleisten.

- Aus der Justiz wurde die Frage gestellt, wie eine Aufsichtsbehörde für die Justiz eingerichtet werden könnte.

- Die Frage, unter welchen Voraussetzungen Beschäftigte bei datenschutzrechtlichen Pflichtverletzungen zur Verantwortung gezogen werden könnten, wurde angesprochen.

- Des Weiteren wurden einige Vorschläge für Regelungen zu bisher nicht geregelten Bereichen vorgebracht. Regelungen zu Datenschutz-Folgeabschätzungen (Artikel 35 DSGVO) und Regelungen für behördliche Datenschutzbeauftragte (Artikel 37 bis 39

DSGVO) könnten die Verwaltungsarbeit erleichtern. Der Abschluss von Auftragsverarbeitungsverträgen (Artikel 28 DSGVO) könnte durch gesetzliche Vorgaben standardisiert werden.

II. Kommunale Landesverbände

Für die Kommunen haben der Gemeindetag und der Landkreistag am 29. Oktober 2021 eine gemeinsame Stellungnahme abgegeben, welche dem Bericht angefügt ist. Diese betont die hohe Belastung der kommunalen Praxis durch die Vorschriften der DSGVO. Insbesondere kleinere Gemeinden mit wenigen Mitarbeitern habe die Umsetzung der datenschutzrechtlichen Vorgaben über Gebühr belastet. Dies gelte auch noch im Jahr 2021, drei Jahre nach der Geltung der DSGVO. Vor allem die mangelnde Praxistauglichkeit der Vorschriften verhindere sogar oftmals Projekte. Dies führe zur öffentlichen Wahrnehmung des Datenschutzes als Verhinderungsinstrument anstatt als Mittel zur Durchsetzung des Grundrechts auf informationelle Selbstbestimmung. Die kommunalen Spitzenverbände plädieren daher ausdrücklich dafür, „etwaige Änderungen des LDSG vor deren Umsetzung stets im Lichte von Umsetzbarkeit und Praxistauglichkeit zu überprüfen und vorhandene Öffnungsklauseln der DSGVO in diesem Sinne zu nutzen“. Die Komplexität des Datenschutzrechts müsse auch bei der gegebenenfalls angedachten Sanktionierung von Datenschutzverstößen angemessene Berücksichtigung finden.

Im Einzelnen wird seitens der kommunalen Landesverbände vor allem auf die Vorschrift zur Videoüberwachung in § 18 LDSG eingegangen. Die datenschutzrechtlichen Vorschriften zur Videoüberwachung seien für die Städte, Gemeinden und Landkreise von besonderer praktischer Relevanz. Zur Verbesserung der Praxistauglichkeit werden mehrere Vorschläge eingebracht. Insbesondere wird eine Erweiterung des Anwendungsbereichs vorgeschlagen, um die Videoüberwachung generell zur Verhinderung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung nutzen zu können. Darüber hinaus wird zur Vermeidung unnötigen Verwaltungsaufwands eine Überarbeitung der Informationspflicht vorgeschlagen.

Die kommunalen Landesverbände betonen außerdem, dass die in Absatz 5 festgelegte vierwöchige Höchstspeicherfrist für Videoaufzeichnungen benötigt werde, um für den Fall der späteren Meldung einer Sachbeschädigung ausreichend Zeit zur Auswertung der Aufnahmen zu haben.

III. LfDI

Der LfDI hat zu einzelnen Normen des LDSG Handlungsempfehlungen ausgesprochen. Für einige Normen sieht er Korrekturbedarf. Dies betrifft im Wesentlichen folgende Themen:

- Vom LfDI wird die Einrichtung einer unabhängigen Kontrollstelle beim Landtag vorgeschlagen.

- Sicherstellung des Datenschutzes, § 3:
  Der LfDI bittet um Überarbeitung der Vorschrift für die Praxis, des Weiteren um spezifische Vorschriften für besondere Verarbeitungssituationen.

- Überprüfung der Systematik der §§ 4 bis 6 LDSG:
  Die Vorschriften zur Generalklausel, Zweckänderung und Übermittlung bedürfen nach Auffassung des LfDI der Konkretisierung und Ergänzung. Die Verantwortungsregelung sei zu korrigieren.

- Ein Vertrag zur Auftragsverarbeitung sollte durch die Fachaufsichtsbehörde getroffen werden können.

- An mehreren Stellen kritisiert der LfDI eine europarechtswidrige Verkürzung der Betroffenenrechte. Er bezieht sich auf die §§ 8, 9, 14 und 16 LDSG.

- Überarbeitung der Forschungsregelung:
  Es sollte zum Schutz betroffener Personen über die Aufnahme bisher nicht geregelter technisch-organisatorischer Maßnahmen nachgedacht werden, ohne die Forschungsinteressen außer Verhältnis zu setzen.

- Videoüberwachung nicht öffentlich zugänglicher Räume, § 18:
  Für die Videoüberwachung nichtöffentlicher Räume wurde ein Regelungsbedarf erkannt. Der LfDI geht diesbezüglich von einem erhöhten Schutzbedarf vor Überwachung aus. Des Weiteren soll zur Einhaltung des Grundsatzes der Speicherbegrenzung nach Auffassung des LfDI die Regelung der Höchstspeicherfrist von vier Wochen gestrichen werden.

- Aufgaben und Befugnisse, § 25
  Der LfDI sieht seine Befugnisse europarechtswidrig eingeschränkt. Die Durchführung von Maßnahmen dürfe nicht von weiteren Voraussetzungen abhängig gemacht werden. Auch die Beschränkung der Aufsichtsbefugnisse gegenüber Notarinnen und Notaren sieht der LfDI als europarechtswidrig an und fordert ihre Streichung.

- Nach Auffassung des LfDI sollten ihm Vollstreckungsbefugnisse zustehen und Rechte zur Beteiligung an gerichtlichen Verfahren.

- Der LfDI wünscht sich die gesetzliche Verankerung der Teilnahme des Personals des LfDI an der Personalrotation der Innenverwaltung.

- Für den LfDI sollten neben seine Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten nach dem Telekommunikation- und Telemediengesetz Aufsichtsbefugnisse hinzutreten.

IV. Rundfunkbeauftragter für den Datenschutz

Der damalige Rundfunkbeauftragte für den Datenschutz beim SWR, Herr Professor Herb, sah die zu bewältigende Herausforderung in der Umsetzung der DSGVO, nicht des LDSG. Berücksichtigt werden müsse, dass die datenschutzrechtlichen Regelungen für den Rundfunkbereich bislang im Rundfunkstaatsvertrag, nunmehr im Medienstaatsvertrag geregelt seien.

Nach Meinung von Professor Herb habe sich das datenschutzrechtliche Kontrollmodell beim SWR, das nur einen Rundfunkdatenschutzbeauftragten und keinen zusätzlichen behördlichen Datenschutzbeauftragten vorsehe, bewährt.

Er legt einige Vorschläge zur Verbesserung der unabhängigen Stellung des Rundfunkbeauftragten für den Datenschutz vor. Unter anderem setzt er sich für ein Diskriminierungsverbot nach dem Ende der Amtszeit, eine gesetzliche Regelung der Vergütung sowie eine stärkere Einbindung des Rundfunkbeauftragten für den Datenschutz in die nationale Datenschutzkonferenz ein.

V. Landtag

Der Landtag spricht das Urteil des Europäischen Gerichtshofs vom 9. Juli 2020[22] an, das anders als das LDSG keine Ausnahme vom sachlichen Anwendungsbereich der DSGVO anerkenne. Zu den Konsequenzen aus diesem Urteil finde eine Abstimmung unter den Landtagsdirektoren und Landtagspräsidenten statt. Falls die DSGVO Anwendung finde, seien insbesondere die Einschränkungen der Betroffenenrechte im Hinblick auf die Besonderheiten der parlamentarischen Tätigkeit zu überprüfen. Zum Schutz der Arbeitsfähigkeit der Untersuchungsausschüsse bedürfe es gegebenenfalls eines weitergehenden Ausschlusses des Auskunftsrechts sowie des Rechts auf Einschränkung der Verarbeitung nach den §§ 9 und 10 LDSG.

Die Derogationen der Betroffenenrechte durch § 14 LDSG bei der Archivierung von Dokumenten, insbesondere in Bezug auf das Auskunftsrecht, hält der Landtag für praxisgerecht und bittet um Beibehaltung.

[22] EuGH , Urteil vom 09.07.2020, Rechtssache C-272/19, abrufbar unter CURIA - Dokumente (europa.eu).

Darüber hinaus beschäftigt den Landtag die Öffentlichkeitsarbeit bzw. ihre datenschutzrechtliche Legitimation, insbesondere für die Anfertigung von Fotografien und das Veranstaltungsmanagement. Für die Kommunikation über Parlaments- und Behördengrenzen hinweg würde der Landtag gerne Kontaktdaten vorhalten.

Der Landtag regt außerdem an, zu untersuchen, ob das LDSG sicherheitstechnisch erforderliche Maßnahmen ausreichend legitimieren kann.

VI. Justiz

Wegen der oben erwähnten eingeschränkten Anwendbarkeit des LDSG nur für die Verwaltungsangelegenheiten der Justiz wurde aus der Justizpraxis nur von geringen Erfahrungen mit der Anwendung des LDSG berichtet. Soweit Gerichte, Staatsanwaltschaften, das Justizministerium und die Justizvollzugsbehörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung tätig werden, sei gemäß § 2 Absatz 1 Satz 3 Nummer 3 LDSG der Anwendungsbereich ebenfalls ausgeschlossen. Die dennoch bislang auftretenden Fragestellungen ließen sich mit dem geltenden Recht zufriedenstellend lösen. Allerdings erscheint teilweise die Abgrenzung zwischen Verwaltungsangelegenheiten und justiziellen Tätigkeiten nicht immer einfach. In der Gesetzesbegründung zum LDSG-JB seien nähere Erläuterungen und Beispiele zur Abgrenzung angeführt[23], die die Anwendung erleichtern könnten. Die Begrifflichkeiten sind nach Auffassung des Justizministeriums damit ausreichend geklärt.

Auch im Bereich der Justiz stelle sich mit dem Aufkommen von KI und der kommenden Regulierung des Einsatzes durch die KI-Verordnung nun die Aufgabe, eine einfache und sichere Rechtsgrundlage für das erforderliche Training von KI-Anwendungen mit personenbezogenen Daten zu schaffen. Dies habe, solange die EU oder der Bundesgesetzgeber von seiner Regelungskompetenz keinen Gebrauch gemacht haben, landesrechtlich im Rahmen des LDSG zu erfolgen.

Aus der Praxis wurde außerdem darauf hingewiesen, dass gemäß Artikel 55 Absatz 3 der DSGVO die allgemeinen Aufsichtsbehörden nicht für die Aufsicht über die justizielle Tätigkeit der Gerichte zuständig seien. Deshalb wurde teilweise angeregt, im Rahmen einer etwaigen Novellierung des LDSG zu überprüfen, ob das Unionsrecht für die in Erwägungsgrund 20 der DSGVO genannte Betrauung besonderer Stellen im Justizsystem für die Aufsicht über Datenverarbeitungsvorgänge eine besondere gesetzliche Regelung des Landes- oder des Bundesrechts erfordere. Dies werde teilweise in der Literatur gefordert; der Gesetzgeber habe dies bisher nicht für zwingend erforderlich gehalten. Bejahendenfalls müsse geprüft werden, durch

[23] LT-Drs. 16/5984, S. 88.

wen (Bund oder Land) und mit welchem Inhalt eine entsprechende Regelung unter Berücksichtigung der richterlichen Unabhängigkeit erlassen werden könnte.

In einer Einzeläußerung aus der Justiz wurden ferner Zweifel geäußert, ob der Landesgesetzgeber die Richtlinie (EU) 2016/680 vollständig in nationales Recht umgesetzt habe. Sofern dies nicht der Fall sei, müsse das LDSG a. F. angewendet werden, und zwar in richtlinienkonformer Auslegung.

VII. Rechnungshof

Der Rechnungshof hat mitgeteilt, dass das Inkrafttreten der DSGVO und die damit verbundene Neufassung des LDSG zwar zu einem gewissen Mehraufwand in der Dokumentation und Umgang mit personenbezogenen Daten geführt habe. Aufgrund der erarbeiteten Checklisten und Handreichungen hätten diese jedoch in den Arbeitsablauf integriert werden können.

D. Untersuchungsergebnisse

I. Zusammenfassung der Handlungsempfehlungen

Die Evaluierung des LDSG zeigt im Ergebnis, dass das Landesdatenschutzrecht sich im Wesentlichen bewährt hat, an einigen Stellen aber einer Nachbesserung bedarf, um praktischen Bedarfen der Verwaltung oder berechtigten Interessen der betroffenen Person zu genügen oder neuen Rechtsentwicklungen zu entsprechen. Soweit die DSGVO es zulässt, wird insoweit für Änderungen bzw. Ergänzungen im LDSG plädiert.

Deutlich wurde, dass das Datenschutzrecht wichtig ist, um die zunehmenden Formen der Datennutzung, zusammengefasst unter dem Begriff der Datenökonomie, zu flankieren. Diesbezüglich entscheidet das Datenschutzrecht in wesentlichem Umfang über die Möglichkeiten der Datennutzung. Hier ist es die Aufgabe des Landesgesetzgebers, im Rahmen seiner Kompetenzen einen vernünftigen Ausgleich zwischen den Interessen der Nutzer und der betroffenen Personen herzustellen.

Weil sich die Nutzung von personenbezogenen Daten für die Forschung als besonders relevant herausgestellt hat, widmet der Evaluierungsbericht einen Schwerpunkt der Ausgestaltung der datenschutzrechtlichen Regelungen für die Forschung.

1. Änderungsbedarf

Wesentlichen Änderungsbedarf sieht die Landesregierung in folgenden Punkten:

- Die Sicherstellung des Datenschutzes durch technische und organisatorische Maßnahmen ist zentral für alle Datenverarbeitungen. Ihrer Regelung kommt daher großes Gewicht zu. Dies sollte in § 3 LDSG und den Vorschriften zu besonderen Verarbeitungssituationen stärker herausgearbeitet werden.

- Das LDSG sollte über die Generalklausel hinaus differenzierte Regelungen für die Öffentlichkeitsarbeit der öffentlichen Stellen zur Verfügung stellen.

- Der Einsatz von KI stellt neue Anforderungen an die Verwaltung. Der zunehmende technische Fortschritt erlaubt es öffentlichen Stellen nicht mehr nur Menschen zur Aufgabenerledigung auszubilden, sondern auch technische Systeme zu „trainieren“, die bestimmte Aufgaben oder Teile von Aufgaben selbständig erledigen können. Diese bestehende technische Möglichkeit dürfte sich im Zuge des demografischen Wandels

und des damit einhergehenden Fachkräftemangels zur technischen Notwendigkeit entwickeln. Es sollte ein rechtlich gangbarer Weg gefunden werden, der die Verwaltung unterstützt, KI-Systeme zu entwickeln und einzusetzen und gleichzeitig die Interessen betroffener Personen am Schutz ihrer Daten zu berücksichtigen.

Zu diesem Zweck werden Ergänzungen des LDSG vorgeschlagen.

- Eine Erweiterung der Zweckänderungstatbestände des § 5 LDSG würde zur Rechtssicherheit beitragen, sollten aber in maßvollem Rahmen bleiben. Vorgeschlagen werden insbesondere die Erweiterung zur Verfolgung von Ordnungswidrigkeiten sowie zur Verwendung von Kontaktdaten für die politische Arbeit.

- Abrufverfahren gewinnen zunehmend an Bedeutung in der öffentlichen Verwaltung. Dies sollte auch durch eine ergänzende Regelung hierzu abgebildet werden.

- Für die Auftragsverarbeitung sollte die Beauftragung durch die Fachaufsichtsbehörde zugelassen werden. Für die Erleichterung der Beauftragung könnten eine gesetzliche Grundlage oder standardisierte Vertragsbedingungen zur Verfügung gestellt werden.

- Die Forschungsregelung des § 13 LDSG genügt nicht den Anforderungen, die an die Forschung aus der Praxis gestellt werden. Soweit möglich, werden hier Verbesserungen vorgeschlagen. Die retrospektive Nutzung personenbezogener Daten, das heißt die Weiterverarbeitung bestehender Datensätze für die Forschung, sollte unterstützt werden ebenso Kooperationen mit der Privatwirtschaft ermöglicht werden. Auch für die Veröffentlichung von Forschungsergebnissen entsprechend der guten wissenschaftlichen Praxis sollte die Regelung im LDSG erweitert werden. Die Transparenz und damit das Vertrauen der Bürgerinnen und Bürger in die Datenwirtschaft könnten durch geeignete Maßnahmen wie Anzeige- und Publikationspflichten gestärkt werden.

- Videoüberwachung ist in der Überwachung sensibler öffentlicher Räume nicht wegzudenken. Unbenommen der Vorgabe, dass sich Videoüberwachung auf das geringstmögliche Maß beschränken sollte, wird vorgeschlagen, diesbezüglich abstrakt-generell Videoüberwachungsmaßnahmen zuzulassen.

- Für eine Ermächtigungsgrundlage für sicherheitstechnisch erforderliche Maßnahmen wurde ein Bedarf festgestellt.

Auf die einzelnen Vorschriften bezogen, finden sich die Änderungs- und Ergänzungsvorschläge am Ende des Berichts.

2. Konsens und Dissens mit dem LfDI

In vielen Punkten kann sich die Landesregierung den Anregungen und Vorschlägen des LfDI ganz oder teilweise anschließen. Ebenso wie vom LfDI befürwortet, sollten

- die Einführung einer unabhängigen Kontrollstelle für die Anwendung der DSGVO auf die parlamentarische Tätigkeit des Landtags geprüft werden,
- § 3 LDSG in Bezug auf die Sicherstellung des Datenschutzes,
- sowie die §§ 4 bis 6 LDSG in Bezug auf ihre Systematik überprüft werden,
- der Fachaufsichtsbehörde ermöglicht werden, für nachgeordnete Behörden Auftragsverarbeitungsverträge abzuschließen,
- die Betroffenenrechte teilweise nachgebessert werden,
- die Forschungsregelung überarbeitet werden, wobei hier weitergehende Lockerungen vorgeschlagen werden,
- eine Regelung für die Videoüberwachung in nichtöffentlichen Bereichen erwogen werden.
- Keine Einwendungen bestehen, die Personalrotation in der Landesverwaltung gesetzlich zu verankern
- sowie die Aufsichtszuständigkeit nach dem TDDDG festzuschreiben.

Zu folgenden Anregungen des LfDI ist ein Dissens festzustellen:

- In Bezug auf § 14 LDSG werden die Einschränkungen der Betroffenenrechte als ausgewogen und praxisgerecht angesehen.
- Es wird keine Notwendigkeit gesehen, die in § 18 LDSG geregelte Vier-Wochen-Frist zur Auswertung von Videoaufnahmen aufzugeben.
- Die Abschaffung der Pflicht des LfDI zur Anhörung der Fachaufsichtsbehörde vor Abhilfemaßnahmen sowie die Einführung von Vollstreckungsbefugnissen des LfDI gegenüber öffentlichen Stellen wird abgelehnt.

- Nicht befürwortet wird, die Aufsichtsbefugnisse gegenüber Notarinnen und Notaren auszuweiten.

II. Untersuchung und Bewertung einzelner Regelungen des LDSG

Im Folgenden werden die relevanten Regelungen des LDSG untersucht, und zwar jeweils ihr Norminhalt erläutert und die Rückmeldungen vorgestellt. Die Landesregierung bezieht im Zusammenhang der betroffenen Norm Position zu den geäußerten Rückmeldungen und Vorschlägen. Der Bericht unterbreitet Lösungsvorschläge, sofern nach Auffassung der Landesregierung Anpassungsbedarf besteht.

Der Position der Landesregierung vorangestellt wird jeweils die Wiedergabe der Bewertung des LfDI entsprechend seinem Schreiben vom 13. Februar 2024. Für die Auffindbarkeit seiner Bewertung wird die jeweilige Seitenzahl eingefügt.[24]:

1. Systematik und Normenklarheit im LDSG

Wie festgestellt verhindert das Normwiederholungsverbot die vollständige Regelung des Datenschutzrechts. Dies erschwert dem Normanwender die Anwendung des Datenschutzrechts. Es wurden verschiedene Vorschläge eingebracht, die Normenklarheit zu steigern.

a) Verwendung des Begriffs „Datenschutz-Grundverordnung“

Statt der Normbezeichnung „Verordnung (EU) 2016/679“ wird die Verwendung der eingeführten Bezeichnung „Datenschutz-Grundverordnung“ im Gesetzestext vorgeschlagen.

- Bewertung des LfDI (S. 4):

Der LfDI schließt sich diesem Vorschlag zur Verbesserung der Lesbarkeit an und verweist auf das Niedersächsische Landesdatenschutzgesetz.

Position der Landesregierung:

Für die Zitierweise des Rechts der Europäischen Union hat die Landesregierung die Verwaltungsvorschrift Regelungen erlassen. Diese sieht das Zitat mit der Angabe des Rechtsaktes und der Bezugsnummer vor[25]. Für eine einheitliche Handhabung und Auffindbarkeit sollte hieran festgehalten werden. Der Bundesgesetzgeber verwendet durchgehend die Bezeichnung

[24] Die Stellungnahme des LfDI vom 13. Februar 2024 ist wie folgt zu berichtigen: Auf den Seiten 4, 44 und 62 ist die Stellungnahme des Wissenschaftsministeriums vom 28. Juni 2021, nicht des Innenministeriums in Bezug genommen.
[25] Vgl. Nummer 1.8.2 der Anlage 1 „Regelungsrichtlinien“.

„Verordnung (EU) 2016/679“. Aus der verwendeten Bezeichnung wird damit auch ersichtlich, dass es sich um europäisches Recht handelt.

b) Zur Systematik

Das Verhältnis der §§ 4 bis 6 LDSG zueinander wird als undurchsichtig kritisiert. Dies erschwere die Rechtsanwendung. Es wird eine andere Struktur angeregt, um das Verständnis zu erleichtern. Gewünscht wird, dass das Verhältnis der §§ 4 bis 6 LDSG zu Artikel 6 DSGVO verdeutlicht werde. Der gesamte Normenkomplex der §§ 4 bis 6 LDSG solle in seinem Zusammenspiel klarer gefasst werden. § 6 LDSG dürfe nicht die alleinige Übermittlungsnorm sein, denn neben der zweckändernden Übermittlung in § 6 Abs. 1 LDSG gebe es auch noch andere, die nicht Absatz 2 oder 3 unterfielen, sondern über § 4 LDSG liefen. Auch das Verhältnis zu § 5 LDSG bleibe unklar.

- Bewertung des LfDI (S. 14 letzter Absatz):

Der LfDI unterstützt den Vorschlag. Seiner Auffassung sollte die Systematik der §§ 4 bis 6 LDSG im Einzelnen einer Überprüfung unterzogen werden. So sei es beispielsweise misslich, wenn die Zulässigkeit der (nicht zweckändernden) Übermittlung eines personenbezogenen Datums rechtssicher nur im Wege eines Erst-recht-Schlusses aus der Regelung für zweckändernde Übermittlung in § 6 LDSG hergeleitet werden könne.

Position der Landesregierung:

Die bestehende Systematik ist wie folgt zu erklären. Die Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Diese wird, sofern keine spezielle Regelung (im LDSG oder anderen Gesetzen) vorhanden ist, in § 4 LDSG zur Verfügung gestellt. Der Vorrang der DSGVO wird dabei immer vorausgesetzt, so dass die Regelungen des LDSG die DSGVO im Sinne von Artikel 6 Absatz 3 DSGVO spezifizieren. § 4 LDSG legitimiert auch die Übermittlung, sofern diese zur Aufgabenerfüllung erforderlich ist. Spezieller Erlaubnistatbestände bedarf es im Hinblick auf den Grundsatz der Zweckbindung, um eine Zweckänderung zu legitimieren. Diese sind in § 5 LDSG enumerativ geregelt. Wie sonst auch kann das LDSG nur Regelungen im Rahmen der Öffnungsklauseln (hier Artikel 6 Absatz 4 in Verbindung mit Artikel 23 DSGVO) und unter Beachtung des Wiederholungsverbots treffen, sodass sich auch aus der DSGVO selbst zulässige Zweckänderungen ergeben können. Dies betrifft z. B. die weitere Verwendung zu Forschungs- und Statistikzwecken. In § 6 LDSG werden die Tatbestände des § 5 LDSG auch auf die Übermittlung personenbezogener Daten zu anderen als ihren Erhebungszwecken angewendet und zusätzlich um die Berechtigung zur Übermittlung an nichtöffentliche Stellen erweitert.

Diese Struktur ist nicht zwingend. In Bezug auf die Übermittlung personenbezogener Daten bedarf es im Prinzip keiner Regelung, da diese entweder ihrem Zweck entsprechend zur Aufgabenerfüllung oder berechtigterweise für einen anderen Zweck verarbeitet werden. Die entsprechenden Voraussetzungen sind in den §§ 4 und 5 LDSG geregelt. Im Gesetzgebungsverfahren wurde jedoch eine Regelung der Übermittlung gewünscht. Diesem Bedürfnis der Praxis sollte nach wie vor nachgekommen werden. Im Rahmen einer Novellierung sollte aber geprüft werden, wie die Systematik besser abgebildet werden kann.

2. Anwendungsbereich (§ 2 LDSG)

a) Zum Norminhalt

§ 2 LDSG regelt den Anwendungsbereich des LDSG, vor allem in Abgrenzung zu polizeilicher, justizieller, parlamentarischer, privatwirtschaftlicher Tätigkeit. Ferner wird der Vorrang oder Nachrang des LDSG zu anderen Gesetzen geregelt.

b) Rückmeldungen und Bewertung

aa) Zu § 2 Absatz 1 LDSG

Definition des Verantwortlichen

Für die kommunalen Landesverbände regen der Gemeindetag und der Landkreistag an, in § 2 Absatz 1 Satz 2 LDSG die Definition des Verantwortlichen dergestalt zu konkretisieren, dass abweichende Definitionen des Verantwortlichen in einem anderen Gesetz erfasst werden. Hingewiesen wird auf § 67 Absatz 4 SGB X, der für Gebietskörperschaften als Leistungsträger die funktional zuständige Organisationseinheit als Verantwortlichen festlegt. Vorgeschlagen wird folgende Formulierung:

„Die öffentliche Stelle ist zugleich Verantwortlicher nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit dieses oder ein anderes Gesetz nichts Abweichendes bestimmt."

- Bewertung des LfDI (S. 5):

Der LfDI hält die vorgeschlagene Änderung nicht für erforderlich und unsystematisch. Wie in der Stellungnahme von Gemeinde- und Landkreistag selbst dargestellt wird, ergebe sich bereits aus § 2 Absatz 3 LDSG, dass besondere Rechtsvorschriften anderer Gesetze denjenigen des LDSG vorgehen. Die Bestimmung des Verantwortlichen in § 2 Absatz 1 Satz 2 LDSG sei eine solche (materielle, also nicht nur den Anwendungsbereich betreffende) Vorschrift des LDSG. Warum ausgerechnet bei dieser Norm erneut der Vorrang spezifischerer Regelungen

aus anderen Gesetzen erwähnt werden solle, erschließe sich ihm nicht. Der Einschub könnte im Gegenteil verwirren, indem sich die Frage stellen könnte, ob an Stellen, an denen nicht erneut der Vorrang anderer Gesetze betont wird, dieser Vorrang im Umkehrschluss (abweichend von § 2 Absatz 3 LDSG) nicht gelten solle.

Position der Landesregierung:

Den Erwägungen des LfDI kann gefolgt werden. Allerdings kann die bisherige Fassung des Gesetzes missverständlich sein, da sie nur eine andere Bestimmung durch „dieses Gesetz“ erwähnt. Insofern könnte der Formulierungsvorschlag der kommunalen Landesverbände eine Klarstellung bedeuten.

bb) Zu § 2 Absatz 3 LDSG

Sachverhaltsermittlung

In der Landesverwaltung begegnet der Begriff der „Sachverhaltsermittlung“ in § 2 Absatz 3 LDSG Auslegungsschwierigkeiten. Dies ist relevant für die Frage, wie mit § 73 Absatz 1 des Landesverwaltungsverfahrensgesetzes (LVwVfG) in Bezug auf Anhörungsverfahren in Planfeststellungsverfahren umzugehen ist. Dort ist die Veröffentlichung personenbezogener Daten der Grundstückseigentümer, nämlich Namen und Anschriften, vorgeschrieben. Diesbezüglich wird eine Klarstellung gewünscht, da dies ohne „Korrektur“ durch das Datenschutzrecht bedeuten würde, dass die hier bezeichneten personenbezogenen Daten veröffentlicht würden.

- Bewertung des LfDI (S. 5f.):

Dem LfDI erscheint die Kritik zutreffend. Zur Beseitigung des Problems sollte, zusätzlich zu einer Klarstellung im LDSG, eine Änderung von § 73 Abs. 1 S. 2 LVwVfG angestrengt werden. Zur Begründung führt er aus:

Die im Jahr 1991 als gewollte Erleichterung eingeführte Regelung führe mittlerweile zu Problemen. Denn naturgemäß wurde damals nicht berücksichtigt, dass die Auslegung der Unterlagen in Zukunft im Internet erfolgen könnte und Eigentumsverhältnisse dadurch potenziell für jedermann weltweit einsehbar sind. Die Praxis zeige die Schwierigkeiten: Pläne würden nach Auskunft eines Regierungspräsidiums uneinheitlich – teils ohne Namen und Anschriften (online) und teils mit den entsprechenden personenbezogenen Daten (in Gemeinden) – ausgelegt. Andere Regierungspräsidien verzichteten (entgegen dem eigentlichen Gesetzeswortlaut) teilweise gänzlich auf Namen und Anschriften. Letztere Praxis, das Weglassen, ergebe jedoch sowohl unter praktischen als auch unter rechtlichen Gesichtspunkten Sinn: Eigentümer vermögen schließlich anhand der Flurstücknummer eindeutig zu ermitteln, ob es sich um ihr

Grundstück handelt – und könnten daraus folgern, ob ihr Eigentum von dem jeweiligen Planfeststellungsverfahren betroffen ist. Bei Unklarheiten ließe sich über das Pseudonym in Gestalt der Flurstücknummer der Eigentumsstatus auch durch eine entsprechende Grundbuchabfrage klären. Aus einer Nennung von Namen und Anschrift in veröffentlichten Plänen ergebe sich hier kein Mehrwert, der die damit verknüpften Gefahren aufwöge. Eigentümer könnten aufgrund der bekannt gemachten Daten potenziell von Dritten erheblich belästigt werden. Auch in rechtlicher Hinsicht erscheine § 73 Absatz 1 Satz 2 LVwVfG bedenklich. Die durch die Nennung der personenbezogenen Daten verfolgten Zwecke sein in der Vorschrift nicht weiter dargelegt, was es äußerst fraglich erscheinen lasse, ob eine nach Artikel 6 Absatz 3 Satz 2 DSGVO und gemäß Artikel 5 Absatz 1 Buchst. b DSGVO erforderliche Festlegung der mit der Datenverarbeitung verfolgten Zwecke hinreichend erfolgt sei. Alles in allem sollte somit eine Anpassung des § 73 Absatz 1 LVwVfG erfolgen, die (gleichzeitig vereinheitlichend) zurück zur Fassung des § 73 Absatz 1 VwVfG (Bund) führe.

Position der Landesregierung:

Die Landesregierung schließt sich der Bewertung des LfDI im Wesentlichen an. Zur Verdeutlichung des Sinngehalts der bestehenden Regelung des § 2 Absatz 3 LDSG wird ausgeführt:

Die Vorschrift schränkt die Befugnisse der Verwaltungsbehörden zur Sachverhaltsermittlung in Bezug auf die Verarbeitung personenbezogener Daten ein. Diese Befugnisse sind insbesondere in § 24 LVwVfG (Untersuchungsgrundsatz) und § 26 LVwVfG (Beweismittel) geregelt. Für die Art und Weise der zur Sachverhaltsaufklärung benötigten oder zu verarbeitenden Informationen sowie die Modalitäten der Erhebung oder Verarbeitung ist damit das Datenschutzrecht anzuwenden, sofern personenbezogene Daten verarbeitet werden. Im Übrigen haben die Vorschriften des Landesverwaltungsverfahrensgesetzes Vorrang, sofern sie nicht dem Anwendungsvorrang der DSGVO widersprechen.

Aus datenschutzrechtlicher Sicht besteht kein Änderungsbedarf im LDSG. Es wird im Einklang mit dem LfDI vorgeschlagen, die Regelung an § 73 VwVfG des Bundes anzugleichen. Das VwVfG schreibt in § 73 nur die Vorlage des Plans, bestehend „aus den Zeichnungen und Erläuterungen, die das Vorhaben, seinen Anlass und die von dem Vorhaben betroffenen Grundstücke und Anlagen erkennen lassen“, vor. Dies erlaubt es, auf die Angabe der personenbezogenen Daten von Namen und Anschrift der betroffenen Eigentümer zu verzichten und ist daher geeignet, dem Anwendungsvorrang der DSGVO zu genügen.

Ein Entwurf zur Änderung des LVwVfG in Angleichung des § 73 Absatz 1 Satz 2 LVwVfG an die Bundesregelung befindet sich in Vorbereitung.

cc) Zu § 2 Absatz 4 LDSG

Anwendung des LDSG außerhalb des Geltungsbereichs der DSGVO und der Richtlinie (EU) 2016/680 (JI-Richtlinie)

Eine Verwaltungsrichterin äußerte Zweifel an der vollständigen Umsetzung der JI-Richtlinie in das Landesrecht, da § 2 Absatz 1 Satz 3 LDSG-JB lediglich für die Verarbeitung personenbezogener Daten zur Verfolgung und Ahndung von Straftaten anwendbar sei. Damit sei die Verarbeitung personenbezogener Daten zur Verhütung, Ermittlung, Aufdeckung von Straftaten, die von der JI-Richtlinie umfasst sei, vom LDSG-JB nicht erfasst. In der Folge wäre das LDSG in der bis 20. Juni 2018 geltenden Fassung anwendbar.

- Bewertung des LfDI (S. 75f.):

Der LfDI äußert ebenfalls Kritik am LDSG-JB. Er stellt in Frage, dass das LDSG-JB auf Behörden außerhalb des Justizbereichs, soweit sie personenbezogene Daten zur Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten oder zur Vollstreckung von Geldbußen verarbeiten[26], anwendbar sei und möchte diesbezüglich eine Überprüfung und ggf. Klarstellung im Gesetzestext.

Position der Landesregierung:

Die vorgebrachten Bedenken der Richterin werden nicht geteilt. Zwischenzeitlich ist mit dem Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 für die Polizei in Baden-Württemberg und zur Änderung weiterer polizeirechtlicher Vorschriften vom 6. Oktober 2020 eine entsprechende Umsetzung für den Bereich der Polizei erfolgt. Datenverarbeitungen zur Gefahrenabwehr durch allgemeine Sicherheitsbehörden ebenso wie durch Fachbehörden sind grundsätzlich nach den Vorschriften der DSGVO zu beurteilen; erst, wenn ein Verwaltungsverfahren formal in ein konkretes Ordnungswidrigkeitenverfahren übergeht, finden die Bestimmungen des LDSG-JB nach § 2 Absatz 1 Satz 3 dieser Vorschrift auch auf die Tätigkeit dieser Behörden Anwendung. Es ist damit davon auszugehen, dass der gesamte Bereich der straftatenbezogenen Tätigkeiten, der vom Anwendungsbereich der Richtlinie (EU) 2016/680 erfasst ist, abgedeckt ist.

Im Übrigen enthält § 2 Absatz 4 LDSG einen Auffangtatbestand für alle nicht von der DSGVO oder der JI-Richtlinie erfassten Datenverarbeitungen.

[26] Vgl. § 2 Absatz 1 Satz 3 LDSG-JB

dd) Zu § 2 Absatz 5 LDSG

Anwendung für den Landtag

Der Landtag sieht im Hinblick auf das bereits erwähnte Urteil des Europäischen Gerichtshofs vom 9. Juli 2020 gegen das Land Hessen Prüfungsbedarf, ob Absatz 5 aufgehoben werden muss. Er hat mitgeteilt, dass hierzu eine Abstimmung unter den Parlamenten im Rahmen von Landtagsdirektorenkonferenz und Landtagspräsidentenkonferenz stattfinde.

In dem bezeichneten Urteil hat der Europäische Gerichtshof für Recht erkannt[27]:

„Artikel 4 Nr. 7 der 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) ist dahin auszulegen, dass der Petitionsausschuss eines Gliedstaats eines Mitgliedstaats insoweit, als dieser Ausschuss allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als „Verantwortlicher“ im Sinne dieser Bestimmung einzustufen ist, so dass die von einem solchen Ausschuss vorgenommene Verarbeitung personenbezogener Daten in den Anwendungsbereich dieser Verordnung, u. a. unter deren Artikel 15, fällt.“

- Bewertung des LfDI (S. 6f.):

Der LfDI führt aus:

Inwieweit die DSGVO tatsächlich für den parlamentarischen (Kern-)Bereich gelte, sei trotz des zitierten Urteils des Europäischen Gerichtshofs im Jahr 2020 nicht abschließend entschieden, da dies dort nicht streitentscheidend gewesen sei. Deutlich in Richtung einer Anwendbarkeit auch im besagten Kontext könne man aber das jüngst ergangene Urteil des Europäischen Gerichtshofs vom 16. Januar 2024[28] lesen. Die Befunde des Gerichtshofs zu den Tätigkeiten eines Untersuchungsausschusses dürften auf andere Bereiche der parlamentarischen Tätigkeiten übertragbar sein. Wie weit § 2 Absatz 5 LDSG dann vor diesem Hintergrund im Lichte von Artikel 6 Absatz 1 Unterabsatz 1 Buchst. e in Verbindung mit Artikel 6 Absatz 3 Satz 1 DSGVO Bestand haben könne, bleibe weiterer Analyse vorbehalten. Soweit nach dem genannten Urteil vom 16. Januar 2024 eine Datenschutzaufsicht auch für den parlamentarischen Bereich erforderlich sei, rege er – mit Blick darauf, dass aus verfassungsrechtlichen Gründen eine Kontrolle der parlamentarischen Arbeit durch die Exekutive, zu der der LfDI insoweit

[27] Siehe Urteil des EuGH unter Fußnote 22, am Ende.
[28] EuGH, Urteil vom 16.1.2024, Rechtssache C-33/22, CURIA - Dokumente (europa.eu).

gehöre, wegen des Gewaltenteilungsprinzips untunlich sei – an, die Einrichtung einer unabhängigen Kontrollstelle beim Landtag zu prüfen, die dort die Datenschutzaufsicht übernehme und bei deren Ausgestaltung die parlamentarischen Besonderheiten berücksichtigt würden.

Anlässlich der Rechtsprechung des Europäischen Gerichtshofs sollte außerdem überprüft werden, ob die Datenschutzordnung des Landtags, die noch aus der Zeit vor der Geltung der DSGVO stamme, noch hinreichend aktuell sei.

Position der Landesregierung:

Ausgehend von den Urteilen des Europäischen Gerichtshofs ist § 2 Absatz 5 LDSG zu eng gefasst und sollte angepasst werden. Bei einer Neufassung wäre zu diskutieren, generell die Landtagsarbeit der DSGVO zu unterstellen. Explizit betrifft das erstgenannte Urteil nur die Tätigkeit des Petitionsausschusses. Der Europäische Gerichtshof führt jedoch aus, dass die Definition des in der Verordnung 2016/679 enthaltenen Begriffs „Verantwortlicher“ nicht auf Behörden beschränkt sei, sondern hinreichend weit, um jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, einzuschließen[29]. Im Folgenden sieht der Europäische Gerichtshof keine Ausnahmen nach Artikel 2 Absatz 2 DSGVO als gegeben an. Er stellt fest: „…letztens ist in der Verordnung 2016/679, insbesondere in deren 20. Erwägungsgrund und deren Artikel 23, keine Ausnahme in Bezug auf parlamentarische Tätigkeiten vorgesehen“[30].

Hierauf weist auch nach Auffassung der Landesregierung das vom LfDI genannte jüngste Urteil des Europäischen Gerichtshofs vom 16. Januar 2024 hin. Der Europäische Gerichtshof hat für Recht erkannt:

„Art. 16 Abs. 2 Satz 1 AEUV und Art. 2 Abs. 2 Buchst. a der Verordnung (EU) 2016/679 …sind dahin auszulegen, dass nicht angenommen werden kann, dass eine Tätigkeit allein deshalb außerhalb des Anwendungsbereichs des Unionsrechts liegt und damit der Anwendung dieser Verordnung entzogen ist, weil sie von einem vom Parlament eines Mitgliedstaats in Ausübung seines Kontrollrechts der Vollziehung eingesetzten Untersuchungsausschuss ausgeübt wird.“[31]

Des Weiteren legt der Europäische Gerichtshof Artikel 77 Absatz 1 und Artikel 55 Absatz 1 der DSGVO so aus, dass diese der Datenschutzaufsichtsbehörde unmittelbar die Zuständigkeit übertragen, über Beschwerden betreffend von diesem Untersuchungsausschuss durchgeführte Verarbeitungen personenbezogener Daten zu befinden, wenn das Recht des Mitgliedstaats die

[29] A.a.O. Rn. 65.
[30] A.a.O. Rn. 72.
[31] A.a.O. Rn.73.

parlamentarische Tätigkeit nicht der Aufsicht der eingerichteten Aufsichtsbehörde unterstellt.[32]

Die Landesregierung enthält sich einer endgültigen Bewertung, da die Abstimmung des Änderungsbedarfs dem Parlament überlassen bleiben sollte. Das Datenschutzrecht des Parlaments ist bisher in der Datenschutzordnung des Landtags geregelt.

Hierin könnten auch notwendige Einschränkungen der Betroffenenrechte ihren Platz finden (hierzu unten unter „Zu den Einschränkungen der Betroffenenrechte (§§ 8 bis 11 LDSG).

Anwendung für die Gerichte

Bislang hat das LDSG wegen seiner Beschränkung in § 2 Absatz 5 LDSG in der Justiz wenig praktische Bedeutung erlangt. Soweit durch das Aufkommen des Einsatzes von KI Novellierungsbedarf besteht, bedarf es einer Erweiterung des Anwendungsbereichs auch auf den Bereich außerhalb der Verwaltungsangelegenheiten (justizielle Tätigkeiten), solange der Bundesgesetzgeber von seiner konkurrierenden Gesetzgebungskompetenz hierzu keinen Gebrauch gemacht hat.

ee) Zu § 2 Absatz 6 LDSG

Unternehmensbegriff

Aus dem Wissenschaftsministerium wird um eine Definition des in § 2 Absatz 6 LDSG verwendeten Unternehmensbegriffs gebeten.

- Bewertung des LfDI (S. 8):

Dem LfDI sind hinsichtlich des Unternehmensbegriffs in der Praxis Einordnungs- und damit Anwendungsproblemen nicht bekannt. Etwaige Einzelfallprobleme dürften sich durch Auslegung mit Hilfe eines Rückgriffs auf die Definition des Artikels 4 Nummer 18 DSGVO sowie die weitere Tatbestandsvoraussetzung der Teilnahme am Wettbewerb lösen lassen. Sollte eine Klarstellung dennoch für erforderlich gehalten werden, böte sich eine Bezugnahme auf Artikel 4 Nummer 18 DSGVO an.

Position der Landesregierung:
Eine Definition im Gesetz wird nicht für notwendig erachtet. Die DSGVO definiert den Unternehmensbegriff in Artikel 4 Nummer 18. Danach ist ein „Unternehmen“ eine natürliche

[32] A.a.O. Rn. 73.

oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen. Damit kommt es in § 2 Absatz 6 LDSG funktional auf die ausgeübte wirtschaftliche Tätigkeit der öffentlichen Stelle an.

Dementsprechend kann für den Unternehmensbegriff die Rechtsprechung des Europäischen Gerichtshofs herangezogen werden, der sich in seinem Urteil vom 12. Juli 2012[33] mit dem Unternehmensbegriff des Artikels 102 AEUV befasst hat. Danach ist die wirtschaftliche Tätigkeit von der Ausübung hoheitlicher Befugnisse in folgender Weise abzugrenzen: „Soweit eine öffentliche Einheit nämlich eine wirtschaftliche Tätigkeit ausübt, die von der Ausübung ihrer hoheitlichen Befugnisse losgelöst werden kann, handelt sie in Bezug auf diese Tätigkeit als Unternehmen; ist die wirtschaftliche Tätigkeit dagegen mit der Ausübung ihrer hoheitlichen Befugnisse untrennbar verbunden, bleiben sämtliche Tätigkeiten dieser Einheit Tätigkeiten in Ausübung hoheitlicher Befugnisse“[34]. Ein gesetzlich vorgesehenes Entgelt für die hoheitliche Tätigkeit macht sie noch nicht zu einer wirtschaftlichen Tätigkeit[35].

3. Sicherstellung des Datenschutzes (§ 3 LDSG)

a) Zum Norminhalt

Diese Vorschrift ist § 22 Absatz 2 BDSG nachgebildet. Während sie dort im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener Daten eingeführt ist, um der Forderung der DSGVO nach „angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ zu genügen[36], wird sie im LDSG als bei jeder Datenverarbeitung zu beachtende Norm den Rechtsgrundlagen der Datenverarbeitung vorangestellt. Sie enthält anwenderbezogen einen Katalog geeigneter Maßnahmen zur Sicherstellung des Datenschutzes nach Artikel 25, 32 DSGVO.

b) Rückmeldungen und Bewertung

aa) Zu § 3 Absatz 1 LDSG

(1) Technische und organisatorische Maßnahmen

Nach Auffassung des LfDI in seiner ersten Stellungnahme vom November 2020 lese sich § 3 Absatz 1 Satz 3 Nummer 1 LDSG derzeit so, als seien technische und organisatorische Maßnahmen (TOM) ein „Kann“, kein „Muss“. Das widerspreche dem Wortlaut des Artikels 32

[33] EuGH, Urteil vom 12.07.2012, Rechtssache C-138/11, Rn. 35 ff., abrufbar unter CURIA - Ergebnisliste (europa.eu).
[34] A.a.O. Rn. 38.
[35] A.a.O. Rn. 39.
[36] Vgl. z. B. Artikel 9 Absatz 2 Buchst. g und j DSGVO.

Absatz 1 Halbsatz 1 DSGVO, wonach (unter Berücksichtigung des Stands der Technik usw.) der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen müssten, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Erst im zweiten Halbsatz zähle Artikel 32 Absatz 1 DSGVO in den Buchstaben a bis d auf, welche Maßnahmen „gegebenenfalls“ zu den TOM gehören. Der LfDI empfiehlt daher, in § 3 LDSG klarzustellen, dass entsprechend Artikel 32 DSGVO technische und organisatorische Maßnahmen stets, nicht nur fakultativ, zu treffen seien, indem § 3 Absatz 1 Satz 3 Nummer 1 LDSG „vor die Klammer“ gezogen werde.

Aus Sicht eines Regierungspräsidiums wird in der Vorschrift die Bedeutung des technischen und organisatorischen Datenschutzes hervorgehoben, welches als Konkretisierung der in Artikel 32 Absatz 1 DSGVO genannten Maßnahmen zielführend sei.

- Bewertung des LfDI (S. 8 f.):

Der LfDI hält die Regelung des § 3 Absatz 1 LDSG nach wie vor für systematisch verfehlt und in der Praxis verwirrend. Zunächst zieht er die Regelungsbefugnis des Landesgesetzgebers für konkretisierende Regelungen in Frage, da eine Öffnungsklausel zu Artikel 32 DSGVO nicht existiere. Für spezifische Regelungen im Sinne des Artikels 6 Absatz 2 und 3 DSGVO zusätzlich zu Artikel 32 DSGVO seien die aufgeführten Maßnahmen zu vage. Entgegen der Gesetzesbegründung sei auch nicht erkennbar, dass „spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ im Sinne von Artikel 9 Absatz 2 Buchst. g DSGVO für die Verarbeitung besonderer Kategorien personenbezogener Daten getroffen worden seien. Überdies sei die Verarbeitung durch Auftragsverarbeiter unzureichend berücksichtigt.

Insgesamt hält er eine grundlegende Überarbeitung der Norm für erforderlich, wobei nach den verschiedenen ihr zugedachten Funktionen zu differenzieren sei.

Position der Landesregierung:

Grundsätzlich wird die Regelung des § 3 LDSG als geeignet angesehen, vom Verantwortlichen zu treffende TOM beispielhaft zu konkretisieren. Deren Wichtigkeit in Bezug auf sämtliche Datenverarbeitungen wird betont, indem die Regelung unter der Überschrift „Sicherstellung des Datenschutzes“ den Rechtsgrundlagen zur Datenverarbeitung vorausgeht. Im Sinne des LfDI wird aber für eine sprachliche Korrektur plädiert. Richtig ist, dass die DSGVO in Artikel 32 generell TOM verlangt. Diese Verpflichtung sollte, um Missverständnisse zu vermeiden, entsprechend klargestellt werden.

Die ausnahmsweise zulässige Verarbeitung nach Artikel 9 Absatz 2 DSGVO muss grundsätzlich höheren Ansprüchen genügen als nach den allgemeinen Anforderungen der DSGVO gefordert wird[37]. Verlangt werden diesbezüglich „Garantien“ und „angemessene und spezifische Maßnahmen“. In Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten sollten im jeweiligen Kontext der Regelung daher besondere technische und organisatorische Maßnahmen verlangt werden.[38].

(2) Terminologie

Unter Bezug auf § 3 Absatz 1 Nummer 2 LDSG wurde aus einem Ressort uneinheitliche Terminologie bemängelt. Die genannte Vorschrift erfasse nur einzelne Verarbeitungsvorgänge, hier das Erfassen, Verändern und Löschen. Es erscheine sinnvoll, im Allgemeinen von der Datenverarbeitung zu sprechen.

- Bewertung des LfDI (S. 9f.):

Generell treffe es zu, dass Terminologien, wo möglich, vereinheitlicht werden sollten. Inwieweit hier eine Ersetzung der Einzelbeschreibung von Verarbeitungsformen durch den allgemeinen Begriff der Verarbeitung erfolgen solle, bedürfe indes sorgfältiger Abwägung. Einerseits könnten auch weitere (unberechtigte) Formen der Verarbeitung als das Erfassen, Veränderung und Löschen von hinreichender Eingriffsintensität sein, dass es angemessen sein könne, auch insoweit für eine Möglichkeit der Überprüfung und Nachvollziehbarkeit Sorge zu tragen, wie zum Beispiel die unbefugte Einsichtnahme oder die unbefugte Übermittlung. Andererseits könne es nicht das Ziel sein, standardmäßig eine vollständige, lückenlose Protokollierung im Zusammenhang mit personenbezogenen Daten zu etablieren. Eine solche würde im Ergebnis dazu führen, dass sich jeder einzelne Arbeits-/Bearbeitungsschritt vollständig nachvollziehen ließe. Eine solche vollumfängliche Kontrollmöglichkeit liefe wiederum Gefahr, unverhältnismäßig in das Recht auf informationelle Selbstbestimmung von Beschäftigten einzugreifen. Daher sollte nicht ungeprüft standardmäßig eine Vollprotokollierung im vorgenannten Sinne erfolgen. Diese Aspekte sollten im Gesetzestext zum Ausdruck kommen, wobei anzumerken sei. dass es sich bei den derzeit in § 3 Absatz 1 LDSG aufgelisteten Maßnahmen ohnehin nur um Beispiele handele.

Position der Landesregierung:
Der Bewertung des LfDI wird zugestimmt. Im Übrigen wurde im Gesetzestext auf einheitliche Terminologie geachtet.

[37] Vgl. Frenzel in Paal/Pauly, BDSG § 22 Rn. 12 bis 14.
[38] Vgl. hierzu die Ausführungen zu § 13 LDSG.

Überall, wo nur einzelne Verarbeitungsschritte erfasst sind, ist dies dem Regelungszweck geschuldet[39].

bb) Zu § 3 Absatz 2 LDSG

(1) Datengeheimnis

Die Regelung hat das Datengeheimnis aus § 6 LDSG a. F. übernommen. Laut Gesetzesbegründung sollte damit entsprechend Artikel 32 Absatz 4 DSGVO sichergestellt werden, dass die Beschäftigten personenbezogene Daten nur auf Anweisung des Verantwortlichen verarbeiten.

- Bewertung des LfDI (S. 10f.):

Der LfDI führt ergänzend zu § 3 Absatz 2 LDSG aus, dass nach seiner Auffassung die Konzeption des § 3 Absatz 2 LDSG mit seiner Anknüpfung an die alte Rechtslage insoweit unionsrechtsverkürzend sei, als Artikel 29 und Artikel 32 Absatz 4 DSGVO anders als das landesrechtliche Konzept des gesetzlichen „Datengeheimnisses“ von einer auf Dauer angelegten (und nicht nur initialen) Pflicht des Verantwortlichen ausgingen, die Beschäftigten zur Einhaltung datenschutzrechtlicher Vorschriften anzuhalten[40]. Diesen Bedenken sollte im Rahmen der Überarbeitung des LDSG Rechnung getragen werden. Dabei sollte freilich die Strafbarkeit von Beschäftigten unter den Voraussetzungen des § 29 LDSG erhalten bleiben.

Position der Landesregierung:

Die vom LfDI angeführte Pflicht des Verantwortlichen, die Beschäftigten mittels konkreter Maßnahmen stetig zur Einhaltung datenschutzrechtlicher Vorschriften anzuhalten, wird nicht in Abrede gestellt. Sie folgt unmittelbar aus Artikel 29 und 32 Absatz 4 DSGVO und wird durch die Vorschrift des Datengeheimnisses nicht derogiert. Die Vorschrift sollte wegen ihrer Appellfunktion und der Verlängerung des Dienstgeheimnisses über das Beschäftigungsverhältnis hinaus beibehalten werden. Vergleichbare Vorschriften finden sich auch in anderen Landesgesetzen[41].

(2) Bußgeldbewehrung

In seiner ersten Stellungnahme vom November 2020 fordert der LfDI, einen Verstoß der Mitarbeiter in öffentlichen Stellen gegen das Datengeheimnis mit einem Bußgeld zu bewehren.

[39] Vgl. hierzu auch die Ausführungen zu § 29 LDSG.
[40] Vgl. näher Keber in Debus/Sicko, LDSG BW, § 3 LDSG, Rn. 10 ff.
[41] Vgl. z. B. Artikel 11 Bayerisches Datenschutzgesetz, § 41 Datenschutzgesetz Nordrhein-Westfalen.

Er begründet dies folgendermaßen:

In der bisherigen Praxis der Bußgeldbehörde würden Behördenmitarbeiter, die ihre gesetzlichen Datenverarbeitungsbefugnisse überschritten und damit gegen das Datengeheimnis des § 3 Absatz 2 LDSG verstießen, wie Privatpersonen nach der DSGVO und dem BDSG behandelt. Klarer wäre es, dies ausdrücklich im LDSG zu regeln. Es sei nicht nachvollziehbar, weshalb öffentlich Bedienstete sanktionslos gegen Datenschutzbestimmungen verstoßen könnten.

- Bewertung des LfDI (S. 10f.):

Der LfDI hält an seinen Ausführungen in der Form nicht mehr fest. Maßgeblich für eine Sanktionierung Beschäftigter durch ein Bußgeld sei nach der ständigen Praxis des LfDI nicht die Frage, ob die beschäftige Person gegen das Datengeheimnis verstoßen habe, sondern inwieweit sie personenbezogene Daten zu eigenen, nicht-dienstlichen Zwecken verarbeitet habe. Soweit Beschäftigte öffentlicher Stellen zu eigenen Zwecken Daten verarbeiten, unterfielen sie als Verantwortliche (auch sanktionsrechtlich) den Haftungsregeln der DSGVO. In diesem Bereich sei eine Sanktionierung also möglich. Eine Sanktionierung sei dort nicht möglich, wo Beschäftigte zwar gegen Datenschutzvorschriften verstießen, dies aber im Rahmen ihrer Tätigkeit für die öffentliche Stelle machten. In diesem Bereich sei eine Zurechnung zur öffentlichen Stelle als Verantwortliche konsequent.

Position der Landesregierung:

In das LDSG wurden keine Bußgeldtatbestände für Verstöße von Mitarbeitenden aufgenommen. Es wurde davon ausgegangen, dass die Bußgeldtatbestände abschließend in Artikel 83 DSGVO geregelt sind. Es handelt sich jedoch um ein streitiges Thema, das bisher nicht gerichtlich geklärt ist. Außer im Bundesdatenschutzgesetz und im Datenschutzgesetz von Schleswig-Holstein enthalten die Datenschutzgesetze anderer Länder Sanktionsvorschriften für Verstöße von Mitarbeitenden gegen Datenschutzvorschriften[42]. Diese wurden auf der Grundlage von Artikel 84 DSGVO erlassen.

Aus den folgenden Gründen sollte an der bisherigen Regelung festgehalten werden:

Artikel 84 DSGVO erlaubt und fordert weitere Sanktionen in mitgliedstaatlichen Regelungen, und zwar „insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen“. Da Artikel 83 DSGVO Geldbußen gegen natürliche Personen nicht generell ausschließt[43], ergibt

[42] Vgl. z. B. Artikel 23 Absatz 1 Bayerisches Datenschutzgesetz, § 33 Datenschutzgesetz Nordrhein-Westfalen.
[43] Vgl. Artikel 83 in Verbindung mit Artikel 28 Absatz 10 DSGVO.

sich mithin eine Sperrwirkung für landesgesetzliche Bußgeldvorschriften gegen Mitarbeitende.

Der LfDI kommt, wie ausgeführt, zu dem Ergebnis, dass der Bedienstete selbst als Verantwortlicher im Sinne von Artikel 4 Nummer 7 DSGVO handelt und daher mit einem Bußgeld nach Artikel 83 DSGVO sanktioniert werden kann. Eine andere Rechtsauffassung als der LfDI vertritt das Bayerische Landesamt für Datenschutzaufsicht (BayLDA)[44]. Wer dienstliche Daten für private Zwecke missbrauche, werde dadurch nicht zum Verantwortlichen, da hierbei entscheidend sei, wer über die Zwecke der Verarbeitung und die Mittel der Abfragesysteme bestimme: „Der Mitarbeitende mag die Daten zwar zweckwidrig verarbeiten, er bestimmt aber nicht über den Mitteleinsatz. Vielmehr stellt das Beschäftigungsunternehmen die Datenbanken zur Verfügung; der Mitarbeitende macht sich die vorhandene Infrastruktur lediglich zunutze“[45].

Die Entscheidung über die Auslegung des Artikels 83 Absatz 5 DSGVO muss den Gerichten überlassen werden.

Verstöße gegen das Datengeheimnis können ggf. auch dienstrechtlich oder entsprechend der Strafrechtsvorschrift in § 29 LDSG sanktioniert werden.

4. Zulässigkeit der Verarbeitung personenbezogener Daten (§ 4 LDSG)

a) Zum Norminhalt

Diese Regelung wurde auf der Grundlage von Artikel 6 Absatz 1 Buchst. e in Verbindung mit Absatz 3 DSGVO getroffen. Als allgemeine Rechtsgrundlage kann sie für Datenverarbeitungen öffentlicher Stellen zur Erfüllung öffentlicher Aufgaben herangezogen werden, sofern keine bereichsspezifischen Rechtsgrundlagen bestehen. Zugleich ist § 4 LDSG nicht geeignet, wesentliche Eingriffe in das informationelle Selbstbestimmungsrecht zu legitimieren. Da die Regelung keine konkrete Zweckbestimmung enthält, kann sie nur als subsidiäre Rechtsgrundlage angesehen werden. Denn wesentliche Eingriffe in ein Grundrecht, hier das Grundrecht der informationellen Selbstbestimmung, bedürfen nach der Rechtsprechung des Bundesverfassungsgerichts einer speziellen Ermächtigungsgrundlage.

§ 4 LDSG kommt als Rechtsgrundlage für Verarbeitungen durch öffentliche Stellen in Betracht, wenn die Verarbeitung eine in der Zuständigkeit des Verantwortlichen liegende Aufgabe erfüllen soll. Die Bezugnahme auf die Zuständigkeit verdeutlicht, dass der Gesetzgeber die im öffentlichen Interesse liegende Aufgabe dem Verantwortlichen übertragen haben

[44] Vgl. BayLDA, 9. TB 2019, S. 71 f. u. 10. TB 2020, S. 78 f.
[45] BayLDA 10. TB, S. 78.

muss[46]. Des Weiteren ist Voraussetzung, dass die Datenverarbeitung für die Aufgabenerfüllung oder in Ausübung öffentlicher Gewalt erforderlich ist.

Die zu erfüllende Aufgabe ist nicht in § 4 LDSG, sondern in den allgemeinen oder spezifischen Fachgesetzen definiert.

In der Verwaltung wird die Vorschrift des § 4 LDSG insbesondere als Rechtsgrundlage für die Verarbeitung personenbezogener Daten für die Öffentlichkeitsarbeit verwendet. Grundsätzlich ist die Öffentlichkeitsarbeit eine aus dem Demokratieprinzip folgende verfassungsrechtliche Obliegenheit. Daher kann für die Erfüllung dieser Aufgabe grundsätzlich auf die Ermächtigungsgrundlage des § 4 LDSG zurückgegriffen werden.

Daneben wird § 4 LDSG von praktischer Bedeutung, wenn es um bisher nicht geregelte konkrete Datenverarbeitungen geht. In jüngster Zeit wird dies in Bezug auf den Einsatz von KI für Zwecke der Verwaltung und der Justiz diskutiert.

b) Rückmeldungen und Bewertung

aa) Bestimmtheitsgebot

Aus der Landesregierung wurde die Frage gestellt, inwieweit die Generalklausel des § 4 LDSG dem Bestimmtheitsgebot entspreche, da nicht ersichtlich sei, welche Maßnahmen bzw. Grundrechtseingriffe in welcher Tiefe darauf gestützt werden können. Einschränkende Tatbestandsmerkmale lägen nicht vor. Für Eingriffe, die das allgemeine Persönlichkeitsrecht beträfen, werde zusätzlich eine Einwilligung der betroffenen Person für erforderlich gehalten. Angeführt wird die Berichterstattung durch Bild- und Tonaufnahmen. Ggf. könnte daher eine Klarstellung, Konkretisierung oder Einschränkung des § 4 LDSG sinnvoll sein.

- Bewertung des LfDI (S. 14)

Der LfDI hält trotz der in der Literatur geäußerten Kritik die Generalklausel für zulässig, da der Begriff der Erforderlichkeit in Rechtsprechung und Literatur ausreichend geklärt sei. Entscheidend für die Erforderlichkeit sei, dass eine normenklare Regelung bestehe, welche Aufgaben von der Stelle zu erfüllen seien.

Der LfDI weist ebenfalls darauf hin, dass die Generalklausel nur für Datenverarbeitungen mit geringer Eingriffsintensität tauge. Er gehe noch von einer ausreichend normenklaren Regelung aus.

[46] Vgl. Petri in Kühling/Buchner, BDSG § 3 Rn. 8.

Vor allem für neue, bislang nicht spezifisch geregelte Formen (digitaler) Datenverarbeitungen komme der Generalklausel des § 4 LDSG praktische Bedeutung zu.

Position der Landesregierung:

Es entspricht der Auffassung der Landesregierung, dass für alle Eingriffe, die das informationelle Selbstbestimmungsrecht wesentlich berühren, eine spezifische Rechtsgrundlage gefunden bzw. geschaffen werden sollte. Aus denselben Erwägungen, die der LfDI anführt, sollte aber an der Generalklausel festgehalten werden. Zurecht wird im Zusammenhang mit der Generalklausel auf die Öffentlichkeitsarbeit hingewiesen, auf die sogleich einzugehen ist.

bb) Öffentlichkeitsarbeit öffentlicher Stellen

Aus einigen Ressorts und dem Landtag sowie aus dem kommunalen Bereich werden konkrete Regelungen für die viel genutzte Öffentlichkeitsarbeit gewünscht. Diese reiche von der Nutzung sozialer Medien bis zum Streaming von Veranstaltungen, der Anfertigung und Nutzung von Bild- und Tonaufnahmen bis zur Verwendung und Weiterleitung von Kontaktdaten für Einladungen, Weihnachtspost etc. Es bedürfe konkretisierender Regelungen für die Abgrenzung, welche Formen mit der Generalklausel zu legitimieren seien, beziehungsweise für welche die Einwilligung der betroffenen Personen erforderlich sei.

Der LfDI schlägt vor, in § 4 LDSG eine Regelung zur Öffentlichkeitsarbeit zu integrieren, um die Arbeit der Behörden in diesem Bereich zu legitimieren. Nur so könnten rechtsklare und bestimmte Vorgaben für den immer wichtiger werdenden öffentlichen Auftritt von Behörden und anderen öffentlichen Stellen in sozialen Netzwerken geschaffen werden, während der Schutz personenbezogener Daten gewährleistet werde. Er schlägt in seiner Stellungnahme vom November 2020 vor, § 4 LDSG um einen Absatz 2 wie folgt zu ergänzen:

„(2) Als Aufgabe der öffentlichen Stelle gilt auch deren Öffentlichkeitsarbeit. Findet die Öffentlichkeitsarbeit durch Nutzung eines sozialen Netzwerks statt, ist die öffentliche Stelle für die Verarbeitung personenbezogener Daten gemäß Artikel 26 der DSGVO gemeinsam mit dem Anbieter des sozialen Netzwerks verantwortlich. Sie hat die Einrichtung und Einhaltung geeigneter technischer und organisatorischer Maßnahmen nach der DSGVO zu gewährleisten.“

Damit zielt er insbesondere auf die seit dem Urteil des Europäischen Gerichtshofs zu Facebook stark diskutierte gemeinsame Verantwortlichkeit von Facebook und dem Facebook-Fanpage-Betreiber.

- Bewertung des LfDI (S. 15 f.):

Der LfDI befürwortet eine gesetzliche Regelung der Öffentlichkeitsarbeit, um Rechtsunsicherheiten auszuräumen. Dabei sei danach zu differenzieren, welche Datenverarbeitung für die Aufgabenerfüllung erforderlich sei. Hierunter rechnet er z. B. die Speicherung von personenbezogenen Daten angemeldeter Personen für eine behördliche Veranstaltung, Veranstaltungshinweise an die Dienstadressen von Bediensteten anderer Dienststellen im dienstlichen Zusammenhang. Für über die Ausgabenerfüllung hinausgehende Datenverarbeitung bedürfe es dagegen der Einwilligung der betroffenen Personen, wie z. B. bei der Versendung von Newslettern, der Fertigung von Fotografien und Videoaufnahmen von Besucherinnen und Besuchern einer Veranstaltung (sofern dies nicht nach dem Kunsturhebergesetz zulässig ist).

In Bezug auf die Verwendung sozialer Netzwerke hält der LfDI an seiner vorgeschlagenen Formulierung nur noch teilweise fest. Durch die Rechtsprechung des Europäischen Gerichtshofs dürfte ausreichend geklärt sein, unter welchen Voraussetzungen die Nutzung eines sozialen Netzwerks eine gemeinsame Verantwortung bewirke. Es sei für öffentliche Stellen zielführender und datenschutzrechtlich sicherer, wenn öffentliche Stellen für ihre Öffentlichkeitsarbeit durch soziale Netzwerke solche Anbieter auswählten, die die personenbezogenen Daten nicht auch für eigene Zwecke verarbeiteten (z. B. Mastodon).

Position der Landesregierung:

Aus Sicht der Landesregierung besteht ein praktisches Bedürfnis für die datenschutzrechtliche Regelung der Öffentlichkeitsarbeit. Die Landesregierung stimmt dem LfDI zu, dass die Verwendung personenbezogener Daten für die Öffentlichkeitsarbeit auf eine Norm gestützt werden sollte, die bestimmt und rechtsklar regelt, welche Formen in welchem Umfang zulässig sind.

Die Öffentlichkeitsarbeit umfasst neben dem Einsatz sozialer Medien sehr viele Möglichkeiten, beispielsweise:
- Fotografien,
- Fertigen von Bild- und Tonaufnahmen einschließlich deren Verbreitung,
- Streaming von Veranstaltungen,
- Nutzung sozialer Netzwerke,
- Einladung und Organisation von Veranstaltungen.

Diese Tätigkeiten greifen in unterschiedlicher Tiefe in das Recht auf informationelle Selbstbestimmung ein. Die Generalklausel kann die Eingriffe daher nicht ausreichend legitimieren. Es bedarf vielmehr einer spezifizierten Rechtsgrundlage entsprechend Artikel 6 Absatz 1 Buchst.

e und Absatz 3 DSGVO. Diese Rechtsgrundlage zu schaffen, erfordert, das Grundrecht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung mit dem Verfassungsauftrag der Information der Bürgerinnen und Bürger in einem demokratischen Rechtstaat in Einklang zu bringen.

Soweit keine Rechtsgrundlage zur Verfügung steht, kann die entsprechende Datenverarbeitung nur auf eine Einwilligung gemäß Artikel 6 Absatz 1 Buchst. a DSGVO gestützt werden. Sofern dies der Fall ist, sind die besonderen Voraussetzungen für die Wirksamkeit einer Einwilligung zu beachten. Insbesondere ist Freiwilligkeit zu garantieren, die aber im Verhältnis der Behörde zu Bürgerinnen und Bürgern, jedenfalls im Subordinationsverhältnis, in der Regel als nicht gegeben anzusehen ist. Für die öffentliche Verwaltung sollte die Einwilligung als Rechtsgrundlage für eine Datenverarbeitung daher nur dann in Frage kommen, wenn der Eingriff sich nicht auf eine Befugnisnorm stützen lässt, insbesondere, weil die Tiefe des Eingriffs in das Persönlichkeitsrecht dies nicht zulässt bzw. dies für die Aufgabenerfüllung nicht erforderlich ist. Zugleich sollte der Gesetzgeber dafür sorgen, dass die Verwaltung die notwendigen und geeigneten Maßnahmen treffen kann. Hierbei können insbesondere die Grenze, ab der eine Einwilligung zu fordern ist, bestimmt und zugleich die erforderlichen datenschutzrechtlichen Vorkehrungen festgelegt werden.

Leitender Gesichtspunkt für die Abgrenzung zur Notwendigkeit einer Einwilligung sollte sein, ob das Demokratieprinzip eine Information der Öffentlichkeit durch Bild und oder Ton gebietet. Diesbezüglich wird es auch auf das Ausmaß der Betroffenheit ankommen. Im öffentlichen Leben stehende Personen (z. B. Mandatsträgerinnen und Mandatsträger) dürften weniger Schutz ihrer persönlichen Daten benötigen als Zuschauerinnen, Zuschauer oder zufällig anwesende Personen. Für Fotografien ergeben sich die Grenzen aus dem Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG).

Im Hinblick auf die Rechtsprechung des Europäischen Gerichtshofs zur Nutzung von Facebook sind für die datenschutzrechtliche Bewertung sozialer Medien weitere Gesichtspunkte einzubeziehen:

Bereits 2018 hat der Europäische Gerichtshof in einem Verfahren entschieden, dass Betreiber von Fanpages auf Facebook gemeinsam mit Facebook als Dienstanbieter für den Schutz der Nutzerdaten verantwortlich sind[47]. Im zugrundeliegenden Verfahren ging es darum, ob die schleswig-holsteinische Datenschutzbehörde der Wirtschaftsakademie des Landes den Auftritt auf Facebook untersagen durfte. Begründet wurde dies damit, dass weder die Wirtschaftsakademie noch Facebook die Besucher der Fanpage darauf hinwiesen, dass Facebook mittels Cookies sie betreffende personenbezogene Daten erhebe und diese Daten danach verarbeite.

[47] EuGH, Urteil vom 05.06.2018, Rechtssache C-210/16, abrufbar unter CURIA - Ergebnisliste (europa.eu).

51

Seine Entscheidung begründet der Europäische Gerichtshof u. a. damit, dass die Betreiber einer Facebook-Fanpage über das Ausmaß und Mittel der Datenverarbeitung mitentscheiden können. „Auch wenn der bloße Umstand der Nutzung eines sozialen Netzwerks wie Facebook für sich genommen einen Facebook-Nutzer nicht für die von diesem Netzwerk vorgenommene Verarbeitung personenbezogener Daten mitverantwortlich macht, ist indes darauf hinzuweisen, dass der Betreiber einer auf Facebook unterhaltenen Fanpage mit der Einrichtung einer solchen Seite Facebook die Möglichkeit gibt, auf dem Computer oder jedem anderen Gerät der Person, die seine Fanpage besucht hat, Cookies zu platzieren, unabhängig davon, ob diese Person über ein Facebook-Konto verfügt.“[48].

Damit richtet sich die Zulässigkeit der Nutzung sozialer Netzwerke nach den Vorschriften der DSGVO. Die Prüfung der Tatbestandsvoraussetzungen des Artikels 26 DSGVO entscheidet darüber, ob eine gemeinsame Verantwortlichkeit anzunehmen ist und vor allem, wie weit diese reicht. Dies kann bezüglich verschiedener sozialer Netzwerke unterschiedlich zu bewerten sein, je nachdem wie die Verantwortlichkeit ausgestaltet ist. Insgesamt ist zu konstatieren, dass bezüglich der Nutzung sozialer Netzwerke grundlegende Rechtsfragen bisher nicht abschließend rechtlich geklärt sind.

Mit einer landesrechtlichen Regelung könnte der Einsatz sozialer Medien für die Öffentlichkeitsarbeit im LDSG grundsätzlich legitimiert werden. Auch zur Gewährleistung der öffentlichen Sicherheit kann die Nutzung sozialer Medien zulässig sein. Dies betrifft die Nutzung durch Polizei oder Katastrophenschutz. Allerdings ist der Landesgesetzgeber im Hinblick auf den Anwendungsvorrang der DSGVO daran gehindert, die Voraussetzungen der Zulässigkeit zu regeln. Die gemeinsame Verantwortlichkeit kann nicht per Landesgesetz konstituiert oder ausgeschlossen werden. Allenfalls könnte die Verwendung sozialer Medien unter der Voraussetzung, dass die Nutzung mit der DSGVO konform ist, im Hinblick auf zu treffende (technische und organisatorische Maßnahmen) geregelt werden. Die vom LfDI in seiner Broschüre „Wesentliche Anforderungen an die behördliche Nutzung Sozialer Netzwerke“ vorgeschlagenen Maßnahmen sind geeignet, die Schranken der Nutzung festzulegen. Hierzu gehören ein schriftliches Nutzungskonzept, die Einhaltung der Informationspflichten nach § 5 des Telemediengesetzes, eine Datenschutzerklärung, eine kontinuierliche Betreuung des Accounts sowie das Angebot alternativer Informations- und Kommunikationswege.

cc) Einsatz von KI datenschutzrechtlich ermöglichen

Die Möglichkeiten der KI sollten nach Auffassung der Landesregierung nicht nur der privaten Wirtschaft, sondern auch der Verwaltung und der Justiz selbst zur Verfügung stehen. Im Zuge

[48] A.a.O. Rn. 35.

des demografischen Wandels und des damit einhergehenden Fachkräftemangels sowie der zunehmenden Digitalisierung der Gesellschaft wird die Verwaltung in Zukunft auf Einsatz von KI zur Aufgabenbewältigung angewiesen sein.

Aktuell sind die technischen Möglichkeiten jedoch nur eingeschränkt in technische Produkte und KI-Anwendungen für die Verwaltung umsetzbar, da keine spezifische Rechtsgrundlage vorhanden ist und die Generalklausel des § 4 LDSG wie gesehen nur für eingriffsarme Datenverarbeitungen herangezogen werden sollte.

Das Europäische Parlament und der Rat der EU haben die „Verordnung über künstliche Intelligenz“ erlassen (im folgenden KI-Verordnung)[49]. Danach wird für die Anwendung von KI, sofern personenbezogene Daten verarbeitet werden sollen, eine datenschutzrechtliche Rechtsgrundlage vorausgesetzt. Erwägungsgrund 63 Satz 3 führt dazu aus:
„Diese Verordnung sollte nicht so verstanden werden, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, gegebenenfalls einschließlich besonderer Kategorien personenbezogener Daten, bildet, es sei denn, in dieser Verordnung ist ausdrücklich etwas anderes vorgesehen.“ Ausdrückliche Regelungen zur Verarbeitung personenbezogener Daten enthalten Artikel 10 Absatz 5 und Artikel 59 der KI-Verordnung.

Die KI-Verordnung setzt für die Regulierung bei den Gefahren von KI-Systemen und KI-Modellen an. Je nach Risiko werden spezifische Anforderungen gestellt. KI-Praktiken, die wegen ihres unannehmbaren Risikos als Bedrohung für die Grundrechte der EU-Bürgerinnen und -Bürger eingestuft werden, werden verboten[50]. Hierzu zählen unter anderem kognitive Verhaltensmanipulation, Emotionserkennung am Arbeitsplatz, Sozialkreditsysteme. Hochriskante Anwendungen werden strengen Anforderungen unterworfen und verlangen ein umfassendes Qualitäts- und Risikomanagementsystem[51]. Weniger Pflichten gelten bei KI-Modellen mit allgemeinem Verwendungszweck mit und ohne systemisches Risiko[52]. Der Entwicklung und der Erprobung von KI-Systemen und damit der Forschung und der Innovation der Verwaltung sowie der Justiz kann zugutekommen, dass die Etablierung von KI-Reallaboren zum Erproben von KI-Technologien zulässig ist[53].

Soweit in KI-Reallaboren die Weiterverarbeitung personenbezogener Daten erforderlich ist, sieht Erwägungsgrund 140 vor:
„Die vorliegende Verordnung sollte im Einklang mit Artikel 6 Absatz 4 und Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 und den Artikeln 5, 6 und 10 der Verordnung

[49] Veröffentlicht am 12. Juli 2024, Quelle siehe unter Fußnote 21.
[50] Vgl. Artikel 5 der KI-Verordnung.
[51] Vgl. Artikel 6 ff. in Verbindung mit Anhang III der KI-Verordnung.
[52] Vgl. Art. 51 ff. der KI-Verordnung.
[53] Vgl. Artikel 57 ff. der KI-Verordnung.

(EU) 2018/1725 sowie unbeschadet des Artikels 4 Absatz 2 und des Artikels 10 der Richtlinie (EU) 2016/680 die Rechtsgrundlage für die Verwendung – ausschließlich unter bestimmten Bedingungen – personenbezogener Daten, die für andere Zwecke erhoben wurden, zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse innerhalb des KI-Reallabors durch die Anbieter und zukünftigen Anbieter im KI-Reallabor bilden. Alle anderen Pflichten von Verantwortlichen und Rechte betroffener Personen im Rahmen der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 gelten weiterhin. Insbesondere sollte diese Verordnung keine Rechtsgrundlage im Sinne des Artikels 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 und des Artikels 24 Absatz 2 Buchstabe b der Verordnung (EU) 2018/1725 bilden. Anbieter und zukünftige Anbieter im Reallabor sollten angemessene Schutzvorkehrungen treffen und mit den zuständigen Behörden zusammenarbeiten, unter anderem, indem sie deren Anleitung folgen und zügig und nach Treu und Glauben handeln, um etwaige erhebliche Risiken für die Sicherheit, die Gesundheit und die Grundrechte, die bei der Entwicklung, bei der Erprobung und bei Versuchen im Reallabor auftreten können, zu mindern."

Dementsprechend soll in Artikel 59 zur Entwicklung von KI-Systemen im Reallabor unter bestimmten Prämissen die Weiterverarbeitung von personenbezogenen Daten zur Wahrung eines erheblichen öffentlichen Interesses durch eine Behörde oder eine andere natürliche oder juristische Person und in einem oder mehreren der folgenden Bereiche zugelassen werden: der öffentlichen Sicherheit, der öffentlichen Gesundheit, dem Umweltschutz, dem Klimaschutz, nachhaltiger Energie, der Widerstandsfähigkeit von Verkehrssystemen und kritischen Infrastrukturen, aber auch zugunsten der Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste.

Die KI-Verordnung gilt wie die DSGVO allgemein und unmittelbar. Soweit sie keine datenschutzrechtlichen Regelungen enthält, müssen die entsprechenden Rechtsgrundlagen im Wesentlichen außerhalb der KI-Verordnung gefunden werden.

Es wird daher vorgeschlagen, für den Einsatz von KI besondere landesrechtliche Regelungen zu erlassen, um mindestens folgende drei Möglichkeiten datenschutzrechtlich zuzulassen.

Möglichkeit 1: Geschäftsprozessautomation

Zugelassen werden sollte die Verarbeitung personenbezogener Daten zu Entwicklung, Testung oder Monitoring von Systemen der Informationstechnik (IT-Systeme), die der Vereinfachung oder der teilweisen oder vollständigen Automation von Geschäftsprozessen öffentlicher Stellen dienen. Diese IT-Systeme könnten dazu beitragen, die öffentlichen Stellen mehr als nur unerheblich zu entlasten, die Qualität der Geschäftsprozesse der öffentlichen Stellen zu

steigern oder die im öffentlichen Interesse erbrachten Leistungen der öffentlichen Stellen weniger aufwändig anzubieten. Zugleich könnte der Einsatz von KI einen Beitrag dazu leisten, in erheblichem öffentlichen Interesse liegende Ziele, beispielsweise den Schutz der natürlichen Lebensgrundlagen oder die Sicherstellung europäischer technologischer Souveränität, zu befördern.

Möglichkeit 2: Erzeugung anonymisierter und pseudonymisierter Datensätze

Zugelassen werden sollte die Anonymisierung und Pseudonymisierung personenbezogener Daten zur Herstellung von Test-, Trainings oder Referenzdatensätzen, soweit mit den so erzeugten Datensätzen im öffentlichen Interesse liegende Aufgaben wahrgenommen werden sollen, wozu auch die unter Möglichkeit 1 genannte Vereinfachung oder teilweise oder vollständige Automation von Geschäftsprozessen gehört.

Möglichkeit 3: Experimentierklausel

Zugelassen werden sollte die Verarbeitung personenbezogener Daten zur Entwicklung oder Erprobung von Technologie für den Einsatz bei öffentlichen Stellen, soweit sich die Entwicklung oder Erprobung in einem Experimentellen- oder einem Prototypenstadium befindet und die Verarbeitung personenbezogener Daten nicht umfangreich ist.

Datenschutzrechtlich bestehen mehrere Probleme, die zu lösen sind:

- Zum einen bedürfen mitgliedstaatliche Regelungen auf der Grundlage von Artikel 6 Absatz 1 Buchst. e in Verbindung mit Absatz 3 DSGVO der Festlegung eines Zweckes, für den die Datenverarbeitung erforderlich ist.

  Lösungsvorschlag:
  Hierzu wird die Auffassung vertreten, dass der Einsatz von KI analog zu den Prozessen der Digitalisierung grundsätzlich als Annex zur Aufgabenerfüllung zugelassen werden sollte. Voraussetzung ist, dass die KI-Technik die Prinzipien des Vorrangs des menschlichen Handelns, der menschlichen Aufsicht und Verantwortlichkeit, der Transparenz, der technischen Robustheit und Sicherheit, der Vielfalt, Nicht-Diskriminierung, Fairness sowie des gesellschaftlichen und ökologischen Wohlergehens verfolgt[54].Hierfür wird die KI-Verordnung den wesentlichen Rahmen setzen. Landesrechtlich bedarf es der notwendigen Ermächtigungsgrundlage für die Verarbeitung personenbezogener Daten.

[54] Vgl. § 1 des Gesetzes über die Möglichkeit des Einsatzes von datengetriebenen Informationstechnologien bei öffentlich-rechtlicher Verwaltungstätigkeit (IT-Einsatz-Gesetz – ITEG) vom 16. März 2022.

Allerdings kann das Training entsprechender Systeme mindestens in einigen Fällen nicht der Aufgabenerfüllung im Sinne des § 4 LDSG zugerechnet werden. Hierfür bedarf es einer eigenständigen Rechtsgrundlage, sofern hierfür personenbezogene Daten verarbeitet werden sollen[55]. Da es sich um eine Zweckänderung handelt, muss die Rechtsvorschrift den Voraussetzungen des Artikels 6 Absatz 4 in Verbindung mit Artikel 23 DSGVO entsprechen.

- Des Weiteren ist Datenminimierung für die Entwicklung von KI-Technik kontraproduktiv, da die Qualität von KI-Techniken von der Anzahl und Qualität der Trainingsdaten abhängt.

  Lösungsvorschlag:
  Deshalb muss die Verwendung nach dem aktuellen Stand der Technik automatisiert anonymisierter und pseudonymisierter Daten in den Blick genommen werden. Es sollte eine datenschutzrechtliche Rechtsgrundlage zur Anonymisierung von Daten geschaffen werden.

- Die DSGVO verlangt gemäß Artikel 5 Absatz 1 Buchst. a eine transparente Verarbeitung. Die Betroffenenrechte müssen erfüllt oder im Rahmen des Artikels 23 DSGVO beschränkt werden.

  Lösungsvorschlag:
  Die Datenschutzerklärungen sollten entsprechende Verarbeitungen aufführen. Nach Möglichkeit sollte nachvollziehbar bleiben, welche Daten einer KI-Anwendung zugrunde liegen. Sofern dies nicht möglich ist, ist über Beschränkungen der Betroffenenrechte nachzudenken. Für Trainingsdaten könnte ggf. auch auf die in der KI-Verordnung geregelten Reallabore zurückgegriffen werden.

Aus diesen Erwägungen ergibt sich, dass eine Experimentierklausel (Möglichkeit 3) am ehesten auf datenschutzrechtliche Probleme stößt, da personenbezogene Daten ohne Anonymisierung oder Pseudonymisierung weiterverarbeitet werden sollen, während die DSGVO den Grundsatz der Zweckbindung und Datenminimierung verfolgt. Geeignete Schutzmaßnahmen müssen gefunden werden.

Inwieweit eine Verarbeitung personenbezogener Daten mittels KI und eine Zweckänderung zugunsten der Entwicklung von KI-Systemen zugelassen werden kann, bedarf weiterer Vertiefung im Rahmen des Gesetzgebungsverfahrens.

[55] Vgl. § 8 Absatz 1 ITEG.

5. Datenverarbeitung zu anderen Zwecken (§ 5 LDSG)

a) Zum Norminhalt

Während § 4 LDSG die allgemeine Erlaubnisnorm zur Verarbeitung personenbezogener Daten darstellt, regelt § 5 LDSG die Datenverarbeitung zu anderen Zwecken. Diese ist nach der DSGVO nur eingeschränkt möglich, da personenbezogene Daten nach dem Grundsatz der Zweckbindung nur zu einem bestimmten und legitimen Zweck verarbeitet werden dürfen. Die Regelung stellt daher eine Durchbrechung dieses Grundsatzes auf der Grundlage des Artikels 6 Absatz 4 DSGVO sowie Artikel 23 Absatz 1 DSGVO dar und ist entsprechend restriktiv gestaltet. Weitere zulässige Zweckänderungen können sich direkt aus Artikel 6 Absatz 4 DSGVO ergeben, wenn die Verarbeitung mit dem Primärzweck vereinbar ist. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke sowie für statistische Zwecke gilt gemäß Artikel 5 Absatz 1 Buchst. b DSGVO als vereinbar mit dem ursprünglichen Zweck.

b) Rückmeldungen und Bewertung

aa) Zu § 5 Absatz 1 Nummer 1 LDSG

Zweckänderung zu Gemeinwohlzwecken

Eine Rückmeldung aus einem Regierungspräsidium weist darauf hin, dass die Begriffe „Abwehr erheblicher Nachteile für das Gemeinwohl“ oder „zur Wahrung erheblicher Belange des Gemeinwohls“ in § 5 Absatz 1 Nummer 1 LDSG konkretisierungsbedürftig seien. Für den Regionalen Sonderstab gefährliche Ausländer sei insoweit relevant, dass hierunter auch die Ausweisung oder Verlustfeststellung eines Ausländers subsumierbar sei.

- Bewertung des LfDI (S. 19f.):

Der LfDI zweifelt wegen der Weite der Vorschrift an der Europarechtskonformität der Vorschrift. Artikel 23 Absatz 2 Buchst. a DSGVO verlange die Festlegung der Verarbeitungszwecke durch den Gesetzgeber.

Position der Landesregierung:

Eine weitere Konkretisierung des Gemeinwohlbegriffs sollte geprüft werden, da der Begriff des Gemeinwohls bei den in Artikel 23 DSGVO aufgeführten Schutzzielen nicht explizit aufgeführt ist. Er ist von der Intention gleichzusetzen mit den in Artikel 23 Absatz 1 Buchst. e DSGVO geschützten Zielen des allgemeinen öffentlichen Interesses der Union oder eines

Mitgliedstaats. Alle Gemeinwohlziele müssen die gleiche Relevanz aufweisen wie die genannten Ziele im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit. Das Gegenteil davon sind die Interessen oder Wünsche Einzelner oder einer Gruppe dieser Gemeinschaft[56].

bb) Erweiterung der Zweckänderungstatbestände

Die Rückmeldungen zu § 5 LDSG weisen auf zusätzliche Bedarfe für Zweckänderungen hin. Im Kultusministerium stellte sich immer wieder die Frage, ob die Voraussetzungen des § 5 Absatz 1 LDSG erfüllt seien, wenn beispielweise die Polizei, die Staatsanwaltschaft (wegen möglicher Straftaten) oder das Jugendamt (wegen potentieller Kindesgefährdung) bei Schulen personenbezogene Daten erheben wollten.

Normenklare Regelungen werden befürwortet, um eindeutige Rechtsgrundlagen für die Praxis zur Verfügung zu stellen. Zu beachten ist aber, dass die DSGVO nur im Rahmen der Öffnungsklausel des Artikels 6 Absatz 4 Ausnahmen vom Zweckbindungsgrundsatz zulässt. Voraussetzung ist, dass die Rechtsvorschrift „in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt“. Damit werden die zulässigen Zwecke für Zweckänderungen beschränkt und sind jeweils aufzuführen. Leitend ist das öffentliche Interesse unter Einhaltung des Verhältnismäßigkeitsgrundsatzes.

(1) Strafverfolgungszwecke

Seitens der Polizei kam die Rückmeldung, dass die Tatbestände, die eine Zweckänderung betreffen, nicht ausreichend seien. Es wurde angemerkt, dass § 5 Absatz 1 LDSG zu eng gefasst sei. Relevant werde dies insbesondere bei der Zweckänderung von Daten für die Verfolgung von Straftaten und Ordnungswidrigkeiten, welche keine Taten von erheblicher Bedeutung im Sinne des § 5 Absatz 1 Nummer 3 LDSG darstellten.

In seiner Stellungnahme vom November 2020 weist der LfDI darauf hin, dass § 5 Absatz 1 LDSG im Hinblick auf das Erfordernis, Daten zweckändernd für Strafverfolgungszwecke weiter zu verarbeiten, zu eng gefasst sei und diesbezüglich keine ausreichende Ermächtigungsgrundlage enthalte. Er empfiehlt, sich an der Fassung des § 23 Absatz 1 BDSG zu orientieren.

[56] Vgl. Bundeszentrale für politische Bildung Gemeinwohl | bpb.de.

Aus dem Kultusministerium wurde Unsicherheit darüber berichtet, ob die Voraussetzungen des § 5 LDSG in Fällen erfüllt seien, in denen Schulen personenbezogene Daten (wegen möglicher Straftaten) an die Polizei, Staatsanwaltschaft oder das Jugendamt (wegen potentieller Kindesgefährdung) übermitteln sollten.

- Bewertung des LfDI (S. 20):

Der LfDI tritt der Forderung, die Vorschrift generell auf die Verfolgung von Ordnungswidrigkeiten auszuweiten, entgegen. Die Öffnungsklausel des Artikels 23 Absatz 1 Buchst. d DSGVO spreche nur von Straftaten. Für die notwendige Konkretisierung könne auf § 44 Absatz 10 Satz 3 PolG zurückgegriffen werden, wonach die Bedeutung einer Ordnungswidrigkeit erheblich ist, „wenn nach den Umständen des Einzelfalls ein Schaden für ein wichtiges Rechtsgut oder für andere Rechtsgüter in erheblichem Umfang droht oder wenn die betreffende Vorschrift ein sonstiges wichtiges Interesse der Allgemeinheit schützt."

Im Übrigen beziehe sich die Vorschrift nur auf Ordnungswidrigkeiten von erheblicher Bedeutung, während diese Beschränkung nicht für Straftaten gelte, da Artikel 23 Absatz 1 Buchst. d DSGVO Straftaten generell umfasse.

Position der Landesregierung:

Zur Klarstellung wird empfohlen, sich hinsichtlich der Zweckänderung am Wortlaut des § 23 Absatz 1 Nummer 4 BDSG zu orientieren. Danach ist „die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung … zulässig, wenn…sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist..". Die vorliegende Fassung wird als zu eng geführt angesehen.

Mit der neuen Fassung würde entsprechend der Fragestellung des Kultusministeriums klargestellt, dass Schulen personenbezogene Daten an die Polizei oder Staatsanwaltschaft zur Verfolgung von Straftaten übermitteln dürfen, sofern dies notwendig und verhältnismäßig ist. Für die Übermittlung an das Jugendamt ist ggf. auf § 5 Absatz 1 Nummer 2 LDSG zurückzugreifen.

Aus polizeilicher Sicht ist es, wie in § 23 BDSG geregelt, vorzugswürdig, in Bezug auf die Verfolgung von Ordnungswidrigkeiten keine Einschränkung nur für Ordnungswidrigkeiten

von erheblicher Bedeutung vorzunehmen. Es widerspricht dem Gerechtigkeitsempfinden, Ordnungswidrigkeiten aus Gründen des Datenschutzes nicht zu verfolgen, obwohl die Verfolgung aus Opportunitätsgründen angezeigt ist. Anzumerken ist, dass auch ohne die Beschränkung auf Ordnungswidrigkeiten von erheblicher Bedeutung immer die Verhältnismäßigkeit der Verarbeitung personenbezogener Daten zu prüfen ist. Eine Änderung wird daher empfohlen.

(2) Disziplinarmaßnahmen

Es wird seitens des Landespolizeipräsidiums des Weiteren vorgeschlagen, eine Regelung zur Weiterverwendung von Daten zur Einleitung von Disziplinarmaßnahmen einzufügen. Es gebe Fälle, in denen Beamte im privaten Lebensbereich gegen Vorschriften des Beamtenstatusgesetzes verstießen, ohne dass Straftaten oder Ordnungswidrigkeiten vorliegen. Eine Informationsmöglichkeit bzw. Informationspflicht an den Dienstherren sei in solchen Fällen – welche keine Straftaten oder Ordnungswidrigkeiten darstellten, jedoch dennoch für das Beamtenverhältnis von Relevanz seien – daher nicht nach § 5 LDSG möglich.

- Bewertung des LfDI (S.21):

Der LfDI sieht keinen Bedarf für eine entsprechende Regelung. Innerhalb einer Dienststelle lasse sich bei Pflichtverletzungen eine Verarbeitung personenbezogener Daten über § 15 LDSG legitimieren. Allenfalls, wenn bekannt gewordene Pflichtverletzungen von Beschäftigten anderer öffentlicher Stellen an deren Dienstherrn weitergegeben werden sollten, könnte eine Ermächtigung fehlen.

Position der Landesregierung:

Die Landesregierung schließt sich der Auffassung des LfDI an. Des Weiteren wird es für schwierig angesehen, eine entsprechende Erweiterung auf Artikel 23 Absatz 1 DSGVO zu stützen. Es sind auch keine sonstigen Landesdatenschutzgesetze bekannt, die eine solche Regelung enthalten. Hinzuweisen ist auf die spezialgesetzliche Regelung in § 19 des Landesdisziplinargesetzes, die Übermittlungsbefugnisse für innerdienstliche Informationen enthält.

(3) Landtagsanfragen

Es wurde vorgeschlagen, die Weiterverwendung personenbezogener Daten zur Beantwortung von Landtagsanfragen ausdrücklich zu erwähnen.

- Bewertung des LfDI (S. 19):

Dem LfDI erscheint eine eigene gesetzliche Regelung als wertvoll für die Praxis. Diesbezüglich bietet er seine Expertise an.

Position der Landesregierung:

Die Thematik der Verarbeitung von Daten für die Beantwortung von Landtagsanfragen berührt verfassungsrechtliche Fragen. Es wird daher nicht für ausreichend erachtet, die Verwendung von Daten zur Beantwortung von Landtagsanfragen in § 5 LDSG zu regeln. Nähere Ausführungen hierzu finden sich unten zu § 6 LDSG.

(4) Adressdaten und politische Arbeit

Dem Landtag ist es ein Anliegen, Daten für das Veranstaltungsmanagement weiternutzen zu können. Auch nach Auffassung des LfDI wäre im Bereich der „politischen Arbeit“ eine Erweiterung denkbar, um z. B. Kontaktdaten für Einladungen zu öffentlichen Anhörungen, zum Erfahrungsaustausch etc. zu verwenden.

Einige Kommunen wünschen sich eine Rechtsgrundlage für die Weitergabe von Adressdaten an kommunale Unternehmen und Einrichtungen mit eigener Rechtspersönlichkeit (z B. Musik-, Kunst- und Volkshochschulen, die als gGmbH oder als eingetragener Verein organisiert sind), damit diese Adressaten werbliche Maßnahmen gezielt durchführen können.

- Bewertung des LfDI (S. 11, 16):

In Bezug auf die Verarbeitung von Adressdaten unterscheidet der LfDI zwischen der Erhebungsbefugnis der kommunalen Einrichtungen einerseits und der Übermittlungsbefugnis der Meldebehörden auf der anderen Seite. Für letzteres sieht er das BMG als maßgebliche Vorschrift. In § 46 BMG seien unter den dort genannten Voraussetzungen Gruppenauskünfte gestattet. Kritischer sieht er die Erhebungs- und Verwendungsbefugnis der Musik-, Kunst- und Volkshochschulen für werbliche Zwecke. Hier solle bedacht werden, dass die genannten Schulen als öffentliche Stellen vielfach mit privaten Stellen mit einem ähnlichen Leistungsangebot konkurrieren. Als datensparsamere Variante schlägt er die Nutzung des Adressmittlungsverfahrens in Betracht, bei dem die Kommune die Versendung der Werbepost im Auftrag der Schulen vornimmt, ohne der Schule gegenüber die Identität der Empfängerinnen und Empfänger offenzulegen.

Der LfDI zieht die Grenze für die Verarbeitung von Kontaktdaten dort, wo diese zur Aufgabenerfüllung erforderlich ist.

Position der Landesregierung:

Dem LfDI ist zuzustimmen, dass in Bezug auf die Übermittlung von Adressdaten durch die Meldebehörden das BMG als Lex specialis Anwendung findet.

Die Frage der Verwendung von Adressdaten führt zurück zur Rechtsgrundlage für die Öffentlichkeitsarbeit. Wie unter § 4 LDSG ausgeführt, erfordert moderne Öffentlichkeitsarbeit Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Es bedarf klarer Regelungen, bis zu welchem Maß Eingriffe zulässig sind. Die Weiterverwendung von Kontaktdaten für (werbliche) Zwecke öffentlicher Stellen oder des Landtags wäre nach Auffassung der Landesregierung ein weiterer Fall, in dem einer Zweckänderung zugestimmt werden könnte, sofern der öffentlichen Stelle ein Auftrag zur politischen Bildung, zur Bürgerinformation oder ein Erziehungsauftrag obliegt.

Hierfür sprechen auch Überlegungen zur Sozialadäquanz. Eine Verwendung im Rahmen des sozial Üblichen und von der Allgemeinheit Gebilligten sollte zulässig sein. Dies kann z. B. bei der Verwendung von Adressen für Einladungen in der Regel angenommen werden. Schwerwiegende Folgen für die betroffenen Personen dürften diesbezüglich nicht zu erwarten sein. Wie der LfDI richtig anmerkt, sind dabei insbesondere der Grundsatz der Datenminimierung sowie die Voraussetzung der Erforderlichkeit zu beachten. Des Weiteren ist ein möglicher Widerspruch zu beachten.

Eine gesetzliche Regelung ist insoweit nur erforderlich, als die Zweckänderung nicht bereits durch Artikel 6 Absatz 4 DSGVO abgedeckt ist.

(5) Glückwunschschreiben im kommunalen Bereich

Im kommunalen Bereich besteht Unsicherheit über die Verwendung von Melderegisterdaten für Glückwunschschreiben zu Geburtstagen, insbesondere Jubiläen.

Position der Landesregierung:

Die Weitergabe von Melderegisterdaten beurteilt sich nach dem Melderecht. Das BMG erlaubt die Weiterleitung der genannten Daten an Mandatsträger gemäß § 50 BMG. Gemäß § 50 Absatz 5 BMG steht den betroffenen Personen aber ein Widerspruchsrecht zu. Des Weiteren ist die Herausgabe zur Aufgabenerfüllung, auch innerhalb der Verwaltungseinheit, gemäß

§§ 37, 34 BMG zulässig. Bei Herausgabe zur Aufgabenerfüllung obliegt der Meldebehörde die Prüfung, ob diese zur öffentlichen Aufgabenerfüllung erforderlich ist. Auch hier ist ggf. ein vorliegender Widerspruch zu beachten. Datenschutzrechtlich ist also entscheidend, ob die Daten zur Aufgabenerfüllung erforderlich sind.

Die Landesregierung vertritt die Auffassung, dass Jubiläumsgratulationen zur Aufgabenerfüllung des Bürgermeisters gehören. Dementsprechend könnte für die Erhebung und Weiterverarbeitung der Daten hier auf die Generalklausel des § 4 LDSG zurückgegriffen werden.

Davon zu unterscheiden ist die Veröffentlichung der Jubilare im Amtsblatt oder sonstige öffentliche Gratulation. Für diese bedarf es einer eigenständigen Rechtsgrundlage. Eine solche ergibt sich nicht aus dem Melderecht. Auch das LDSG würde hierzu nur ermächtigen, wenn die Veröffentlichung als öffentliche Aufgabe angesehen werden könnte. Dies wird hier nicht vertreten. Im Ergebnis sollte die Veröffentlichung durch die Gemeinde daher nur mit Einwilligung der Jubilare erfolgen.

cc) Zu § 5 Absatz 4 LDSG

Protokolldaten

Das Landespolizeipräsidium wies darauf hin, dass die Übermittlung von Protokolldaten hiernach unter anderem möglich sei, wenn sie zur „Verhütung und Verfolgung von Straftaten gegen Leib, Leben oder Freiheit einer Person erforderlich sind“. Mit diesen Tatbestandsvoraussetzungen lege das LDSG hier einen höheren Maßstab an, als beispielsweise die JI-Richtlinie[57], das BDSG[58], das BMG[59] und nicht zuletzt das PolG[60]. Die DSGVO enthalte hierzu keine entsprechende Regelung.

- Bewertung des LfDI (S. 21):

Eine Aufweichung der Norm durch eine Entfernung der Anforderungen des § 5 Absatz 4 LDSG könnte zu einer unverhältnismäßigen Zweckentfremdung personenbezogener (Protokoll)Daten führen, die es zu vermeiden gelte. Ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs gespeicherte Daten unterlägen einer engen Zweckbindung im Sinne des Artikels 5 Absatz 1 Buchst. b DSGVO. Diese spiegele sich richtigerweise in § 5 Absatz 4 LDSG wider. Zudem sei darauf hinzuweisen, dass neben § 5 Absatz 4 LDSG weitere spezialgesetzliche Ermächtigungen zur Weiterverarbeitung, insbesondere im Straf- oder Steuerrecht, bestünden.

[57] Vgl. Artikel 25 Abs. 2 JI-Richtlinie, der nur von „Strafverfahren“ spricht.
[58] Vgl. § 76 Abs. 3 BDSG, „Strafverfahren“.
[59] Vgl. § 40 Abs. 4 BMG „Strafverfahren“.
[60] Vgl. § 73 Abs. 3 PolG Strafverfahren“.

63

Position der Landesregierung:

Die entsprechende Regelung im BDSG beruht auf Artikel 25 Absatz 2 der JI-Richtlinie. Das LDSG hat sich dagegen an der DSGVO zu orientieren. Zwar erlaubt Artikel 6 Absatz 4 in Verbindung mit Artikel 23 Absatz 1 Buchst. d DSGVO die Aufhebung der Zweckbindung für die Verfolgung von Straftaten, aber nur, soweit dies eine notwendige und verhältnismäßige Maßnahme darstellt. Hieran bestehen im Hinblick auf die schrankenlose Verwendung von Daten, die ausschließlich der Datensicherung oder Datenschutzkontrolle dienen, für die Verfolgung von Straftaten Zweifel. Zu argumentieren ist hier auch mit dem Normzweck der Vorschrift. Die strikte Zweckbindung im Hinblick auf die in § 5 Absatz 4 LDSG genannten Daten soll ausschließen und verhindern, dass die Verwendung dieser zusätzlich angelegten Datenbestände datenschutzwidrig als Informationsgrundlage für andere Zwecke den Einsatz wirksamer Datenschutz- und Sicherungsmethoden indirekt behindert[61]. Deshalb sollte die Erweiterung der Vorschrift unterbleiben.

Andere Landesdatenschutzgesetze unterwerfen personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle verarbeitet werden – sofern überhaupt eine Regelung erfolgt – ebenfalls einer strengen Zweckbindung[62].

6. Übermittlung personenbezogener Daten (§ 6 LDSG)

a) Zum Norminhalt

Die Datenübermittlung ist ein Unterfall der Datenverarbeitung. Sie unterliegt daher denselben Voraussetzungen wie die Datenverarbeitung selbst, nämlich dem in Artikel 6 Absatz 1 DSGVO geregelten Verbot mit Erlaubnisvorbehalt. Sofern sie also in Wahrnehmung einer Aufgabe erfolgt, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, ist sie entsprechend Buchst. e des genannten Artikels zulässig. Das Recht der Mitgliedstaaten hat hierfür gemäß Artikel 6 Absatz 3 DSGVO die erforderlichen Rechtsgrundlagen bereitzustellen. In der Regel sind die Voraussetzungen für Datenübermittlungen fachspezifisch geregelt. Im allgemeinen Datenschutzrecht werden nur subsidiär die Voraussetzungen für Datenübermittlungen geregelt. Zu unterscheiden sind die Fälle, in denen Daten zur Erfüllung öffentlicher Aufgaben erhoben und übermittelt werden und diejenigen, in denen Daten zu einem anderen Zweck übermittelt werden sollen, als sie erhoben wurden.

[61] Vgl. Osterried in Debus/Sicko, LDSG BW, § 5 Rn. 93.
[62] Vgl. Artikel 6 Absatz 4 Bayerisches Datenschutzgesetz, § 6 Absatz 4 Niedersächsisches Datenschutzgesetz, § 4 Absatz 4 Datenschutzgesetz für das Land Mecklenburg-Vorpommern, jeweils ohne Ausnahme.

Während für den erstgenannten Fall, sofern keine fachspezifische Regelung besteht, auf § 4 LDSG zurückzugreifen ist, stellt § 6 LDSG klar, dass für den letztgenannten Fall dieselben Voraussetzungen vorliegen müssen wie für eine Zweckänderung nach § 5 LDSG. In § 6 LDSG wird auch der Sonderfall der Übermittlung an nichtöffentliche Stellen geregelt.

Ein eigenständiger Regelungsgehalt kommt § 6 Absatz 2 und Absatz 3 LDSG zu. Dort wird die Verantwortlichkeit bei Datenübermittlung aufgrund eines Ersuchens oder aufgrund eines automatisierten Abrufverfahrens geregelt.

Zu beachten ist, dass die Regelung zur Datenübermittlung aufgrund eines Ersuchens nicht der Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Doppeltürmodell widerspricht. Wegen des Gesetzesvorbehalts für Grundrechtseingriffe bedürfen sowohl das Ersuchen als auch die korrespondierende Datenübermittlung einer eigenen Rechtsgrundlage in einfachgesetzlichen Vorschriften.

b) Rückmeldungen und Bewertung

aa) Zu § 6 Absatz 1 LDSG

(1) Übermittlung personenbezogener Daten an den Landtag

Im Rahmen der Beantwortung von Landtagsanfragen ist die Frage zu beantworten, in welchem Umfang personenbezogene Daten übermittelt werden dürfen. Aus Gründen der Rechtssicherheit und Rechtsklarheit wurde hierfür die Schaffung einer Rechtsgrundlage vorgeschlagen.

- Bewertung des LfDI (S. 19):

Der LfDI hält eine gesetzliche Regelung für wertvoll für die Praxis. Denn für die Beantwortung von Landtagsanfragen sei unmittelbar auf Verfassungsrecht zurückgreifen, was zu Verunsicherung führe. Der LfDI könnte seine in dieser Frage gesammelte Expertise für die Beratung einer geeigneten Rechtsvorschrift zur Verfügung stellen. Hierbei sei auch über die Vereinbarung und Schaffung korrespondierender Schutzmaßnahmen auf Seiten des Landtags zu befinden.

Position der Landesregierung:

Die Landesregierung ist den Landtagsabgeordneten gegenüber auskunftspflichtig. Dies gebietet die Landesverfassung. Damit kann auch die Übermittlung personenbezogener Daten im

Raum stehen. In diesen Fällen steht die Landesregierung vor der Aufgabe, das parlamentarische Fragerecht mit dem aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Grundrecht auf informationelle Selbstbestimmung in Einklang zu bringen. Denn der Informationsanspruch der einzelnen Abgeordneten besteht nicht grenzenlos. Das Fragerecht der Abgeordneten und die Antwortpflicht der Regierung können dadurch begrenzt sein, dass diese gemäß Artikel 1 Absatz 3 des Grundgesetzes Grundrechte zu beachten haben. Hierzu zählt nach der Rechtsprechung des Bundesverfassungsgerichts im sogenannten Volkszählungsurteil[63]das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Grundrecht auf informationelle Selbstbestimmung. Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen und damit Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der auf ihn bezogenen, individualisierten oder individualisierbaren Daten.

Entsprechend den anerkannten Regeln bei der Kollision verfassungsrechtlich begründeter Rechtspositionen ist jeweils eine Abwägung anhand sämtlicher Umstände des Einzelfalls unter Berücksichtigung des Grundsatzes der praktischen Konkordanz vorzunehmen.

Manche Landesdatenschutzgesetze regeln die Datenübermittlung an den Landtag gesondert, z. B. § 23 des Landesdatenschutzgesetz Rheinland-Pfalz[64] und § 27 des Gesetzes zum Schutz personenbezogener Daten im Land Brandenburg[65], die sich mit der „Verarbeitung zu Zwecken der parlamentarischen Kontrolle“ befassen.

---

[63] BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209/83, abrufbar unter https://www.bverfg.de/e/rs19831215_1bvr020983.html.

[64] § 23 LDSG Rheinland-Pfalz:
Verarbeitung zu Zwecken der parlamentarischen Kontrolle
Die Landesregierung darf personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Abs. 1 der Datenschutz-Grundverordnung zur Beantwortung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten an den Landtag in dem dafür erforderlichen Umfang verarbeiten. Eine Übermittlung der personenbezogenen Daten zu einem der in Satz 1 genannten Zwecke ist nicht zulässig, wenn dies wegen des streng persönlichen Charakters der Daten für die betroffene Person unzumutbar ist oder wenn der Eingriff in ihr informationelles Selbstbestimmungsrecht unverhältnismäßig ist. Satz 2 gilt nicht, wenn durch die Datenschutzordnung im Sinne des § 2 Abs. 3 Satz 2 oder sonstige geeignete Maßnahmen sichergestellt ist, dass schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden. Besondere gesetzliche Übermittlungsverbote bleiben unberührt.

[65] § 27 Brandenburgisches Datenschutzgesetz:
Verarbeitung personenbezogener Daten zu Zwecken der parlamentarischen Kontrolle
(1) Die Landesregierung darf personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 zur Beantwortung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten an den Landtag in dem dafür erforderlichen Umfang verarbeiten. Eine Übermittlung der Daten zu einem der in Satz 1 genannten Zwecke ist nicht zulässig, wenn dies wegen des streng persönlichen Charakters der Daten für die betroffene Person unzumutbar ist oder wenn der Eingriff in ihr informationelles Selbstbestimmungsrecht unverhältnismäßig ist. Dies gilt nicht, wenn im Hinblick auf § 2 Absatz 2 Satz 2 oder durch sonstige geeignete Maßnahmen sichergestellt ist, dass schutzwürdige Interessen der betroffenen Personen nicht beeinträchtigt werden. Besondere gesetzliche Übermittlungsverbote bleiben unberührt.
(2) Von der Landesregierung übermittelte personenbezogene Daten dürfen nicht in Landtagsdrucksachen aufgenommen oder in sonstiger Weise öffentlich zugänglich gemacht werden. Dies gilt nicht, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der betroffenen Personen beeinträchtigt werden.

Aus denselben Gründen, die der LfDI aufführt, wird eine gesetzliche Regelung befürwortet. Diese sollte sich nicht darauf beschränken, vor einer Datenübermittlung nur die Abwägung zwischen den beiden Verfassungsgütern vorzuschreiben. Der Gesetzgeber sollte vielmehr auf der Grundlage des Verfassungsrechts die Richtschnur für die Abwägung vorgeben, z. B. indem, wie in den erwähnten Gesetzesregelungen, ein absoluter Schutz für Daten und Informationen streng persönlichen Charakters vorgesehen wird, im Übrigen aber eine Verhältnismäßigkeitsprüfung stattzufinden hat. Damit würde auch für mehr Transparenz auf Seiten der betroffenen Personen gesorgt werden.

(2) Datenübermittlung an nichtöffentliche Stellen

Bezüglich der Datenübermittlung an nichtöffentliche Stellen wird eingewandt, dass die Übermittlung zugelassen werde, ohne dass dies der ursprüngliche Zweck der Erhebung war und ohne Einwilligung der betroffenen Person. Ein Katalog wie in § 5 LDSG sei nicht vorgesehen, sondern allein eine Interessenabwägung. Hier sollte geprüft werden, ob nicht ebenfalls die Angabe des damit verfolgten Zwecks oder Ziels erforderlich ist.

In Absatz 1 wird außerdem ein Redaktionsfehler in Bezug auf den zweiten Halbsatz der Nummer 2 beanstandet. Da dieser Zusatz bereits in der Einleitung des § 6 Absatz 1 LDSG erwähnt wird, könne er bei den nichtöffentlichen Stellen entfallen.

- Bewertung des LfDI (S. 22f.):

Der LfDI hält eine Konkretisierung des Zwecks für angezeigt. Diese müsse sich an den Zwekken des Artikels 23 Absatz 1 DSGVO ausrichten, von denen allein der Schutz der Rechte und Freiheiten anderer Personen (Buchst. i) und die Durchsetzung zivilrechtlicher Ansprüche (Buchst. j) einschlägig seien.

Den redaktionellen Korrekturvorschlag hält er für berechtigt.

Position der Landesregierung:

Es ist angezeigt, die Voraussetzungen näher zu bestimmen, unter denen eine nichtöffentliche Stelle nach dem LDSG Empfänger der Übermittlung personenbezogener Daten durch eine öffentliche Stelle sein kann. Es werden deshalb zwei Klarstellungen empfohlen:

In Nummer 1 sollte klargestellt werden, dass die Übermittlung auch an eine nichtöffentliche Stelle zulässig ist, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle

liegenden Aufgaben erforderlich ist und die Voraussetzungen für eine Zweckänderung nach § 5 LDSG vorliegen.

Nummer 2 gilt nur für die Übermittlung an nichtöffentliche Stellen und setzt deren berechtigtes Interesse voraus, welches glaubhaft dargelegt werden muss. Damit entspricht die Regelung in Bezug auf die Tatbestandsvoraussetzungen der früheren Fassung in § 18 LDSG a. F. sowie der Regelung in § 25 Absatz 3 Nummer 2 BDSG. Sie kann auf der Grundlage von Artikel 23 Absatz 1 Buchst. i DSGVO mit dem Schutz der Rechte und Freiheiten anderer Personen begründet werden. Zu beachten ist, dass auch in diesem Fall die Erforderlichkeit und Verhältnismäßigkeit der Übermittlung zu prüfen ist. Die Übermittlung darf nicht erfolgen, wenn dem Begehren des Antragstellers auch durch die Übermittlung anonymisierter oder pseudonymisierter Daten Rechnung getragen werden kann. Zum Schutz des informationellen Selbstbestimmungsrechts ist eine Abwägung mit dem schutzwürdigen Interesse der betroffenen Person vorgeschrieben. Die Glaubhaftmachung obliegt dem Dritten. Die Interessen der betroffenen Person hingegen muss die öffentliche Stelle aufgrund des Amtsermittlungsgrundsatzes des § 24 LVwVfG selbstständig ermitteln[66]

Zur weiteren Konkretisierung wird empfohlen, der Vorschrift als weitere Alternative die Datenübermittlung an nichtöffentliche Stellen zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche hinzuzufügen, wie in § 25 Absatz 2 Nummer 3 BDSG geregelt.

Der Einschätzung zum zweiten Halbsatz des Absatz 1 Nummer 2 wird zugestimmt. Der Redaktionsfehler sollte beseitigt werden.

bb) Zu § 6 Absatz 2 LDSG

Datenübermittlung auf Ersuchen

Aus dem Kultusministerium wird für die Praxis um Konkretisierung gebeten, welche Pflichten der übermittelnden Stelle im Falle eines Ersuchens obliegen. Dies betrifft die Frage, wie die Prüfung, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden öffentlichen Stelle liegt, erfolgen muss. Weiterhin war in der Praxis nicht klar, wann ggf. gemäß § 6 Absatz 2 Satz 4 LDSG Anlass besteht, die Rechtmäßigkeit eines Ersuchens zu prüfen.

- Bewertung des LfDI (S. 23-25):

Nach Auffassung des LfDI sollte die Vorschrift gestrichen werden, da sie weder normenklar noch sachgerecht sei. Die Anforderung an die ersuchende Stelle, die Übermittlungsbefugnis

[66] Vgl. zur gesamten Thematik Sandfuchs in Gola/Heckmann, § 25 Rn. 22-25.

der übermittelnden Stelle zu prüfen, führe zur Überforderung der ersuchenden Stelle und werde in der Praxis nicht erfüllt. Darüber hinaus stehe die Gesetzgebungskompetenz für Stellen außerhalb des Landes infrage.

Position der Landesregierung:

Die Vorschrift hat keine Neuerung zu der Vorgängervorschrift des § 16 Absatz 2 LDSG a. F. gebracht. Dem LfDI ist aber zuzustimmen, dass die Norm in der Anwendung zu Unklarheiten führt. Das BDSG hat von einer entsprechenden Regelung abgesehen. Es wird daher vorgeschlagen, § 6 Absatz 2 LDSG zu streichen. Die Verantwortung für die Übermittlung würde dann die übermittelnde Stelle tragen, auch in Fällen von Ersuchen einer öffentlichen Stelle. Dies bedarf keiner gesonderten Regelung und entspricht dem Doppeltürmodell. Damit die übermittelnde Stelle ihre Verantwortung wahrnehmen kann, ist folgendes klarzustellen:

Die ersuchende Stelle ist verpflichtet, darzulegen, wofür und aufgrund welcher Rechtsgrundlage sie die Daten benötigt. Des Weiteren kann nur die ersuchende Stelle die Verantwortung dafür tragen, dass die Tatbestandsvoraussetzungen für das Ersuchen vorliegen. Dies sollte die übermittelnde Stelle nur in Zweifelsfällen gemäß Satz 4 überprüfen müssen. Eine entsprechende Regelung kann auch § 7 LVwVfG entnommen werden. Damit würden die Voraussetzungen denen entsprechen, die für automatisierte Abrufe in § 6 Absatz 3 LDSG geregelt sind. Im Ergebnis könnte die Übermittlung auf Ersuchen in § 6 Absatz 3 LDSG integriert werden.

cc) Zu § 6 Absatz 3 LDSG

Automatisierte Abrufverfahren

Unter Bezug auf das Vorhaben der Registermodernisierung, welches zu vermehrten Abrufen von Daten durch Behörden führen wird, wurde in der Anhörung seitens des Innenministeriums darauf hingewiesen, dass die Vorschriften des LDSG zum Abruf im Wege eines automatisierten Verfahrens mit den Vorschriften zur Registermodernisierung kohärent sein sollten.

Da das LDSG keine Vorschriften enthält, unter welchen Voraussetzungen ein Abrufverfahren eingerichtet werden darf oder regelmäßige Datenübermittlungen zulässig sind, stellt sich des Weiteren die Frage, ob entsprechende Vorschriften erforderlich sind.

Position der Landesregierung:

Zum Nachweisabruf entsprechend den Vorschriften des Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung wei-

terer Gesetze (Registermodernisierungsgesetz – RegMoG) bedarf es entsprechend dem Doppeltürmodell des Bundesverfassungsgerichts zum einen der datenschutzrechtlichen Ermächtigung, die Daten abzurufen, zum anderen der datenschutzrechtlichen Ermächtigung, die angeforderten Daten zu übermitteln.

Für den automatisierten synchronen Nachweisdatenabruf in antragsbasierten Verwaltungsverfahren für den nationalen und grenzüberschreitenden Nachweisdatenaustausch ist eine Regelung im E-Government-Gesetz (des Bundes) geplant. Die Vorschriften beziehen sich auf Nachweisdatenabrufe aus allen Datenbeständen und nicht nur auf Register im Sinne des RegMoG. Die Änderungen des E-Government-Gesetzes sind im Rahmen des Gesetzgebungsverfahrens für das OZG-Änderungsgesetz erfolgt. Auch im Land müssen entsprechende Regelungen geschaffen werden. Hierfür bieten sich entsprechende Regelungen im E-Government-Gesetz Baden-Württemberg an.

Für asynchrone Abrufe (aus Registern) bleiben die Regelungen des LDSG in § 6 Absatz 1 Nummer 1 LDSG maßgeblich. Bei der asynchronen Datenübertragung werden im Gegensatz zur synchronen Datenübertragung die Zeichen nachrichtentechnisch zu beliebigen Zeiten übertragen. Die Übertragung ist also, im Gegensatz zur synchronen Datenübertragung, nicht an einem Taktsignal ausgerichtet[67].

Des Weiteren gilt das LDSG für alle automatisierten Abrufverfahren aus Registern, die nicht dem RegMoG unterfallen.[68].
Diesbezüglich wird eine entsprechende Regelung im LDSG befürwortet, um eine gesetzliche Legitimation bereitzustellen.

Die Zulässigkeit sollte voraussetzen, dass die Einrichtung automatisierter Verfahren sowie sonstiger regelmäßiger Datenübermittlungen unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können. Sofern automatisierte Verfahren ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bedeuten können, sollten sie nur zulässig sein, wenn sie durch Gesetz oder auf Grund eines Gesetzes eingerichtet werden. Letzteres erlaubt ggf. die Einrichtung durch Verordnung.

[67] Vgl. in Wikipedia unter https://de.wikipedia.org/wiki/Asynchrone_Daten%C3%BCbertragung, letzter Abruf am 1. Juli 2024.
[68] Vgl. Anlage zu § 1 des Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung (Identitätsnummerngesetz – IDNrG).

7. Einschränkungen der Betroffenenrechte (§§ 8 bis 11 LDSG)

a) Zum Norminhalt

Die Rechte der betroffenen Personen wie die Informationspflicht und das Auskunftsrecht sind ein Kernstück der DSGVO. Sie dienen der Transparenz der Datenverarbeitung und dürfen vom nationalen Gesetzgeber nur aus den in Artikel 23 DSGVO genannten übergeordneten Gründen beschränkt werden.

Die Beschränkungen in §§ 8 ff. LDSG dienen im Wesentlichen dem Schutz öffentlicher Interessen. Der letzte Halbsatz des § 8 Absatz 1 LDSG verlangt aber entsprechend dem Grundsatz der Verhältnismäßigkeit eine Einzelfallabwägung mit den Interessen der betroffenen Person.

b) Rückmeldung und Bewertung

Beschränkungen gegenüber dem Landtag

Der Landtag hält die Einschränkungen der Betroffenenrechte derzeit für ausreichend. In Bezug auf das Urteil des Europäischen Gerichtshofs vom 9. Juli 2020[69] stellt er jedoch die Frage, ob die Einschränkungen ausreichen, wenn auch die parlamentarischen Verarbeitungsvorgänge im Landtag in den Anwendungsbereich der DSGVO fallen sollten. Zu denken sei hier insbesondere an die Arbeit der Untersuchungsausschüsse, die einen ausreichenden Quellenschutz und damit unter Umständen eine Einschränkung des Auskunftsrechts erforderten. Denn mit einem Auskunftsverlangen könnten sich Personen, die von einem Untersuchungsausschuss geladen worden sind, zur Vorbereitung danach erkundigen, was der Ausschuss bereits über sie herausgefunden hat, einschließlich der Quellen, aus denen die Informationen kommen. Auch im Hinblick auf § 10 LDSG (Beschränkung des Rechts auf Löschung) sei Vorsorge zu treffen, dass die Verarbeitung von Protokollen, in denen eine Person namentlich erwähnt werde, nicht eingeschränkt werden müsse.

- Bewertung des LfDI (S. 7):

Der LfDI plädiert dafür, für das Problem der Betroffenenrechte im Untersuchungsausschuss eine Lösung im Untersuchungsausschussgesetz zu suchen, falls dieses einschließlich seiner Verweisungen auf die Strafprozessordnung nicht in erforderlichem Maß Einschränkungen der Betroffenenrechte vorsehe.

[69] Siehe oben unter Fußnote 22.

71

Position der Landesregierung:

Das Anliegen des Landtags kann im LDSG nur Berücksichtigung finden, wenn dieses zukünftig auch auf die parlamentarische Tätigkeit des Landtags Anwendung finden soll. In diesem Fall wären die Regelungen des § 9 Absatz 1 in Verbindung mit § 8 Absatz 1 Nummer 1 und 4 LDSG geeignet, in gewissem Umfang Quellenschutz zu gewährleisten. Weitere Beschränkungen müssten geprüft werden.

Unterstützt wird auch die vom LfDI vorgeschlagene Regelung im Untersuchungsausschussgesetz. Umfassender könnte das Anliegen des Landtags in der Datenschutzordnung des Landtags geregelt werden. Diesbezüglich bedarf es der Überprüfung durch den Landtag, inwieweit die in § 6 der Datenschutzordnung des Landtags vom 12. Juli 2012 getroffene Regelung ausreicht.

8. Beschränkung der Informationspflicht (§ 8 LDSG)

a) Zum Norminhalt

Die Beschränkung der Informationspflicht betrifft sowohl die Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person nach Artikel 13 DSGVO wie auch die Informationspflicht nach Artikel 14 DSGVO, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.

b) Rückmeldungen und Bewertung

aa) Bestimmtheitsgrundsatz

Der LfDI hält nach seiner Stellungnahme vom November 2020 § 8 LDSG für nicht vereinbar mit den Vorgaben der DSGVO, da die Anforderungen des Artikels 23 Absatz 2 DSGVO für die Beschränkung der Informationspflicht nicht eingehalten seien. Damit sei der Bestimmtheitsgrundsatz verletzt.

Des Weiteren wurde angeregt, die Formulierung in § 8 LDSG zu überdenken. Das dort vorgesehene grundsätzliche Überwiegen der in den Absatz 1 Nummern 1 bis 5 aufgezählten Fallgruppen könnte dem in Artikel 23 Absatz 1 DSGVO angelegten Grundsatz der Verhältnismäßigkeit widersprechen und sollte durch eine Einzelfallabwägung ersetzt werden.

- Bewertung des LfDI (S. 25f.):

Der LfDI teilt die vorgebrachte Kritik und hält an seiner Bewertung in Bezug auf den Konkretisierungsbedarf fest.

Position der Landesregierung:

Die Vorschrift des § 8 LDSG sieht bereits eine Beschränkung der Informationspflicht nur im erforderlichen Umfang vor, wie sich aus der Einfügung von „soweit und solange“ ergibt. Die Notwendigkeit einer Einzelfallprüfung ergibt sich daraus, dass jeweils festgestellt werden muss, dass die aufgezählten Interessen an der Beschränkung der Informationspflicht hinter dem Interesse der betroffenen Person zurücktreten müssen.

Aus Gründen der Klarstellung wird vorgeschlagen, eine Regelung entsprechend § 32 Absatz 2 und 3 BDSG einzufügen,

- wonach die Erteilung der Information nachzuholen ist, wenn die Gründe für ein Absehen von der Information nicht mehr bestehen und
- die öffentliche Stelle geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der notwendigen Informationen für die Öffentlichkeit ergreift, sofern eine Information der betroffenen Person nach Absatz 1 unterbleiben muss.

bb) Information über Protokollierungs- und Backupmaßnahmen

Aus dem Wissenschaftsbereich wurde die Frage aufgeworfen, ob ein Verantwortlicher, der nicht über Daten Auskunft geben müsse, die er ausschließlich zum Zweck der Datensicherung oder Datenschutzkontrolle gespeichert hat, über diese Erhebungen (Protokollierungs- und Backupmaßnahmen) informieren müsste. Es sei zielführend, wenn – bezogen auf Mitarbeiterdaten – auch die Informationspflicht in § 8 LDSG eingeschränkt würde.

- Bewertung des LfDI (S. 27f.):

Der LfDI hält eine weitere Einschränkung nicht für gerechtfertigt. Auch hier argumentiert er mit der erforderlichen Transparenz für die betroffene Person. Auch die Bereiche der Datensicherung und Datenschutzkontrolle müssten für die betroffenen Personen offengelegt werden. Für die Datenschutzinformation reiche im Übrigen eine allgemeine Information. Es müssten nicht wie für die Auskunft über die gespeicherten Inhalte informiert werden.

Position der Landesregierung:

Aus Sicht der Landesregierung besteht kein Bedürfnis für eine entsprechende Einschränkung, da der Aufwand für die Informationserteilung im Gegensatz zur Auskunft gering ist. Im Übrigen ist auch der Auskunftsanspruch für die genannten Daten im Gesetz nicht generell ausgeschlossen.

cc) Ausweitung der Einschränkungen des Artikels 14 DSGVO

Seitens des Umweltministeriums wurden Probleme bei der Formulierung von Datenschutzerklärungen im Zusammenhang mit der Datenübermittlung bei der Beantwortung von Landtagsanfragen geschildert. Es seien Anpassungen des § 8 LDSG wünschenswert, um die Informationspflichten des Artikels 13 DSGVO weiter einzuschränken. Denn in den Anwendungsfällen des Artikels 14 DSGVO, also wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben würden, könne die Information der betroffenen Person gemäß Absatz 5 in wesentlich mehr Fallgestaltungen unterbleiben als dies bei der Direkterhebung nach Artikel 13 Absatz 4 DSGVO der Fall sei, unter anderem wenn eine rechtliche Verpflichtung zur Weitergabe bestünde[70]. Anders als sonst sei in diesem Anwendungsbereich nicht überzeugend, dass in den Fällen des Artikels 13 DSGVO ein höheres Schutzniveau als in den Fällen des Artikels 14 DSGVO gefordert werde.

- Bewertung des LfDI (S. 25f.):

Der LfDI rät von einer Übernahme der Ausnahmevorschrift des Artikels 14 Absatz 5 Buchst. c DSGVO ab. Diese Vorschrift regele den Entfall der Informationspflicht in Fällen, in denen die betroffene Person die Hintergründe der Erhebung oder Offenlegung der jeweiligen Rechtsvorschrift entnehmen könne, wenn die Norm also eine entsprechende Information – wie eine sonst durch einen Verantwortlichen zu erteilende – biete und die jeweils betroffene Person dadurch Reichweite und Risiko der Datenerhebung und Weiterverarbeitung ausreichend abschätzen könne. Eine solche Information sei dem LDSG in Bezug auf die Beantwortung von Landtagsanfragen nicht zu entnehmen.

Position der Landesregierung:

Angesichts der hohen Anforderungen an die Beschränkung der Informationspflicht gemäß Artikel 23 Absatz 1 DSGVO erscheint eine Beschränkung in den genannten Fällen, denen eher praktische Erwägungen zugrunde liegen, nicht gerechtfertigt. Die Transparenz sollte für die

[70] Vgl. Artikel 14 Absatz 5 Buchst. c DSGVO.

betroffene Person gewahrt bleiben. Dies gebietet auch die Tatsache, dass die betroffene Person in der Regel keine Kenntnis von Landtagsanfragen erlangt.

9. Beschränkung des Auskunftsrechts (§ 9 LDSG)

a) Zum Norminhalt

Das Auskunftsrecht nach Artikel 15 DSGVO als zentrales Betroffenenrecht ist in der Verwaltungspraxis von besonderer praktischer Relevanz, da Auskunftsanfragen relativ häufig gestellt werden.

b) Rückmeldungen und Bewertung

Zu § 9 Absatz 2 LDSG

Praxisprobleme

Der LfDI hält in seiner Stellungnahme vom November 2020 eine praxisgerechtere Fassung der Vorschrift in Absatz 2 für erforderlich, da sie häufig Auslegungsprobleme bereite. Dies betreffe die Begriffe „große Mengen von Informationen“ sowie den Begriff „unzumutbarer Aufwand“. Darüber hinaus sei eine Klarstellung erforderlich, ob bei der Betrachtung die jeweilige Einzelbehörde entscheidend ist oder ob es auch auf Kommunikationsvorgänge mit anderen Behörden ankommt.

Aus einem Regierungspräsidium kam die Rückmeldung, dass die genannten Begriffe zu viel Interpretationsspielraum ließen und der Verwaltung nicht wirklich helfen würden. Insoweit würde eine klarere Definition gewünscht.

- Bewertung des LfDI (S. 28):

Der LfDI plädiert in seiner Bewertung vom 13. Februar 2024 nunmehr für eine vollständige Streichung des § 9 Absatz 2 LDSG, weil die DSGVO keine Öffnungsklausel hierfür enthalte. Es könne auf Erwägungsgrund 63 Satz 7 der DSGVO zurückgegriffen werden.

Position der Landesregierung:

Mit der Vorschrift wird zum Ausdruck gebracht, dass die Mitwirkung der betroffenen Person im Einzelfall, nämlich bei einer großen Menge vorhandener Informationen, erforderlich ist. Wird diese verweigert, kann die Auskunft verweigert werden, um einen unzumutbaren Auf-

wand zu vermeiden. Damit wird dem Erwägungsgrund 63 gefolgt, nach dem der Verantwortliche verlangen können soll, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht.

Grundsätzlich wird eine Beschränkung des Auskunftsrechts gegenüber Behörden gemäß Artikel 23 Absatz 1 DSGVO für gerechtfertigt gehalten, wenn dies erforderlich ist, um die Funktionsfähigkeit der Verwaltung zu gewährleisten. Vor allem, wenn die Daten nicht automatisiert oder nicht in einem Dateisystem gespeichert sind, kann ein unzumutbarer Aufwand für die Auskunftserteilung entstehen und die Ablehnung rechtfertigen. Unzumutbarkeit ist anzunehmen, wenn der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

Aus Sicht der Landesregierung besteht kein zwingender Grund, die Regelung des § 9 Absatz 2 LDSG zu ändern. Die Verwendung unbestimmter Rechtsbegriffe macht eine Vorschrift nicht impraktikabel. Sie ist im Streitfall in vollem Umfang einer gerichtlichen Überprüfung unterworfen. Für die Regelung besteht zudem ein praktisches Bedürfnis. Denn in großen Behörden kann ohne Präzisierung des Auskunftsersuchens eine Auskunft unter Umständen nur mit unzumutbarem Aufwand erteilt werden. Die betroffene Person wird nach der Vorschrift unterstützt, indem ihm die öffentliche Stelle die Verarbeitungsvorgänge auflistet.

Es wird für zweifelhaft gesehen, sich rechtlich auf einen Erwägungsgrund der DSGVO zu stützen, wie vom LfDI vorgeschlagen. Daher wird der gesetzlichen Regelung der Vorzug gegeben. Eine Mitwirkungspflicht der betroffenen Person lässt sich im Übrigen auch aus § 25 LVwVfG herleiten, sollte aber gesetzlich präzisiert werden.

10. Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (§ 13 LDSG)

a) Zum Norminhalt

Die besondere Konstellation in Bezug auf die Verarbeitung personenbezogener Daten im Forschungsbereich rekurriert auf die Grundrechtsbezogenheit der Forschungstätigkeit auf der einen Seite (Artikel 13 GRCh) und das Grundrecht auf Datenschutz (Artikel 8 GRCh) auf der anderen Seite. In dem Widerstreit dieser Grundrechte ist es die Aufgabe des Gesetzgebers, eine Regelung zu treffen, die beiden unter Beachtung des Verhältnismäßigkeitsgrundsatzes Rechnung trägt.

Die DSGVO privilegiert die Forschung in mehreren Vorschriften, unterwirft sie aber gleichzeitig der Anforderung von angemessenen Garantien und Bedingungen. Die Privilegierungen ergeben sich aus den folgenden Vorschriften:

- Gemäß Artikel 5 Absatz 1 Buchst. b DSGVO gilt die Weiterverarbeitung personenbezogener Daten für wissenschaftliche Forschungszwecke gemäß Artikel 89 Absatz 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken.

- Eine längere Speicherdauer ist gemäß Artikel 5 Absatz 1 Buchst. e DSGVO für Forschungszwecke möglich (Ausnahme vom Grundsatz der Speicherbegrenzung).

- Für die Forschung kann die Verarbeitung besonderer Kategorien personenbezogener Daten unter den Voraussetzungen des Artikels 9 Absatz 2 Buchst. j DSGVO durch das Recht des Mitgliedstaats zugelassen werden, sofern sie erforderlich ist. Voraussetzung ist aber, dass die Garantien und Ausnahmen in Bezug auf die Verarbeitung zu Forschungszwecken gemäß Artikel 89 Absatz 1 DSGVO beachtet werden.

- Zugunsten der Forschung sind entsprechend Artikel 89 Absatz 2 DSGVO Ausnahmen von den Betroffenenrechten im Recht der Mitgliedstaaten möglich. Werden die personenbezogenen Daten für Forschungszwecke nicht bei der betroffenen Person erhoben, kann die Information der betroffenen Person bei Unmöglichkeit oder unverhältnismäßigem Aufwand gemäß Artikel 14 Absatz 5 Buchst. b DSGVO entfallen.

Wegen der privilegierten Verarbeitung personenbezogener Daten für Forschungszwecke werden an die Forschung besondere datenschutzrechtliche Anforderungen bezüglich der Verarbeitung personenbezogener Daten gestellt. In Artikel 89 Absatz 1 DSGVO wird die Forschung diesbezüglich Mindestanforderungen für Garantien für die Rechte und Freiheiten der betroffenen Person unterworfen. Zu diesen gehört insbesondere das Gebot der Datenminimierung. Von der datenverarbeitenden Stelle wird gefordert, dass sie nur die personenbezogenen Daten verarbeitet, deren Verarbeitung für den jeweils bestimmten Verarbeitungszweck erforderlich ist. Des Weiteren ist zunächst die Verwendung von Daten zu prüfen, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist (anonymisierte Daten). Falls für die Forschung ein Rückgriff auf anonymisierte Daten ausscheidet, weil die personenbezogenen Daten benötigt werden, ist in einem zweiten Schritt zu prüfen, ob die Verwendung pseudonymisierter Daten nach dem Forschungszweck möglich ist. Technische und organisatorische Maßnahmen müssen gemäß Artikel 25, 32 DSGVO getroffen werden.

Den besonderen Anforderungen entsprechend wurde im LDSG für die Forschung öffentlicher Stellen mit personenbezogenen Daten in § 13 eine besondere Rechtsgrundlage geschaffen. Diese erlaubt die Verarbeitung personenbezogener Daten für Forschungszwecke ohne Einwilligung der betroffenen Personen, setzt aber einen wirksamen Datenschutz entsprechend den Grundsätzen der DSGVO sowie geeigneter Maßnahmen gemäß § 3 LDSG voraus. Die Ano-

nymisierung wird nach § 13 Absatz 2 LDSG sobald wie möglich verlangt. Soweit eine vollständige Anonymisierung nicht möglich ist, ist, außer der Forschungszweck verlangt etwas anderes, Pseudonymisierung die gebotene Maßnahme. Weitere geeignete Maßnahmen sind zu prüfen und ggf. spezialgesetzlich zu regeln. Die Betroffenenrechte einschließlich eines Widerspruchsrechts ergeben sich aus der DSGVO.

Die Vorschrift schließt auf der Grundlage von Artikel 9 Absatz 2 Buchst. j DSGVO die Verarbeitung besonderer Kategorien personenbezogener Daten ein.

b) Rückmeldungen und Bewertung

Die Rückmeldungen zu § 13 LDSG bezogen sich ausschließlich auf die Anwendung zu Forschungszwecken (nicht zu Statistikzwecken).

aa) Grundsätzliche Fragestellungen zur Forschung mit personenbezogenen Daten

Aus der Landesregierung heraus kam die Rückmeldung, dass die Regelungen für die Verarbeitung personenbezogener Daten im Forschungsbereich die Forschung nicht ausreichend unterstützen. Es wurden Verbesserungsvorschläge unterbreitet.

Datenschutzrechtliche Vorgaben sind unbestritten notwendig, um das Grundrecht auf Datenschutz der betroffenen Personen zu wahren, in besonderem Maße, wenn es sich um Gesundheitsdaten handelt, die nach der DSGVO als sensible Daten gemäß Artikel 9 DSGVO besonders geschützt sind. Andererseits können datenschutzrechtliche Vorgaben die Forschung einschränken oder sogar behindern.

Die Landesregierung hat im Dialog mit den Akteuren des Gesundheitswesens festgestellt: Ohne die digitale Nutzung von Gesundheitsdaten ist medizinischer Fortschritt in Zukunft nicht möglich. Grundlegend ist diesbezüglich die vom Forum Gesundheitsstandort Baden-Württemberg erstellte Roadmap Gesundheitsdatennutzung Baden-Württemberg vom April 2022.

Auch für die von der Landesregierung vorangetriebene Entwicklung nachhaltiger Mobilitätskonzepte wird die Nutzung personenbezogener Daten, insbesondere aus der Verkehrsüberwachung, benötigt.

Die Nutzung von Daten mit Personenbezug ist für die gemeinwohlorientierte Forschung öffentlicher Stellen daher von grundlegender Bedeutung. Charakteristisch für eine Gemeinwohlorientierung der Forschung ist, dass nicht in Bezug auf die Personen, deren personenbezogene Daten verarbeitet werden, geforscht wird, sondern die personenbezogenen Daten als

Mittel zur Beförderung des Allgemeinwohls dienen. Das setzt insbesondere die Unabhängigkeit der Forschung von Einzelinteressen voraus. Die Forschungsregelung im LDSG zu ertüchtigen, kann einen wesentlichen Beitrag zum Gemeinwohl liefern.

Die Landesregierung spricht sich im Folgenden dafür aus, zugunsten der Forschung in das LDSG klarstellende Regelungen aufzunehmen, die einen vernünftigen Rahmen für die Forschung erlauben und gleichzeitig die Rechte und Freiheiten der betroffenen Personen garantieren.

Zu berücksichtigen ist diesbezüglich auch die Überlagerung durch europäisches Datenschutzrecht. Wesentliche Regelungen hierzu sind auch in dem Daten-Governance-Rechtsakt und der Datenverordnung der Europäischen Union erfolgt sowie für den spezifischen Bereich der Gesundheitsdaten in den Regelungen zum Europäischen Gesundheitsdatenraum zu erwarten.

Im Folgenden werden die grundlegenden Probleme näher beleuchtet und die Lösungsvorschläge der Landesregierung dargelegt.

(1) Weiterverarbeitung bestehender Datensätze in der Forschung (Sekundärforschung)

Die Forschung ist häufig darauf angewiesen, Datensätze für die Forschung zu nutzen, die für einen anderen Zweck erhoben wurden. Insbesondere für die Entwicklung von KI-Anwendungen ist die Verwendung großer Datensätze essentiell. Datenschutzrechtlich stellt sich die Nutzung entsprechender Daten vor allem im Hinblick auf die Grundsätze der Datenverarbeitung wie Zweckbindung und Datenminimierung als kritisch dar.

Beispielhaft hierfür wird vom Verkehrsministerium ein Sachverhalt aus einem vom Land geförderten Forschungsprojekt geschildert:
Im Forschungsförderprogramm Smart Mobility des Wissenschafts- und des Verkehrsministeriums sollten gemäß der Ausschreibung Daten des Testfelds autonomes Fahren Baden-Württemberg in Karlsruhe verwendet werden. Das Projekt der Universität Ulm beschäftige sich mit der Gesten- und Intentionserkennung von Personen im Straßenverkehr unter Nutzung maschineller Lernverfahren. Hierzu sei geplant gewesen, unverarbeitete Video-Rohdaten aus dem Testfeld zu nutzen, die vom FZI Forschungszentrum Informatik in Karlsruhe gespeichert werden. Die Nutzung dieser Daten sei dem Projekt nach Abstimmung mit dem LfDI unter Verweis auf das Prinzip der Datensparsamkeit verwehrt worden.

Dieselbe Problematik besteht bei der retrospektiven Nutzung von Patientendaten für die Gesundheitsforschung.

Im Ergebnis unterliegt die Forschung mit vorhandenen Datensätzen damit derzeit rechtlicher Unsicherheit. Das Innovationspotential kann unter Umständen nicht vollständig ausgeschöpft werden.

- Bewertung des LfDI (S. 36f.):

Der LfDI weist im Hinblick auf die vom Verkehrsministerium geschilderte Problematik darauf hin, dass der Grundsatz der Erforderlichkeit nach der DSGVO nicht disponibel sei. Für das Training einer KI-Anwendung könnten aber auch große Datenmengen im Sinne der DSGVO erforderlich sein. In Zukunft sei die KI-Verordnung zu beachten, die auch die Möglichkeit zur Einrichtung sogenannter Reallabore biete.

Lösungsvorschlag der Landesregierung:

Das Thema der Nutzung vorhandener Datenmengen berührt die Frage, wie mit den Grundsätzen des Artikels 5 Absatz 1 DSGVO, die Zweckbindung, Datenminimierung und Speicherbegrenzung vorschreiben, umzugehen ist. Bei Anwendung dieser Prinzipien kann man die sehr großen Datenmengen, die für maschinelle Lernverfahren erforderlich sind, nur beschränkt für die Forschung nutzen. Zugleich besteht ein Bedürfnis der KI-Forschung nach realitätsgetreuen (Bild-)Daten, so dass anonymisierte Daten nicht generell als Ersatz geeignet sind. Hinzu kommt, dass Anonymisierung vor allem bei großen Datenmengen mit rechtlichen Risiken behaftet ist, da das Risiko der Re-Identifikation steigt, je mehr Daten zu einer Person vorhanden sind.

Wie ausgeführt genießt die Forschung erhebliche Privilegierungen, die im Bereich der Weiterverwendung von Daten nützlich sein könnten. Diese beziehen sich auf die Durchbrechung der Zweckbindung sowie die Ausweitung der Speicherbegrenzung[71], dagegen nicht auf den Grundsatz der Datenminimierung, der die Verarbeitung auf das für die Zwecke notwendige Maß beschränkt[72]. § 13 Absatz 2 LDSG schreibt dementsprechend die Anonymisierung vor, sobald dies nach dem Forschungszweck möglich ist. Die Verwendung anonymisierter Daten wird als anzustrebender Standard der Datenverwendung anzusehen sein. Artikel 25 Absatz 2 DSGVO geht ebenfalls davon aus, dass durch geeignete technische und organisatorische Maßnahmen der Grundsatz der Datenminimierung wirksam umgesetzt werden kann. Für die Forschung mit Gesundheitsdaten oder sonstigen besonderen Kategorien personenbezogener Daten gelten dieselben Grenzen entsprechend Artikel 9 Absatz 2 Buchst. j DSGVO in Verbindung mit Artikel 89 Absatz 1 DSGVO.

[71] Vgl. Artikel 5 Absatz 1 Buchst. b und e DSGVO.
[72] Vgl. Artikel 89 Absatz 1 in Verbindung mit Artikel 5 Absatz 1 Buchst. c DSGVO.

Nicht unberücksichtigt bleiben sollte in diesem Zusammenhang der Gedanke, dass die Forschung zu Gemeinwohlzwecken ein wichtiges Ziel im allgemeinen öffentlichen Interesse darstellt, zu dessen Gunsten gemäß Artikel 23 Absatz 1 DSGVO bestimmte Grundsätze des Artikels 5 eingeschränkt werden können. Dieser Gedanke liegt der Privilegierung in Artikel 5 Absatz 1 Buchst. b DSGVO bereits zugrunde.

Zu vertiefen ist in Bezug auf § 13 LDSG die Frage, ob weiterer Regelungsspielraum zugunsten der Forschung besteht. Diese Frage stellt sich insbesondere im Hinblick auf das angesprochene Thema der Verwendung bereits erhobener (großer) Mengen personenbezogener Daten auch für andere Zwecke als diejenigen, für die die Daten erhoben wurden, also für die Sekundärforschung.

Diese sollte unter definierten Anforderungen ohne Einwilligung zulässig sein. Ein besonderes Interesse besteht diesbezüglich insbesondere für die gemeinwohlorientierte Forschung mit retrospektiven Gesundheitsdaten aus Untersuchungen und Behandlungen von Patientinnen und Patienten.

Ein Lösungsansatz könnte die ausdrückliche Einfügung eines Erlaubnistatbestandes zugunsten der Forschung zur Verarbeitung bereits erlangter personenbezogener Daten (einschließlich besonderer Kategorien personenbezogener Daten) für weitere Forschungszwecke sein. Damit wäre die Forschung eindeutig nicht auf die Einwilligung der betroffenen Personen angewiesen, die häufig nicht zu erlangen ist, entweder, weil die Daten schon vor längerer Zeit erhoben wurden oder weil die betroffenen Personen gar nicht identifiziert wurden.

Für die Zulässigkeit einer solchen Regelung spricht auch Artikel 6 Absatz 4 DSGVO, wonach die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 DSGVO genannten Ziele darstellt, beruhen kann. Dass wissenschaftliche Forschung öffentlicher Stellen ein wichtiges Ziel des allgemeinen öffentlichen Interesses im Sinn des Artikels 23 Absatz 1 Buchst. e DSGVO sein kann, sollte nicht bezweifelt werden. Das Interesse der betroffenen Personen muss in die Beurteilung des Gesetzgebers eingestellt werden. Geeignete Garantien, wie Verschlüsselung oder Pseudonymisierung, sind soweit möglich zu gewährleisten und können die Vereinbarkeit der Weiterverarbeitung gemäß Artikel 6 Absatz 4 Buchst. e DSGVO befördern.

Zugleich müssten gemäß Artikel 23 Absatz 2 DSGVO geeignete technische und organisatorische Maßnahmen zum Datenschutz in den Grenzen der DSGVO angeordnet werden. Entspre-

chende Schutzmaßnahmen können die Dokumentation entsprechend einem Risiko- und Qualitätsmanagementsystem, menschliche Aufsicht, weitgehende Transparenz in Bezug auf die Verwendung der Daten, Aufzeichnungspflichten, technische und organisatorische Maßnahmen zu Genauigkeit, Robustheit und Cybersicherheit sein. Weitere Beispiele für organisatorische Maßnahmen sind Zugangsbeschränkungen sowie die Vereinbarung einer Schweigepflicht oder eines Datengeheimnisses.

Eine allgemeine Vorratshaltung von Daten muss jedoch vermieden werden, da eine Sammlung unbegrenzter Datenmengen für noch nicht definierte Forschungszwecke unzulässig ist. Dies bedeutet, dass grundsätzlich Speicherfristen festgelegt werden müssen. Artikel 89 Absatz 2 DSGVO sieht hiervon keine Ausnahmen vor. Die längere Speicherung personenbezogener Daten für Forschungszwecke über den primär verfolgten Forschungszweck hinaus kann zulässig sein, sofern Garantien für die betroffenen Personen in Bezug auf die Datenminimierung bestehen. Die Landesregierung schließt sich der Auffassung der Datenschutzkonferenz an, die es als Aufgabe des Gesetzgebers ansieht, im Allgemeininteresse liegende Forschung mit Gesundheitsdaten zu ermöglichen, aber auch ihre Grenzen festzulegen und die Interessen der betroffenen Personen zu wahren[73]. Die Regeln der guten wissenschaftlichen Praxis können hierfür Anhaltspunkte liefern.

Sonderfall: Nutzung von KI in der Forschung

Einen Sonderfall der Weiterverarbeitung bestehender Datensätze in der Forschung stellt die Nutzung von KI dar. Die datenschutzrechtliche Problematik der Verwendung personenbezogener Daten für KI-Anwendungen ist der bereits erläuterten bei der Sekundärforschung vergleichbar. KI arbeitet mit großen Datenmengen, was datenschutzrechtliche Probleme in Bezug auf die Grundsätze der Datenminimierung, der Zweckbindung und der Speicherbegrenzung mit sich bringt. Zwar ist auch nach der DSGVO die Verarbeitung großer Datenmengen erlaubt, wenn sie erforderlich ist. Gerade bei der KI ist aber häufig schwer nachzuvollziehen, welche Daten wofür benötigt werden, wodurch die Transparenz für die betroffene Person in Frage gestellt wird.

Ob in Bezug auf die Verwendung und das Training von KI für die Forschung andere Maßstäbe an die Verarbeitung von Daten anzulegen sind als für die Verwendung zu sonstigen Zwecken, bedarf im Gesetzgebungsverfahren näherer Untersuchung im Hinblick auf die Reichweite der Privilegierung der Forschung.

[73] Vgl. Petersberger Erklärung der Datenschutzkonferenz vom 24.11.2024, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf.

(2) Harmonisierung des Datenschutzrechts für die Forschung

Ein weiteres Problem besteht in der fehlenden Einheitlichkeit der Gesetzgebung in Bund und Ländern zu den Tatbestandsvoraussetzungen der Forschung. Dies erschwert insbesondere die länderübergreifende Forschung. Als Beispiel sei erwähnt, dass gemäß § 13 LDSG die Datenverarbeitung öffentlicher Stellen für Forschungszwecke erlaubt ist, wenn die Interessen an der Durchführung des Forschungsvorhabens die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen, während gemäß § 27 BDSG für die Forschung nichtöffentlicher Stellen ein erhebliches Überwiegen der Forschungsinteressen verlangt wird. Dies führt dazu, dass für die Forschung öffentlicher und nichtöffentlicher Stellen unterschiedliche Anforderungen gelten.

Hinzukommt, dass die Datenschutzaufsichtsbehörden der Länder unterschiedliche Anforderungen stellen. Dies stellt insbesondere länderübergreifende Forschungsvorhaben vor schwierige Herausforderungen. Diese benötigen Rechtssicherheit, wenn es um die datenschutzrechtlichen Anforderungen an die Forschung geht.

Die Bundesregierung hat am 18. Juli 2018 die Datenethikkommission eingesetzt. Sie erhielt den Auftrag, innerhalb eines Jahres ethische Maßstäbe und Leitlinien sowie konkrete Handlungsempfehlungen für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstands im Informationszeitalter zu entwickeln. Die Datenethikkommission empfiehlt in ihrem 2019 vorgelegten Gutachten eine Harmonisierung der forschungsspezifischen Regelungen[74]:

„Auch, wenn der rechtliche Rahmen für datenbasierte Forschung in Deutschland – auch in Bezug auf Gesundheitsdaten und andere besondere Kategorien von Daten – durchaus vorhanden ist, fehlt es diesem Regelungsrahmen schon aufgrund der föderalen Struktur und den grundgesetzlich festgeschriebenen Gesetzgebungskompetenzen von Bund und Ländern in Details an Einheitlichkeit. Dies führt aus Sicht der Forschung zu Rechtsunsicherheit, die zusätzlich dadurch verstärkt wird, dass verlässliche Auslegungshilfen, insbesondere was die Anforderungen an eine wirksame Einwilligung und das „erheblich überwiegende Interesse“ des Forschenden im Sinne des § 27 BDSG betrifft, noch ausstehen. Diese Rechtsunsicherheit könnte die datenbasierte Forschung in Deutschland beeinträchtigen.“[75].

[74] Abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.
[75] A.a.O. S. 65.

- Bewertung des LfDI (S. 37):

Die föderale Diversität der Forschungsregelungen lasse sich durch das LDSG nicht lösen. Der Landesgesetzgeber könnte sich mit anderen Ländern über eine einheitliche Gesetzgebung nach dem Vorbild z. B. der Landesverwaltungsverfahrensgesetze verständigen. Dies entspreche einer Empfehlung der Datenschutzkonferenz vom 23. November 2023.

Lösungsvorschlag der Landesregierung:

Bezogen auf den Gesundheitsstandort Baden-Württemberg hat die Landesregierung mit der Roadmap Gesundheitsdatennutzung bereits ressortübergreifend Maßnahmen zur Harmonisierung angestoßen. Dem Landesgesetzgeber stehen allerdings nur begrenzte Möglichkeiten zu, zur Vereinheitlichung beizutragen. Hierzu gehört vor allem die Empfehlung, die Vorschrift des § 13 LDSG an die Bundesregelung anzugleichen (siehe unten). Vielfach kommt es auf die Auslegung der Vorschriften an. Diesbezüglich kommt den Aufsichtsbehörden die Aufgabe zu, die Grundsätze und Vorgaben der DSGVO einheitlich auszulegen. Einheitliche Standards auf europäischer Ebene für Anonymisierung und Pseudonymisierung, die in der Forschung grundlegende Verfahren sind, würden hier einen erheblichen Fortschritt bedeuten. Hierfür hat sich der Bundesrat mit der Zustimmung Baden-Württembergs im Zuge der Evaluierung der DSGVO durch die Europäische Kommission eingesetzt[76].

Die Weiterentwicklung des § 13 LDSG in Hinblick auf die Nutzung von Gesundheitsdaten wird im Rahmen des Forums Gesundheitsstandort Baden-Württemberg unter Einbeziehung von Expertinnen und Experten weiterverfolgt. Um die Nutzung von Gesundheitsdaten im Sinne der Roadmap Gesundheitsdatennutzung weiter zu verbessern, werden hierbei auch andere Landesgesetze, wie beispielsweise das Landeskrankenhausgesetz, in den Blick genommen. Ziel ist die schnellstmögliche Umsetzung der in der Roadmap eruierten Punkte. Die Stellungnahme ist daher in Bezug auf diesen Aspekt nicht abschließend zu verstehen.

(3) Gemeinwohlorientierte Forschung

Die Datenethikkommission führt des Weiteren aus[77]:

„Soweit die Forschungstätigkeit maßgeblich auf eine gemeinwohlorientierte Datennutzung ausgerichtet ist (etwa zur Gesundheitsvorsorge, zur Entwicklung nachhaltiger Mobilitätskonzepte oder allgemein zur Verbesserung von Lebensbedingungen), empfiehlt die DEK, vorhan-

[76] Vgl. Bundesrat Drs. 639/23.
[77] A.a.O. S. 124.

dene datenschutzrechtliche Privilegierungstatbestände auszuschöpfen und Forschung im Rahmen von Abwägungen als ein besonders gewichtiges Interesse zu werten. Ergänzend sollten die Bundesländer vorhandene Regelungsbefugnisse, beispielsweise im Kontext des Hochschulrechts oder aber auch im Rahmen des Datenschutzrechts, innovationsfreundlich sowie im Geiste des vorgenannten Forschungsprivilegs ausfüllen. Der Begriff der wissenschaftlichen Forschung ist dabei – auch unter Einbeziehung der Rechtsprechung des Bundesverfassungsgerichts – weit zu verstehen. Nicht entscheidend ist dabei, ob die jeweilige Forschungstätigkeit durch öffentliche oder durch private Stellen betrieben wird."

Die Landesregierung schließt sich dem innovationsfreundlichen Ansatz an. Insbesondere ist zu unterstreichen, dass nach Auffassung der Landesregierung kein Grund besteht, private Stellen vom Datenzugang auszuschließen, wenn Forschung auf der Grundlage der DSGVO gemeinwohlorientiert betrieben wird. Grundsätzlich sollten daher auch nichtöffentliche Stellen, z. B. im Rahmen von Forschungsverbünden, von den Forschungsdaten profitieren können.

Zum Gemeinwohlbegriff wurde bereits oben zu § 5 LDSG ausgeführt. Die Datenethikkommission versteht unter gemeinwohlorientierter Forschung wie gesehen solche zur Gesundheitsvorsorge, zur Entwicklung nachhaltiger Mobilitätskonzepte oder allgemein zur Verbesserung von Lebensbedingungen. Der mittlerweile geltende Daten-Governance-Rechtsakt nennt als Gemeinwohlzwecke den Schutz der öffentlichen Gesundheit, der Sicherheit, der Umwelt, der guten Sitten, der Verbraucher sowie der Privatsphäre und personenbezogener Daten[78]. Als Ziele von allgemeinem Interesse werden die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse aufgeführt[79]. Die Auslegung des unbestimmten Rechtsbegriffs „Gemeinwohl" ist gerichtlich überprüfbar.

(4) Generalklausel versus Spezialregelung

Die Regelung in § 13 LDSG wurde als Generalklausel für die Forschung aller öffentlichen Stellen gestaltet. Diese ermöglicht es zwar, unabhängig vom Zweck der Forschung Regeln für die Zulässigkeit aufzustellen. Sie umfasst aber naturgemäß nicht spezifische Vorschriften für bestimmte Bedarfe. Es wird daher als vorzugswürdig angesehen, bei Bedarf spezifische Regelungen zu erlassen, die dann dem LDSG vorgingen.

[78] A.a.O. Erwägungsgrund 24.
[79] A.a.O. Erwägungsgrund 45.

In Bezug auf die Forschung mit Gesundheitsdaten könnte dies durch Änderungen im Landeskrankenhausgesetz umzusetzen sein.

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten können Besonderheiten zu beachten sein. Hingewiesen wird in diesem Zusammenhang auf das Urteil des Verwaltungsgerichts Hamburg vom 22.07.2022[80], das (in Bezug auf das Hamburger Krebsregistergesetz) unter Verweis auf die Rechtsprechung des Europäischen Gerichtshofs zur Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Absatz 2 Buchst. h, i und j DSGVO ausführt:

„Nach der unionsgerichtlichen Rechtsprechung muss eine Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt."

Da entsprechende Garantien nur spezifisch getroffen werden können, bedarf die Verarbeitung besonderer Kategorien personenbezogener Daten in der Regel eines spezifischen Gesetzes. Entsprechende Vorschriften finden sich beispielsweise im Gesundheitsdatennutzungsgesetz (GDNG).

bb) Rückmeldungen zu § 13 LDSG im Einzelnen

Dem befürworteten forschungsfreundlichen Ansatz entsprechend sollte das Datenschutzrecht soweit wie möglich die Forschung unterstützen. Hierzu liegen bezogen auf das Landesrecht konkrete Vorschläge aus dem Wissenschaftsbereich (Kliniken und Hochschulen) vor.

Die Vorschläge zielen auf Erleichterungen für die Forschung, insbesondere für die Sekundärforschung, die Forschung in Verbünden mit der Privatwirtschaft und Veröffentlichungen.

(1) „Erforderlichkeit" der Datenverarbeitung

Es wird angeregt, die Formulierung des § 13 Absatz 1 LDSG an die Formulierung in § 27 BDSG anzugleichen. Dies würde bedeuten, auch im Landesrecht nur auf die Erforderlichkeit der Verarbeitung der personenbezogenen Daten als Tatbestandsvoraussetzung zu rekurrieren,

[80] VG Hamburg, Urteil vom 22.07.2022 - 21 K 1802/21, veröffentlicht in openJur 2022, 22447.

ohne diese, wie in § 13 LDSG erfolgt („wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können“), näher auszuformulieren.

- Bewertung des LfDI (S. 29f.):

Der LfDI unterstützt den Vorschlag. Er nimmt Bezug auf die Entschließung der Datenschutzkonferenz vom 23. November 2011 – „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“ – und regt dementsprechend die Vereinheitlichung der Forschungsregelungen in Bund und Ländern (zum Beispiel nach dem Vorbild der Verwaltungsverfahrensgesetze) mit einem angemessenen und hohen Datenschutzniveau an. Hierfür stehe er zur näheren beratenden Unterstützung zur Verfügung.

Um die Umsetzung in der Forschungspraxis zu befördern, die nach Ansicht des LfDI entscheidend ist, schlägt er Aufzeichnungspflichten und eine Unterrichtungspflicht der Datenschutzbeauftragten der Forschungseinrichtungen entsprechend § 13 Absatz 1 des Niedersächsischen Datenschutzgesetzes vor sowie ein verpflichtendes Schulungsangebot an den Universitäten zum Datenschutz und zur Sicherung der guten wissenschaftlichen Praxis vor. Für die Schulungen stehe er durch seine Erfahrungen mit seinem Schulungszentrum gerne beratend zur Verfügung.

Position der Landesregierung:

Im Interesse einer harmonisierten Forschungsregelung in Bund und Land wird der Vorschlag eines Gleichlaufs mit dem Bundesdatenschutzgesetz, dort in § 27 geregelt, befürwortet. Damit würde diesbezüglich auch gleiches Recht für die öffentlichen und nichtöffentlichen Stellen für die Datenverarbeitung zu Forschungszwecken hergestellt. Der Begriff der Erforderlichkeit wird auch in Artikel 9 Absatz 2 Buchst. j DSGVO verwendet, der der Regelung in § 13 LDSG zugrunde liegt.

Zugleich kann damit dem Missverständnis entgegengewirkt werden, dass die Forschung aufgrund dieser Rechtsgrundlage nachrangig gegenüber der Forschung auf Grundlage einer Einwilligung sei. Beide Rechtsgrundlagen stehen, wie bereits in der DSGVO angelegt, gleichberechtigt nebeneinander.

Dagegen wird es nicht für notwendig erachtet, eine Angleichung an das Bundesdatenschutzgesetz auch in Bezug auf den Grad des Überwiegens der Forschungsinteressen herbeizuführen. Der Landesgesetzgeber hat bewusst kein „erhebliches Überwiegen“ wie in § 27 BDSG für erforderlich erachtet. Zumindest für die öffentlichen Stellen im Land sollte es möglich

sein, Forschung bei überwiegendem Forschungsinteresse durchführen zu können. Kooperationen mit dem Bund sind dennoch unproblematisch, da bei „erheblichem“ Überwiegen immer auch die Tatbestandsvoraussetzung des Überwiegens nach § 13 LDSG erfüllt ist.

(2) Forschung im Interesse der Allgemeinheit

Es wurde angeregt, neben den Interessen der öffentlichen Stelle auch Interessen der Allgemeinheit an einem Forschungsvorhaben in der Vorschrift des § 13 LDSG zu erwähnen und damit als zulässiges Interesse zu berücksichtigen.

- Bewertung des LfDI (S. 30):

Der LfDI rät von einer entsprechenden Regelung ab. Hierdurch entstünde eine Differenz zu § 27 BDSG. Das Interesse der Allgemeinheit sei – richtig verstanden – nicht von dem Interesse der öffentlichen Stelle zu unterscheiden. Maßgeblich müsse immer das allgemein-wissenschaftliche Interesse einschließlich des Interesses am konkret erstrebten Erkenntnisgewinn sein. Nach seiner Auffassung könne ein persönliches Interesse oder ein Individualinteresse der öffentlichen Stelle, z. B. Einführung eines neuen Verfahrens, nicht auf die Vorschrift des § 13 LDSG gestützt werden.

Position der Landesregierung:

In der Regel wird nach Auffassung der Landesregierung davon auszugehen sein, dass das Interesse der öffentlichen Stelle an der Durchführung des Forschungsvorhabens mit dem Interesse der Allgemeinheit identisch ist. Denn öffentliche Stellen sind generell dem Gemeinwohl verpflichtet. Deshalb sollte den öffentlichen Stellen auch erlaubt sein, für die Verbesserung eigener Geschäftsprozesse Forschungsprojekte durchzuführen. Selbstverständlich gilt dies nur unter dem Vorbehalt, dass hierfür nicht anonymisierte Daten ausreichen.

Auch § 27 BDSG stellt auf das Interesse des Verantwortlichen an der Verarbeitung ab, weshalb zur Vermeidung von Abweichungen kein anderer Terminus eingeführt werden sollte.

Für die Sekundärforschung, also die Weiterverarbeitung der Daten, könnte es im Interesse der Rechtssicherheit nützlich sein, wenn aus der Gesetzesvorschrift beispielhaft ersichtlich wäre, welches Forschungsinteresse für die Weiterverarbeitung als gemeinwohlorientiert anzusehen ist. Somit könnte ein Katalog vereinbarer Zwecke entstehen. Zu denken wäre an wissenschaftliche Forschung im Bereich des Gesundheits- oder Pflegesektors, Forschung als Beitrag zur öffentlichen Gesundheit oder sozialen Sicherheit, statistische Auswertungen, Forschung zur

Produktentwicklung zum Nutzen der Allgemeinheit, Forschung zum Schutz vor Naturkatastrophen, zur Verbesserung der öffentlichen Sicherheit, zur Förderung nachhaltiger Mobilität etc.

Entscheidend für die Aufnahme von Regelungen in das LDSG ist diesbezüglich der Regelungsspielraum, den spezifische Gesetze wie das GDNG oder die vorgeschlagene Verordnung für einen europäischen Raum für Gesundheitsdaten (EHDS-VO)[81] dem Landesgesetzgeber belassen. Das GDNG erlaubt in § 6 explizit den datenverarbeitenden Gesundheitseinrichtungen die Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, zur Förderung der Patientensicherheit, zu Forschungs- und statistischen Zwecken. Auch § 7 GDNG lässt abweichende Landesregelungen zu. Ein weiterer Katalog ergibt sich entsprechend dem Entwurf aus Artikel 34 EHDS-VO für den Gesundheitsbereich[82].

(3) Forschung mit Daten, die unter ein Berufsgeheimnis fallen

Es wird darauf hingewiesen, dass die Forschung mit personenbezogenen Daten stets, sofern Berufsgeheimnisse betroffen seien, die Entbindung von der Schweigepflicht durch die betroffenen Personen erfordere. Das Berufsgeheimnis solle der Forschung aber nicht entgegenstehen. Da Artikel 9 Absatz 3 DSGVO eine solche Regelung den Mitgliedstaaten überlasse, könnte der Gesetzgeber hier handeln.

- Bewertung des LfDI (S. 31f.):

Der LfDI weist darauf hin, dass er für die Aufsicht über die Einhaltung des Berufsgeheimnisses nicht zuständig sei. Eine entsprechende gesetzliche Regelung im LDSG werde kritisch gesehen, da damit die berufsrechtlichen Regelungen gelockert werden müssten. Eine Regelung sollte daher, sofern dies überhaupt in Frage kommt, eher in diese aufgenommen werden. Letztere würden bereits unter engen Voraussetzungen Befugnisse zur Offenbarung enthalten.

Ferner verweist er auf die Neuregelung im GDNG, die in §§ 7, 9 für Datennutzende von Gesundheitsdaten zu Forschungszwecken ein strafbewehrtes Forschungsgeheimnis statuiert.

Position der Landesregierung:

Es wurde richtig bemerkt, dass eine Befreiung von der Schweigepflicht für Forschungszwecke den Beschränkungen des Artikels 9 DSGVO unterliegt, soweit besondere Kategorien personenbezogener Daten betroffen sind. In Artikel 9 Absatz 3 DSGVO wird auf Absatz 2

[81] Vgl. Bundesrat Drs. 256/22.
[82] A.a.O. S. 85f.

Buchst. h Bezug genommen. Die Gesundheitsdatenverarbeitung im Gesundheits- oder Sozialbereich wird demnach nur Fachpersonal gestattet, das einem Berufsgeheimnis oder einer Geheimhaltungspflicht nach nationalem Recht unterliegt.

Um den Anspruch, eine Forschungsklausel zu schaffen, auf deren Grundlage personenbezogene Daten ohne Einwilligung der Betroffenen verarbeitet werden können, effektiv umzusetzen, ist eine Regelung zur Entbindung von der Schweigepflicht essentiell für Daten, die unter die Schweigepflicht fallen. Die Befugnis zum Offenbaren kann bei § 203 StGB auch durch Landesrecht begründet werden und damit die Entbindung von der Schweigepflicht. Wie das im konkreten Fall bestmöglich umzusetzen ist, muss ggf. im Gesetzgebungsverfahren unter Einbeziehung der Berufskammern näher untersucht werden.

(4) Forschung mit menschlichen Gewebe- und Körperflüssigkeitsproben

Soweit der LfDI (S. 32) die vom Wissenschaftsministerium vorgeschlagene datenschutzrechtliche Regelung für die Forschung mit Gewebeproben anspricht, wurde vom Wissenschaftsministerium der Wunsch geäußert, das Thema in der laufenden Evaluierung wegen noch nicht abschließend geklärter Fragen nicht aufzugreifen.

(5) Forschung für KI-Anwendungen

Das Land fördert die Nutzung von KI-Anwendungen im Rahmen von gemeinwohlorientierten Forschungszwecken. Nach Auffassung der Hochschulen fehlt es diesbezüglich an definierten datenschutzrechtlichen Anforderungen.

- Bewertung des LfDI (S. 32f.):

Der LfDI verweist auf das kürzlich von ihm veröffentlichte Diskussionspapier zu der Frage, welche datenschutzrechtlichen Rechtsgrundlagen zum Zweck der Verarbeitung personenbezogener Daten in KI-Anwendungen zur Anwendung kommen können[83]. Hierin werde dargelegt, dass schon unter den aktuellen rechtlichen Rahmenbedingungen KI auch zu Forschungszwekken rechtskonform eingesetzt werden könne. Im Hinblick auf die zu erwartende KI-Verordnung und die darin vorgesehene Möglichkeit von Reallaboren bietet der LfDI weitere Beratung an.

[83] Abrufbar unter Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz - Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

Position der Landesregierung:

Zur Thematik des Einsatzes von KI und seinen datenschutzrechtlichen Voraussetzungen wurde bereits ausgeführt. Ergänzend wird angemerkt:

Zur Präzisierung können auch Leitlinien oder Orientierungshilfen für die Forschung mit KI, vorzugsweise in Zusammenarbeit mit dem LfDI, entwickelt werden, der seine Beratung angeboten hat.

Sofern die Datenverarbeitung auf einer Einwilligung beruht, kann diese Problematik auch durch eine weite Zweckfestlegung in einer breiten Einwilligung („Broad Consent“) in die Nutzung pseudonymisierter Daten umgangen werden.

(6) Forschung mit bereits veröffentlichten Daten

Es wird bemängelt, dass eine Regelung fehlt, welche die Verarbeitung veröffentlichter und damit allgemein zugänglicher Daten zu Forschungszwecken erlaubt. Zwar reichten hierfür größtenteils anonymisierte Daten aus. Teilweise würden aber auch bereits veröffentlichte personenbezogene Daten verarbeitet. § 13 Absatz 1 LDSG würde sich hierzu nur beschränkt eignen, da sich nicht durchweg rechtssicher feststellen ließe, ob die Forschungsinteressen gegenüber den Interessen der betroffenen Personen an einem Ausschluss der Verarbeitung überwögen. Um dies rechtssicher zu gestalten, schlägt der Forschungsbereich eine Regelung für die Verarbeitung allgemein zugänglicher personenbezogener Daten für wissenschaftliche Zwecke vor.

- Bewertung des LfDI (S. 34f.):

Der LfDI hält die Zweckänderung nach Artikel 5 Absatz 1 Buchst. b 2. Halbsatz DSGVO für gerechtfertigt. Allerdings bedürfe die Forschungstätigkeit selbst darüber hinaus einer Rechtsgrundlage. Ohne Anhörung ließen sich die in die Abwägung nach § 13 LDSG einzustellenden Interessen der betroffenen Personen tatsächlich schwer ermitteln. Diese könne nötig sein, um auszuschließen, dass die Veröffentlichung rechtswidrig erfolgte. Der LfDI konzediert, dass es aber auch Konstellationen geben könne, in denen das Einverständnis der betroffenen Person mit der Veröffentlichung offensichtlich und der Verarbeitung zu Forschungszwecken entgegenstehende Interessen nicht ersichtlich seien.

Falls eine Rechtsgrundlage für diese Fallkonstellation geschaffen werden sollte, könnten andere Garantien für die Rechte und Freiheiten der betroffenen Personen gesetzlich eingeführt

werden, um den Eingriff in die Rechte betroffener Personen möglichst gering zu halten. Eignen würden sich Vorschriften zur Verfahrensvorsorge, z. B. ein Verfahren, in dem die Angemessenheit des Vorgehens zuvor von einer einzurichtenden unabhängigen Stelle geprüft und genehmigt werden muss, ferner Transparenzanforderungen und die Möglichkeit zur Ausübung von Betroffenenrechten einschließlich des Widerspruchs. Bezüglich der Verknüpfung der veröffentlichten personenbezogenen Daten mit weiteren Datensätzen für das Forschungsvorhalben, wären weitere Risiken zu bedenken und Vorsorge zu treffen. Hierzu verweist der LfDI auf Seite 8 der Petersberger Erklärung der Datenschutzkonferenz[84].

Aus verfassungsrechtlichen Gründen hält er öffentliche Stellen in der Regel für verpflichtet, vor einem Eingriff in das informationelle Selbstbestimmungsrecht eine Anhörung durchzuführen. Zusätzlich weist er auf Erleichterungen für die Erteilung von Datenschutzinformationen nach Artikel 14 Absatz 5 Buchst. b DSGVO hin.

Position der Landesregierung:

Das Anliegen der Forschung sollte berücksichtigt werden. Vorzugsweise sollte dies in § 13 LDSG geregelt werden. Eine Regelung entsprechend dem Regel-Ausnahme-Verhältnis wird empfohlen. Dies würde bedeuten, dass die Verarbeitung allgemein zugänglicher personenbezogener Daten für wissenschaftliche Forschung in der Regel zulässig ist, es sei denn, dass berechtigte Interessen der betroffenen Personen das Interesse der öffentlichen Stelle überwiegen. Eine entsprechende Regelung könnte auch für die in § 13 LDSG ebenfalls geregelten statistischen Zwecke erwogen werden. Inwieweit den Vorschlägen des LfDI für Garantien und Verfahrensvorsorge zu folgen ist, ist des Weiteren im Gesetzgebungsverfahren zu prüfen.

Eine Regelung zur zweckändernden Verarbeitung allgemein zugänglicher Daten war in § 15 Absatz 2 Nummer 7 LDSG a. F. enthalten. Die meisten Länder haben auch in ihre Datenschutzgesetze nach Geltung der DSGVO einen entsprechenden Zweckänderungstatbestand aufgenommen[85].

Die Zweckänderung sollte allerdings auf den Forschungsbereich beschränkt bleiben und unter dem Vorbehalt stehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen nicht entgegenstehen.

Für sonstige Zwecke wird die Verarbeitung allgemein zugänglicher Daten im Allgemeinen nicht für erforderlich gehalten. Denn gemäß Artikel 6 Absatz 4 in Verbindung mit Artikel 23 DSGVO sind Zweckänderungen auf bestimmte Zwecke beschränkt. Generell kann dies nicht

[84] Siehe unter Fußnote 73.
[85] Vgl. z. B. die Regelungen in Artikel 6 Absatz 2 Bayerisches Datenschutzgesetz, § 15 Berliner Datenschutzgesetz, § 9 Absatz 4 Datenschutzgesetz Nordrhein-Westfalen.

begründet werden. Die Forschung kann als wichtiges Ziel des öffentlichen Interesses unter Artikel 23 Absatz 1 DSGVO subsumiert werden. Sollte auch sonst ein Bedürfnis bestehen, allgemein zugängliche Daten zu verarbeiten, sollte auf spezielle Rechtsgrundlagen, z. B. das Polizeigesetz oder die Strafprozessordnung, zurückgegriffen werden. Im Übrigen sind des Weiteren bei der Verarbeitung besonderer Kategorien personenbezogener Daten, wie z. B. Gesundheitsdaten, Artikel 9 Absatz 2 DSGVO und die dort genannten Ausnahmen zu beachten.

(7) Weitergabe von Forschungsdaten an Kooperationspartner

Um exzellente interdisziplinäre Forschungsergebnisse erzielen zu können, betreiben die Universitäten ihre Forschung in Kooperationsverbänden, sowohl mit anderen Universitäten, als auch mit Forschungseinrichtungen, wie der Max-Planck-Gesellschaft oder den Instituten der Leibniz-Gemeinschaft. Ferner finden regelmäßig Forschungsprojekte mit Klinika oder öffentlichen Ämtern statt. Dabei sind Arbeitspakete dergestalt üblich, dass eine Stelle die Daten zum Zweck der eigenen Forschung erhebt und diese dann der anderen Stelle zu deren eigenen Forschungszwecken zur Verfügung stellt. Gerade bei Forschungsprojekten, die nicht auf eine Einwilligung, sondern auf § 13 Absatz 1 LDSG gestützt werden, wird eine Klarstellung zur Übermittlung personenbezogener Daten zu Forschungszwecken angeregt, d.h. zur Frage, inwieweit § 13 Absatz 1 LDSG für die Übermittlung zu Forschungszwecken herangezogen werden kann.

In der Roadmap Gesundheitsdatennutzung Baden-Württemberg wird darüberhinausgehend auch die Kooperation mit der privatwirtschaftlichen Forschung, z. B. Pharmaunternehmen, angesprochen. Hierfür bedarf es ebenfalls entsprechender Rechtsgrundlagen. Ziel ist, gemeinwohlorientierte Forschung unabhängig von der Rechtsform der forschenden Stelle zu ermöglichen.

- Bewertung des LfDI (S. 35f.):

Der LfDI hält eine Gesetzesänderung zu dem angestrebten Zweck nicht für erforderlich. Er hält eine Einwilligungslösung für zielführend. Alternativ würde § 13 LDSG eine geeignete Rechtsgrundlage darstellen, wenn zuvor eine gemeinsame Verantwortlichkeit vereinbart wurde.

Position der Landesregierung:

Grundsätzlich regelt § 13 LDSG jede Form der Verarbeitung von Forschungsdaten, also auch die Übermittlung. Entsprechend der Privilegierung der Forschung in der DSGVO ist die Weitergabe von personenbezogenen Daten für wissenschaftliche oder historische Forschungszwecke in Bezug auf die Durchbrechung der Zweckbindung durch die Vorschrift des Artikels 5 Absatz 1 Buchst. b DSGVO ohne Einwilligung legitimiert. Der Verweis des Artikels 5 Absatz 1 Buchst. b auf Artikel 89 Absatz 1 DSGVO wird in der Kommentarliteratur seinem Sinn und Zweck nach als Bedingung verstanden[86]. Für Gesundheitsdaten sind zusätzlich die Grenzen des Artikels 9 Absatz 2 Buchst. j DSGVO in Verbindung mit Artikel 89 Absatz 1 DSGVO zu beachten. Die Daten sind daher soweit möglich zu minimieren.

Die DSGVO stellt in Bezug auf die Zulässigkeit der Datenverarbeitung auf den Zweck, nicht auf die Rechtsform der verantwortlichen Stelle ab. Auch Kooperationen mit der gemeinwohlorientierten privatwirtschaftlichen Forschung, in Bezug auf Gesundheitsdaten also zum Beispiel mit der Pharmaindustrie, werden daher als zulässig angesehen. Die gemeinsame Verantwortlichkeit ist zu prüfen.

(8) Übermittlung für Nutzung durch Privatwirtschaft

Zur Umsetzung der Roadmap Gesundheitsdatennutzung kam weitergehend die Frage auf, ob und unter welchen Voraussetzungen Gesundheitsdaten für weitere Zwecke an die Privatwirtschaft, unter anderem die Pharmaindustrie, herausgegeben werden dürfen.

Position der Landesregierung:

Nach seinem Wortlaut legitimiert § 13 LDSG die Forschung im Interesse der öffentlichen Stelle. Für die Weitergabe von Daten zu Forschungszwecken der empfangenden Stelle kann nach der bisherigen Rechtslage insbesondere § 6 LDSG herangezogen werden. Diese Norm kann jedoch keine Anwendung auf besondere Kategorien personenbezogener Daten, wie Gesundheitsdaten, finden. Hierfür ist geplant, eine eigene klarstellende Regelung, ggf. auch bereichsspezifisch für Patientendaten, zu erarbeiten, die auch die Bedingungen für die Weitergabe präzise festlegt.

Grundsätzlich sollte die Weitergabe für Forschungszwecke unabhängig von der Rechtsform der forschenden Stelle aus Sicht der Landesregierung zulässig sein. Dies kann auf der Grundlage des in Artikel 9 Absatz 2 Buchst. j DSGVO genannten Zwecks auch für besondere Kategorien personenbezogener Daten zugelassen werden.

[86] Vgl. Heberlein in Ehmann/Selmayr Artikel 5 Rn. 17.

In Artikel 9 Absatz 2 Buchstabe i DSGVO werden neben der Forschung weitere Zwecke im Interesse der öffentlichen Gesundheit genannt wie die Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimittel- und Medizinprodukten. Hierzu trägt insbesondere die Pharmaindustrie bei. Die Weiterverwendung zu diesen Zwecken wird durch Artikel 17 Absatz 3 Buchst. c DSGVO gestützt.

(9) Pseudonymisierung erforderlich

Hinsichtlich der Schutzmaßnahme Pseudonymisierung wurde angeregt, entsprechend der Regelung in § 9 Absatz 2 LDSG eine Bezugnahme auf den Aufwand zu ergänzen.

- Bewertung des LfDI (S. 68)

Der LfDI kann die Anregung nicht nachvollziehen.

Position der Landesregierung:

Gemäß Artikel 89 Absatz 1 in Verbindung mit Artikel 25, 32 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um die Datenschutzgrundsätze wirksam umzusetzen und den betroffenen Personen ausreichende Garantien zu gewähren. Die Pseudonymisierung kann nach Artikel 89 Absatz 1 DSGVO eine solche Maßnahme darstellen. Ihre Erforderlichkeit hat sich nach der DSGVO allein danach auszurichten, ob das Verarbeitungsrisiko und die Eintrittswahrscheinlichkeit des Risikos sie erfordern, wobei der Stand der Technik zu berücksichtigen ist. Die Pseudonymisierung ist beispielhaft als Standardmaßnahme in Artikel 32 DSGVO erwähnt. Eine Ausnahme von den Maßnahmen nach Artikel 32 DSGVO ist im Rahmen von Artikel 89 DSGVO nicht vorgesehen.

(10) Pseudonymisierung statt Anonymisierung

Seitens der Kliniken besteht Interesse daran, patientenbezogene (Behandlungs-)Daten möglichst nicht zu anonymisieren, sondern nur zu pseudonymisieren, um geeignete Kandidaten für Studien finden zu können.

- Bewertung des LfDI (S. 33)

Der LfDI hält eine entsprechende Ergänzung nicht für notwendig. Es sei nicht ersichtlich, warum in solchen Fällen nicht mit einer Einwilligung gearbeitet werden könne. Denn die Mitwirkungsbereitschaft der Patienten sei für die Teilnahme an Studien in jedem Fall erforderlich

und könne vorab erfragt werden. Pseudonymisierung sollte als technische und organisatorische Maßnahme ohnehin genutzt werden. Denn der Schutz persönlicher Informationen sei im Hinblick auf die Sicherstellung des Vertrauens in die wissenschaftliche Forschung sowie die Akquirierung von Teilnehmern für wissenschaftliche Studien essentiell.

Position der Landesregierung:

Die in § 13 Absatz 2 LDSG vorgeschriebene Anonymisierung entspricht den Vorgaben der DSGVO und ist im Übrigen in § 27 Absatz 3 BDSG ebenso geregelt. Grundsätzlich sind gemäß Artikel 89 Absatz 1 DSGVO für die Verarbeitung zu Forschungszwecken technische und organisatorische Maßnahmen als Garantien für die Rechte und Freiheiten der betroffenen Personen zu treffen. Die Pseudonymisierung wird als mögliche Maßnahme beispielhaft erwähnt, der Anonymisierung jedoch Vorrang eingeräumt[87]. Die Pseudonymisierung ist die regelmäßig zu treffende Maßnahme, wenn zur Erreichung des Forschungszwecks eine vollständige Anonymisierung nicht möglich ist[88].

Solange die personenbezogene Information weiterhin in der zugehörigen Akte gespeichert ist, kann die vollständige Anonymisierung nicht möglich sein. Im Einklang mit Artikel 89 Absatz 1 DSGVO ist eine effektive Pseudonymisierung als Schutzmaßnahme zu treffen, wenn die Anonymisierung nicht möglich oder für weitere zulässige Forschungsvorhaben nicht sinnvoll ist. Wenn der Forschungs- oder Statistikzweck dies erfordert, ist – wie in § 13 Absatz 2 LDSG geregelt – die Zusammenführung der Einzelangaben zulässig.

Von entscheidender Bedeutung ist daher, wann die personenbezogenen Daten gemäß Artikel 17 DSGVO zu löschen sind. Wie sich aus Artikel 5 Absatz 1 Buchst. e in Verbindung mit Artikel 17 Absatz 3 DSGVO ergibt, können für Forschungszwecke die Speicherfristen verlängert sein, sofern dies für einzelne Forschungsvorhaben erforderlich ist. Dies ermöglicht es, dass Daten länger zugunsten der Forschung vorgehalten werden können. Hier könnten ggf. die anerkannten Standards der guten wissenschaftlichen Praxis zur Aufbewahrung von Primärdaten zugrunde gelegt werden.

Die Pseudonymisierung kann auch gewählt werden, wenn die Personen im Verlauf des weiteren Forschungsvorhabens zwingend erneut kontaktiert werden müssen. Jedoch ist eine Vorratshaltung geeigneter Kandidaten bzw. deren Daten für weitere Studien undefinierter Art nicht zulässig. Hierfür wäre dann auf die vom LfDI vorgeschlagene Einwilligungslösung zurückzugreifen.

[87] Vgl. Raum in Ehmann/Selmayr, Artikel 89 Rn. 35, 37.
[88] Vgl. Seite 6 der Petersberger Erklärung der Datenschutzkonferenz, wie unter Fußnote 73.

(11) Veröffentlichung von Forschungsdaten

§ 13 Absatz 3 LDSG erlaubt die Veröffentlichung personenbezogener Daten nur in besonderen Ausnahmefällen, im Übrigen nur in anonymisierter Form oder mit informierter Einwilligung.

Seitens der Wissenschaft wird hierzu angemerkt: Veröffentlichung von Forschungsergebnissen sei der Forschung immanent und gehöre zur guten wissenschaftlichen Praxis. Anonymisierung sei nicht immer möglich, vor allem, wenn die personenbezogenen Daten bereits vorher nur pseudonymisiert veröffentlicht wurden. Dementsprechend wird eine Ergänzung des § 13 Absatz 3 LDSG um eine Erlaubnis zur Veröffentlichung von personenbezogenen Daten, die aus allgemein zugänglichen Verzeichnissen oder amtlichen Quellen entnommen werden können, oder deren Veröffentlichung guter wissenschaftlicher Praxis entspricht, sofern nicht der Veröffentlichung entgegenstehende Interessen der betroffenen Person überwiegen, vorgeschlagen.

- Bewertung des LfDI (S. 36):

Der LfDI lehnt die vorgeschlagene Änderung ab. Im Hinblick auf die Sicherstellung des Vertrauens in die wissenschaftliche Forschung sowie die Akquirierung von Teilnehmern für wissenschaftliche Studien sei der Schutz persönlicher Informationen essentiell.

Position der Landesregierung:

Die Veröffentlichung personenbezogener Daten ist derzeit nur mit Einwilligung möglich. Die Schaffung einer Rechtsgrundlage für eine Veröffentlichung ohne Einwilligung müsste außer der Prüfung der Notwendigkeit und Verhältnismäßigkeit folgendes beachten:

Nach Möglichkeit sollte immer versucht werden, Anonymität herzustellen. Vielfach entspricht es jedoch guter wissenschaftlicher Praxis, mit pseudonymisierten Daten zu arbeiten. Für die Veröffentlichung ist die Entfernung des Personenbezugs in diesen Fällen häufig nicht möglich, so dass ohne Rechtsgrundlage keine Veröffentlichung erfolgen kann.

Unter der Voraussetzung, dass die Veröffentlichung für die Erfüllung der wissenschaftlichen Forschungszwecke erforderlich ist, könnte wegen der Grundrechtsbezogenheit der Forschung dem Vorschlag der Wissenschaft zugestimmt werden. Hingewiesen wird auf das KunstUrhG, das zum Schutz der Kunstfreiheit die Veröffentlichung einer Abbildung erlaubt, wenn die abgebildete Person nur als Beiwerk erscheint.

97

11. Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken (§ 14 LDSG)

a) Zum Norminhalt

Die Archivierung besonderer Kategorien personenbezogener Daten bedarf einer besonderen Ermächtigung, welche auf der Grundlage von Artikel 9 Absatz 2 Buchst. j DSGVO zulässig ist. Unter Ausnutzung der Öffnungsklausel des Artikels 89 Absatz 3 DSGVO werden die Betroffenenrechte eingeschränkt.

b) Rückmeldungen und Bewertung

Der LfDI hält entsprechend seiner Stellungnahme vom November 2020 die Beschränkungen der Betroffenenrechte in § 14 Absatz 2 bis 5 LDSG für zu weitgehend. Es dürften gemäß Artikel 89 Absatz 3 DSGVO nur Regelungen zur Einschränkung getroffen werden, ohne die die Archivzwecke unmöglich gemacht oder ernsthaft beeinträchtigt würden. Diese Beschränkung werde nicht eingehalten:

- Dies bezieht er auf Absatz 2, nach dem das Auskunftsrecht wegen eines unvertretbaren Verwaltungsaufwands ausgeschlossen werden könne.

- Nach Auffassung des LfDI berücksichtige der Ausschluss des Berichtigungsrechts in Absatz 3 nicht hinreichend Fälle, in denen die betroffene Person ein gewichtiges Interesse an der Richtigstellung habe und der Archivzweck dennoch nicht unmöglich oder ernsthaft beeinträchtigt werde. Hierbei sei vor allem an Rehabilitationszwecke zu denken.

- In Absatz 4, der die Beschränkung weiterer Betroffenenrechte erlaube, sieht der LfDI eine unzulässige Wiederholung des Wortlauts des Artikels 89 Absatz 3 DSGVO. Er vermisst außerdem die Einhaltung der Anforderungen des Artikels 23 Absatz 2 DSGVO.

Im Ergebnis empfiehlt der LfDI eine Neufassung unter Beachtung des Verhältnismäßigkeits- und Bestimmtheitsgrundsatzes.

Der Landtag sieht dagegen keinen Änderungsbedarf hinsichtlich der Derogationen der DSGVO in § 14 LDSG. Vor allem die Einschränkung des Auskunftsrechts in § 14 Absatz 2 wird als praxisgerecht bewertet.

Seitens eines Regierungspräsidiums wird berichtet, dass eine Stelle die klare Regelung der Anbietungspflicht in § 14 Absatz 5 LDSG begrüße. Andererseits sehe sie zugleich die Gefahr,

dass im Rahmen der zunehmenden Digitalisierung von Verwaltungsprozessen die Funktion der Archive als Langzeitgedächtnis der Verwaltung und Gesellschaft beeinträchtigt werden könnte.

- Bewertung des LfDI (S. 37f.):

Der LfDI hält an seiner Stellungnahme fest. Er empfiehlt eine Neufassung des § 14 LDSG mit nur restriktivem Gebrauch der Öffnungsklausel des Artikels 89 Absatz 3 DSGVO unter Beachtung des Verhältnismäßigkeits- und Bestimmtheitsgrundsatzes.

Position der Landesregierung:

Nach Auffassung der Landesregierung halten sich die Einschränkungen der Betroffenenrechte in § 14 LDSG innerhalb der Grenzen des Artikels 89 Absatz 3 DSGVO.

Zu Absatz 2:
Die Einschränkung des Auskunftsrechts in § 14 Absatz 2 LDSG erfolgt nicht – wie die Stellungnahme des LfDI gelesen werden könnte – allein „aus Gründen des Verwaltungsaufwands“. Die Norm macht das Auskunftsrecht vielmehr abhängig davon, ob das Archivgut durch den Namen der Person erschlossen ist oder ob Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

Was also als vertretbarer Verwaltungsaufwand anzusehen ist, ist durch eine Abwägung festzustellen, in der diese gesetzlich normierten Kriterien ebenfalls einbezogen werden müssen, auf die der Betroffene zumindest hinsichtlich der zu machenden Angaben auch Einfluss hat. Es ist also eine Abwägung zwischen dem Anliegen des Auskunft Suchenden und dem Aufwand zu treffen. Dabei muss auch berücksichtigt werden, inwieweit der Suchaufwand durch konkrete Angaben reduzierbar ist.

Zu Absatz 3:
Die Einwendungen des LfDI werden nicht geteilt. Bei Archivgut geht es um Dokumentation der Vergangenheit, nicht um Material für künftige Entscheidungen. Die Rehabilitation erfolgt nicht dadurch, Vergangenes nicht mehr nachvollziehbar zu machen, sondern indem der Fehler transparent dokumentiert wird. Die Norm beschränkt den Berichtigungsanspruch zwar auf ein Gegendarstellungsrecht, lässt dieses aber generell zu und kommt damit dem eigentlichen Schutzzweck des Betroffenenrechts in ausreichender Art und Weise nach. Etwaige Richtigstellungen (beispielsweise zu Rehabilitationszwecken) erfolgen in einem gesonderten – nicht archivischen – Verwaltungsakt, der wiederum durch die Beifügung im Archiv archiviert werden kann. Nur so wird die Verfälschung der Dokumente vermieden, die ihrerseits auch für

weitere Betroffene für deren Belange in der ursprünglichen Form authentisch bereitstehen müssen. Eine Änderung archivierter Dokumente würde wiederum deren Recht auf Richtigstellung substantiell beeinträchtigen bzw. unmöglich machen. Daher ist diese Umsetzung von Artikel 89 Absatz 3 DSGVO in der geltenden Form für die Verwirklichung der spezifischen Archivzwecke notwendig. Ein Widerspruch zu Artikel 89 Absatz 3 DSGVO ist auch hier nicht erkennbar. Auch hier wird darauf hingewiesen, dass § 28 Absatz 3 BDSG eine wortlautidentische Regelung getroffen hat.

Zu Absatz 4:
Die Norm wiederholt zwar den Wortlaut der Öffnungsklausel des Artikels 89 Absatz 3 DSGVO, hat aber in Bezug auf die nicht einzeln aufgeführten weiteren Betroffenenrechte klarstellenden Charakter. Ein Änderungsbedarf ist daher nicht zu erkennen.

12. Datenverarbeitung bei Dienst- und Arbeitsverhältnissen (§ 15 LDSG)

a) Zum Norminhalt

Die Vorschrift ist die zentrale Norm für die Verarbeitung von Beschäftigtendaten bei den öffentlichen Stellen. Eine entsprechende Norm gab es bereits in der Vorgängervorschrift des LDSG a. F.. Allerdings war es das Anliegen des Gesetzgebers, im LDSG die neuen Gefahren für die Beschäftigten durch die Verarbeitung biometrischer Daten zu berücksichtigen sowie die durch die Digitalisierung verstärkten Möglichkeiten der Verhaltens- und Leistungskontrolle bei der Verarbeitung von Beschäftigtendaten zu beschränken[89]. Mittlerweile werden hier auch die Möglichkeiten der KI zu gewärtigen sein.

An dieser Stelle ist auf das Urteil des Europäischen Gerichtshofs vom 30. März 2023 hinzuweisen, das sich mit der nationalen Umsetzung des Artikels 88 DSGVO (in Hessen) befasst hat und Grundsätze des Beschäftigtendatenschutzes darlegt[90].

Die Öffnungsklausel des Artikels 88 Absatz 1 DSGVO lässt spezifischere nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu. Nach dem Urteil ist fraglich, ob die erlassene Vorschrift den Anforderungen des Artikels 88 DSGVO genügt. Der Europäische Gerichtshof hält eine nationale Rechtsvorschrift nur dann für eine spezifischere Vorschrift, wenn diese den Anforderungen des Artikels 88 Absatz 2 DSGVO genügt. Hierzu genüge das alleinige Abstellen auf die Erforderlichkeit nicht. Vielmehr seien für Regelungen auf der Grundlage von Artikel 88 Absatz 1 DSGVO entsprechend Absatz 2 des genannten Artikels geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die

[89] Vgl. hierzu § 15 Absatz 6 und 7 LDSG.
[90] EuGH, Urteil v. 30.03.2023, Rechtssache C-34/21, abrufbar unter CURIA - Dokumente (europa.eu).

Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz in die Regelung aufzunehmen.

Vor diesem Hintergrund ist § 15 LDSG zu überprüfen. Eine unmittelbare Auswirkung kommt dem Urteil des Europäischen Gerichtshofs zunächst aber nicht zu. Denn der Europäische Gerichtshof hat auch festgestellt, dass die Datenverarbeitung, die im Beschäftigungsverhältnis erforderlich ist, auf Artikel 6 Absatz 1 und 3 DSGVO gestützt werden könne. Die Einhaltung der Grundsätze des Artikels 5 DSGVO wird bei jeder Datenverarbeitung vorausgesetzt. Dies wird in § 15 Absatz 7 LDSG ausdrücklich erwähnt, ist aber generell anzuwenden. Perspektivisch kann an eine gesonderte Regelung des Beschäftigtendatenschutzes gedacht werden[91].

Absatz 2 der Vorschrift befasst sich mit der Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigtenverhältnis. Die Vorschrift stützt sich auf Artikel 9 Absatz 2 Buchst. b DSGVO.

b) Rückmeldungen und Bewertung

aa) Zu § 15 Absatz 2 LDSG

Erweiterung der Zwecke

Das Landespolizeipräsidium bittet darum, in Absatz 2 zusätzlich die Zwecke der Gesundheitsvorsorge und der Arbeitsmedizin entsprechend Artikel 9 Absatz 2 Buchst. h DSGVO aufzunehmen.

- Bewertung des LfDI (S. 40):

Der LfDI verweist auf die entsprechende Regelung in § 22 Absatz1 Nummer 1 Buchst. b BDSG und hält eine vergleichbare Norm in § 15 Absatz 2 LDSG für überlegenswert.

Position der Landesregierung:

Der Vorschlag des Landespolizeipräsidiums sollte umgesetzt werden, da eine entsprechende Regelung bisher fehlt.

[91] Vgl. das entsprechende Vorhaben der Bundesregierung laut Koalitionsvertrag von 2021, S. 18.

bb) Zu § 15 Absatz 5 LDSG

Aufdeckung von Straftaten

§ 15 Absatz 5 LDSG regelt die Herausgabe, soweit Beschäftigte selbst in Verdacht stehen. Das Wissenschaftsministerium bringt hierzu vor, dass es in der Praxis Fälle gebe, in denen zur Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen Daten von Beschäftigten an die Strafverfolgungsbehörden herausgegeben werden müssten, z. B. Dienstpläne, ohne dass die Betroffenen selbst im Verdacht stehen. Dies sollte unter denselben Bedingungen ermöglicht werden.

- Bewertung des LfDI (S. 40f.):

Der LfDI sieht kein Bedürfnis für eine gesonderte Rechtsgrundlage. Verarbeitungen von Daten sonstiger Beschäftigter im Kontext der Aufdeckung von Straftaten und Pflichtverletzungen seien ggf. von § 15 Absatz 1 LDSG gedeckt.

Position der Landesregierung:

Die Landesregierung schließt sich der Auffassung des LfDI an.

cc) Zu § 15 Absatz 6 LDSG

Verarbeitung biometrischer Daten

Die Rückmeldungen geben Anlass, die Normenklarheit der Vorschrift zu untersuchen:

- Der LfDI betrachtet Absatz 6, 2. Halbsatz in Bezug auf das Subjekt „sie“ als nicht normenklar. Die Einwilligung solle im Übrigen nach der Dienst- oder Betriebsverarbeitung erwähnt werden, da sie nur restriktiv als Verarbeitungsgrundlage tauge.

- Die Hochschulen verstehen die Regelung so, dass sie wegen der Verwendung des Wortes „jeweils“ nur eine Einzelfallregelung zuließe. Eine Dienstvereinbarung regele jedoch häufig einen generellen Einsatz, bei dem nicht in jedem Einzelfall ein dringendes dienstliches Bedürfnis besteht. Als Beispiel werden flächendeckende Zutrittskontrollsysteme auf dem Campus einer Universität angeführt. Es wird deshalb die Streichung des Wortes „jeweils“ in Bezug auf eine Dienstvereinbarung angeregt.

- Bewertung des LfDI (S. 41):

Der LfDI lehnt den Vorschlag des Wissenschaftsministeriums ab. Gemäß Artikel 9 Absatz 2 DSGVO sei zu fordern, dass biometrische Zugangssysteme nur installiert werden können, wenn in Bezug auf einzelne Räumlichkeiten jeweils ein dringendes dienstliches Bedürfnis bestehe und kein milderes Mittel in Betracht komme. Denn von der Verarbeitung biometrischer Daten gehe ein hohes Risiko aus. Zur allgemeinen Zugangskontrolle könnten alternativ auch persönliche Passwörter, Chipkarten oder Transponder zum Einsatz kommen.

Des Weiteren sieht er die Notwendigkeit, in Bezug auf biometrische Daten klarzustellen, dass deren Verarbeitung außer zu den in Absatz 6 genannten Zwecken grundsätzlich untersagt sei, also auch nicht nach Absatz 2 in Betracht komme.

Position der Landesregierung:

Das „sie“ bezieht sich auf die Verarbeitung. Eine Klarstellung ist möglich, indem „sie“ durch „die Verarbeitung“ ersetzt wird.

Die Vorschrift erlaubt die Verarbeitung biometrischer Daten, sofern eine betroffene Person ausdrücklich eingewilligt hat oder wenn eine entsprechende Dienst- oder Betriebsvereinbarung geschlossen wurde. In beiden Fällen muss ein dringendes dienstliches Bedürfnis als weiteres Tatbestandsmerkmal gegeben sein. Damit sollte klargestellt sein, dass eine Einwilligung alleine nicht ausreicht beziehungsweise eine entsprechende Dienst- oder Betriebsvereinbarung nur bei einem dringenden dienstlichen Bedürfnis geschlossen werden kann. Inhaltlich sollte hiervon nicht abgewichen werden. Diesbezüglich schließt sich die Landesregierung dem Petitum des LfDI an, die Verarbeitung von biometrischen Daten von Beschäftigten auch per Dienstvereinbarung nur zuzulassen, wo die besondere Situation vor Ort dies erforderlich macht bzw. keine weniger belastenden Maßnahmen zur Verfügung stehen, die denselben Zweck mit geringerer Eingriffstiefe erfüllen. Diesbezüglich ist eine gesetzliche Klarstellung möglich.

Die Einwilligung muss entsprechend Artikel 7 DSGVO freiwillig sein. Dies kann im Beschäftigtenverhältnis fraglich sein und sollte daher auf keinen Fall als vorrangig angesehen werden. Insbesondere kann eine Einwilligung ebenfalls nicht die Prüfung eines milderen Mittels ersetzen. Gegebenenfalls kann dies klargestellt werden.

Für ein weitergehendes Verbot der Verarbeitung biometrischer Daten wird kein Anlass gesehen; Artikel 9 Absatz 2 DSGVO verlangt für biometrische Daten keinen stärkeren Schutz als

für sonstige besondere Kategorien personenbezogener Daten. Dies ist jeweils anhand der Erforderlichkeit und Verhältnismäßigkeit zu entscheiden.

13. Öffentliche Auszeichnungen und Ehrungen (§ 16 LDSG)

a) Zum Norminhalt

Bei Erlass des LDSG wurde davon ausgegangen, dass staatliche Verfahren zur Verleihung von Auszeichnungen und Ehrungen gemäß Artikel 2 Absatz 2 Buchst. a DSGVO nicht unter die DSGVO fallen. Bisher hat keine gerichtliche Überprüfung stattgefunden. Gemäß § 2 Absatz 4 LDSG findet die DSGVO jedenfalls entsprechende Anwendung, sofern nichts anderes bestimmt ist.

Die Vorschrift des § 16 LDSG stellt eine Sonderregelung dar, um die Datenverarbeitung zur Entscheidung über öffentliche Ehrungen auf eine rechtliche Grundlage unabhängig von der Einwilligung zu stellen. Insbesondere zur Feststellung der Ehrwürdigkeit werden die Informationspflicht und das Auskunftsrecht eingeschränkt. Eine Bindung an die Betroffenenrechte wäre in diesen Fällen kontraproduktiv.

Die Vorschrift legitimiert im Übrigen nur die Verarbeitung personenbezogener Daten für die Entscheidung über die Vergabe der Auszeichnungen und Ehrungen. Die weitere Verarbeitung bedarf einer eigenen Rechtsgrundlage, in der Regel einer Einwilligung. Dies betrifft insbesondere die Durchführung der Ehrung sowie deren Veröffentlichung. Es ist auch nicht ersichtlich, dass ein Bedürfnis für die Durchführung öffentlicher Auszeichnungen und Ehrungen ohne eine Einwilligung der Geehrten besteht.

b) Rückmeldungen und Bewertung

„Öffentliche“ Auszeichnungen und Ehrungen

Für die Schulen und Hochschulen wurde die Einbeziehung dort stattfindender Ehrungen und Auszeichnungen vorgeschlagen. Eine entsprechende Regelung für an Hochschulen vorgenommenen Auszeichnungen und Ehrungen würde das Durchführen von z.B. Bachelorfeiern deutlich vereinfachen. Aus dem Schulbereich wird eine genauere Bestimmung dessen gefordert, was unter „öffentliche“ Auszeichnungen und Ehrungen zu subsumieren ist, z. B. im Hinblick auf Abiturfeiern.

Im Ergebnis würde dies eine Einwilligung für die Entscheidung über die Ehrung entbehrlich machen.

- Bewertung des LfDI (S. 43f.):

Der LfDI lehnt die Ausweitung der Vorschrift auf die genannten Ehrungen ab, da die Vereinfachung von Verwaltungsabläufen kein hinreichender Grund für Eingriffe in die Grundrechte der betroffenen Person sei. Unter Umständen könnten Daten zu strafrechtlichen Verurteilungen und andere sensible Daten erfasst sein. Diesen Ehrungen komme im Übrigen nicht derselbe Stellenwert zu wie öffentlichen Ehrungen und Auszeichnungen beispielsweise durch eine Gemeinde.

Für die Regelung in § 16 LDSG sieht er keine Öffnungsklausel gegeben. Außerdem hält er unter Bezugnahme auf die Datenschutzgesetze in Brandenburg und Mecklenburg-Vorpommern eine Ergänzung der Regelung um Betroffenenrechte für erforderlich.

Position der Landesregierung:

Unter den in § 16 LDSG verwendeten Begriff der „öffentlichen Ehrungen“ sollten alle von öffentlichen Stellen vorgenommen Ehrungen gefasst werden. Wegen der entsprechenden Anwendung der DSGVO gemäß § 2 Absatz 4 LDSG sind die Stellen aber verpflichtet, nur die Daten zu erheben, die für die Entscheidung über die vorgesehene Ehrung erforderlich sind. Für Ehrungen für schulische oder akademische Verdienste wird es in der Regel nicht der Erhebung besonderer sensibler Daten bedürfen.

Die Informationspflicht und das Auskunftsrecht werden nicht vollständig ausgeschlossen, sondern es wird der öffentlichen Stelle freigestellt, ob sie die mit der Würdigkeitsprüfung verbundenen Verarbeitungsvorgänge der betroffenen Person offenlegt.[92] Klarstellend könnte eingefügt werden, dass Absatz 1 keine Anwendung findet, wenn der Daten verarbeitenden Stelle bekannt ist, dass die betroffene Person ihrer öffentlichen Auszeichnung oder Ehrung oder der mit ihr verbundenen Datenverarbeitung widersprochen hat[93].

14. Verarbeitung personenbezogener Daten im öffentlichen Interesse (§ 17 LDSG)

a) Zum Norminhalt

Für die Zuverlässigkeitsprüfung im öffentlichen Interesse wird eine eigene Rechtsnorm eingeführt, um die dafür erforderliche Verarbeitung personenbezogener Daten zu legitimieren. Mit der Generalklause in Absatz 2 zur Verarbeitung besonderer Kategorien personenbezogener Daten aus Gründen eines erheblichen öffentlichen Interesses wird von der Öffnungsklausel gemäß Artikel 9 Absatz 2 Buchst. g DSGVO Gebrauch gemacht.

[92] Vgl. Snowadsky in Debus/Sicko, LDSG BW, § 16 Rn. 8.
[93] Vgl. § 13 Hamburgisches Datenschutzgesetz.

b) Rückmeldungen und Bewertung

Aus der Landesverwaltung und seitens der Kommunen gab es zu § 17 LDSG keine Rückmeldungen.

- Bewertung des LfDI (S. 45 bis 47):

Der LfDI fordert, dass der Standort der Regelung geändert und die Regelung selbst inhaltlich konkretisiert werden solle.

Die Vorschrift wiederhole lediglich den Wortlaut der Öffnungsklausel aus Artikel 9 Absatz 2 Buchst. g DSGVO und sei daher zu unbestimmt. Es fehlten überdies die von der Öffnungsklausel geforderten angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person.

Für die in der Praxis häufig angewendete Regelung sollten der Anwendungsbereich und die spezifischen Maßnahmen konkretisiert werden.

Auch der Standort der Regelung werde für verfehlt gehalten, da sie über den Regelungsgehalt in Absatz 1 weit hinausgehe. Eine Zweckänderung, wie in der Gesetzesbegründung angeführt, könne sie auf keinen Fall rechtfertigen.

Position der Landesregierung:

Die Kritik des LfDI wird als nachvollziehbar angesehen. Laut Gesetzesbegründung ergibt sich die Pflicht zu spezifischen Maßnahmen aus § 3 LDSG. Wie bereits festgestellt, bedarf es insbesondere für die Verarbeitung besonderer Kategorien personenbezogener Daten der Regelung spezifischer Maßnahmen im jeweiligen Kontext. Im Zusammenhang mit einer Neuregelung des § 3 LDSG sollten daher auch die spezifischen Maßnahmen des § 17 Absatz 2 LDSG näher bestimmt und ggf. die Vorschrift in eine eigenständige Regelung überführt werden.

15. Videoüberwachung öffentlich zugänglicher Räume (§ 18 LDSG)

a) Zum Norminhalt

Die Videoüberwachung öffentlich zugänglicher Räume wird als besonders eingriffsintensive Form der Datenverarbeitung gesondert geregelt. Die Regelung wird in Bezug auf die Videoüberwachung der Kommunen nach Auffassung der Landesregierung nicht durch die speziellen Regelungen im § 44 PolG zur Videoüberwachung von Kriminalitätsschwerpunkten für Ortspolizeibehörden verdrängt. Die Regelung des PolG dient der Gefahrenabwehr und ist den

Polizeibehörden vorbehalten. Sie wurde im Rechtsregime der Richtlinie (EU) 2016/680 erlassen, während die Regelungen des LDSG, hier § 18, den Rechtskreis der DSGVO regeln[94]. Der in § 2 Absatz 3 LDSG geregelte Vorrang bezieht sich daher nicht auf Regelungen des Polizeigesetzes. Ggf. sollte dies gesetzlich klargestellt werden.

Die Vorschriften haben zu beachten, dass Videoüberwachung überwiegend Personen erfasst, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Dies stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen dar und bedarf daher zum einen besonderer Rechtfertigung, zum anderen besonderer Verfahrensvorschriften zur Speicherung und Löschung der aufgezeichneten Daten.

b) Rückmeldungen und Bewertung:

aa) Zu § 18 Absatz 1 LDSG

Tatbestandsvoraussetzungen der Videoüberwachung

(1) Erforderlichkeit im engeren Sinn: kein milderes Mittel

Der Polizei ist es ein Anliegen, die Tatbestandsvoraussetzungen für die Zulässigkeit von Videoüberwachung dergestalt anzupassen, dass optisch-elektronische Überwachungssysteme generell als gleichwertig zu anderen Überwachungsmitteln zugelassen werden. Da die Videoüberwachungsmaßnahme zur Erfüllung öffentlicher Aufgaben oder zur Ausübung des Hausrechts erforderlich sein müsse, müsste in der Praxis stets milderen Maßnahmen der Vorzug gegeben werden, selbst wenn diese nicht praktikabel seien, z. B., weil sie einen hohen Personaleinsatz oder technisch aufwendige Lösungen benötigten. Daher sei es geboten, die Vorschrift aufzulockern, das heißt die Voraussetzungen zu senken oder zumindest einen Ausnahmetatbestand für die Videoüberwachung von Eingangsbereichen von Dienstgebäuden zu schaffen.

- Stellungnahme des LfDI (S. 51f.):

Für den LfDI steht die Voraussetzung der Erforderlichkeit nicht zur Disposition. Sie sei verfassungsrechtlich bindend. Pauschal könne die Erforderlichkeit nicht festgestellt werden. Auch der Gesetzgeber besitze keine Berechtigung für eine solche Regelung, da weder ein

[94] Vgl. VGH München, Urteil v. 30.05.2023 – 5 BV 20.2104, Leitsatz 1: Die Videoüberwachung einer kommunalen Einrichtung gemäß Art. 24 Abs. 1 BayDSG ist keine Maßnahme zur Strafverfolgung oder zur Gefahrenabwehr im Sinne von Art. 2 Abs. 2 Buchst. d DSGVO. Die Datenschutz-Richtlinie für Justiz und Inneres (RL EU 2016/680 – sog. JI-Richtlinie) ist dafür nicht einschlägig. (Rn. 24).

überwiegendes Allgemeininteresse erkennbar noch die Verhältnismäßigkeit gewahrt seien. In Eingangsbereichen seien auch die Rechte von Beschäftigten zu beachten.

Position der Landesregierung:

Entscheidend für die Zulässigkeit einer Videoüberwachung ist nach den Grundsätzen der DSGVO das Tatbestandsmerkmal der Erforderlichkeit für den angestrebten Zweck, wie in § 18 Absatz 1 LDSG normiert. Im Sinne der Verhältnismäßigkeit ist dies so zu definieren, dass kein gleich geeignetes, aber für die betroffene Person milderes Mittel vorhanden ist, um den Zweck zu erreichen. Vor allem im Verhältnis des Bürgers zum Staat beansprucht der Verhältnismäßigkeitsgrundsatz Geltung.

Damit obliegt jeder öffentlichen Stelle, die Videoüberwachung als Mittel der Gefahrenabwehr einsetzen will, die Prüfung, ob der Einsatz anderer Mittel vorrangig ist. Hinsichtlich der technischen Ausgestaltung der Videoüberwachungsmaßnahme sind als relevante Gesichtspunkte zur Bestimmung möglicher milderer Maßnahmen etwa die Anlassbezogenheit und Streubreite der Maßnahme, der Einsatz datenvermeidender bzw. datensparsamer Technologien wie Black-Boxes und kleiner Speichermedien, die Integration von eingeschränkten Zugriffsmanagementsystemen, Verschlüsselungsmechanismen und sonstigen IT-sicherheitsrechtlichen Vorkehrungen anzuführen[95].

Die Anwesenheit eines Amtsträgers kann im Vergleich zur laufend eingesetzten Videoüberwachung ebenfalls der mildere Eingriff sein. Datenschutzfreundlicher ist dies insofern, als ein Amtsträger personenbezogene Daten zwar erfassen, aber nicht in gleichem Umfang speichern und auswerten kann wie die Videoüberwachungstechnik[96].

Teilweise wird in der Kommentarliteratur die Auffassung vertreten, dass in die Prüfung der Erforderlichkeit auch die objektive und wirtschaftliche Zumutbarkeit des milderen Mittels für die verantwortliche Stelle eingestellt werden kann[97]. Ist diese zu bejahen, würde die Erforderlichkeit der Videoüberwachung entfallen.

Diskutiert werden kann, ob der Gesetzgeber die Frage der Erforderlichkeit wie geschehen auf den Einzelfall bezogen regeln muss, so dass der Verantwortliche jeweils die Prüfung der Erforderlichkeit vornehmen muss. Die Alternative wäre, dass der Gesetzgeber selbst abstrakt-

[95] Vgl. Starnecker in Gola/Heckmann, BDSG § 4 Rn. 46.
[96] Vgl. Frenzel in Paal/Pauly BDSG § 4 Rn. 18.
[97] Vgl. Starnecker in Gola/Heckmann, BDSG § 4 Rn. 44; Buchner in Kühling/Buchner, BDSG § 4 Rn. 8; einschränkend dahingehend, dass höhere Kosten allein nicht ausschlaggebend sein können BeckOK DatenschutzR/Wilhelm-Robertson BDSG § 4 Rn. 31, 32.

generell die Vorrangprüfung der verschiedenen Mittel vornimmt mit dem möglichen Ergebnis, dass im Hinblick auf ihre Verhältnismäßigkeit der Videoüberwachung neben anderen Überwachungsmaßnahmen unter Beachtung der Datenschutzgrundsätze und dem Schutz der betroffenen Personen durch technische Maßnahmen Gleichwertigkeit zuzumessen sein kann. An der Erforderlichkeit in Bezug auf die Schutzbedürftigkeit als Tatbestandsmerkmal, das heißt der Prüfung des „Ob" der Videoüberwachung würde sich dadurch nichts ändern. Eine derartige gesetzliche Regelung wird in der Kommentarliteratur mit dem Hinweis darauf, dass sich der parlamentarische Gesetzgeber, der demokratisch unmittelbar legitimiert ist, nicht in gleicher Weise für eine abstrakt-generelle Regelung rechtfertigen wie sich eine Behörde für eine Maßnahme im Einzelfall rechtfertigen muss, angedacht[98].

Es sind nach Auffassung der Landesregierung durchaus Fallgruppen denkbar, in denen, sofern eine Gefahrenlage besteht, keine vernünftige Alternative zur Videoüberwachung besteht und diese daher vom Gesetzgeber für diese Anwendungsfälle generell zugelassen werden könnte. Dies könnte als gesetzliche Vermutung der Erforderlichkeit einer Videoüberwachung als geeignetes Mittel geregelt werden. Zu denken ist z. B. an unverhältnismäßigen Aufwand, den andere Maßnahmen erfordern würden oder an Fälle, bei denen andere Maßnahmen von vornherein als nicht gleichermaßen geeignet anzusehen sind. Die Eingangsbereiche von sicherheitsrelevanten Dienstgebäuden oder Museen sind hier z. B. zu nennen, evtl. auch die Videoüberwachung in Verkehrsmitteln. Der besonderen Schutzbedürftigkeit von Beschäftigten müsste durch technisch-organisatorische Maßnahmen Rechnung getragen werden. Außerdem dürfen selbstverständlich keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.

(2) Videoüberwachung zur Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten

Den kommunalen Landesverbänden sind die Tatbestandsvoraussetzungen zu eng gefasst. Zum einen sei die Beschränkung auf den „Einzelfall" missverständlich. Es bestehe Klarheit darüber, dass keine anlasslose, rein präventive Videoüberwachung der gesamten Gemeinde zulässig sei. Zum anderen wird als weitere zulässige Zweckbestimmung die Verhinderung von Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung unabhängig von den in Absatz 1 Nummer 1 und 2 genannten Rechtsgütern vermisst. Dies sei nach der Vorgängerregelung des § 20a LDSG a. F. zulässig gewesen. Überwiegend sei die Verhinderung von Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung jedoch die Ursache für den Wunsch einer Videoüberwachung im kommunalen Raum. Die Regelung in § 18 LDSG erschwere zum einen die Begründung, zum anderen beschränke sie die Videoüberwachung auf

[98] Vgl. Frenzel in Paal/Pauly BDSG § 4 Rn. 19.

den Schutz vor Straftaten und Ordnungswidrigkeiten gegen die in Absatz 1 Nummer 1 genannten Rechtsgüter und die in Absatz 1 Nummer 2 genannten baulichen Anlagen und Sachen. Die kommunalen Landesverbände schlagen daher eine entsprechende Ergänzung des Absatz 1 um folgende Nummer 3 vor: „3. um die Begehung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung zu verhindern oder deren Verfolgung zu ermöglichen“.

- Bewertung des LfDI (S. 52 bis 54):

Der LfDI sieht die Begrifflichkeit des „Einzelfalls“ als Hilfestellung für die Anwender der Norm, indem er verdeutliche, dass eine konkrete Prüfung bezogen auf das jeweilige Überwachungsobjekt vorzunehmen sei.

Auch der Vorschlag der Erweiterung der Tatbestandsvoraussetzungen stößt beim LfDI auf Ablehnung. Dies sei auch nach der alten Fassung des LDSG nicht gerechtfertigt gewesen. Diese sei sogar noch strenger gewesen. In Bezug auf Videoüberwachung zur Strafverfolgung sei § 44 Absatz 3 PolG einschlägig, der nicht ausgehöhlt werden dürfe. Aufgrund bereits ausufernder gemeindlicher Videoüberwachung sollte die derzeitige Regelung beibehalten werden.

Position der Landesregierung:

Wie die kommunalen Landesverbände richtig anmerken, will die Formulierung „im Einzelfall“ zum Ausdruck bringen, dass keine anlasslose, rein präventive Videoüberwachung möglich ist. Ob die Videoüberwachung zulässig ist, kann nur bezogen auf den überwachten Ort und die beabsichtigte Zeitdauer beurteilt werden. Die Formulierung verdeutlicht dies und sollte daher beibehalten werden.

Entsprechend dem Grundsatz der Zweckbindung darf Videoüberwachung nur für bestimmte Zwecke eingesetzt werden. Die Regelung des § 18 LDSG stellt ebenso wie die Vorgängerfassung des § 20a LDSG a. F. auf den Schutz bestimmter hochwertiger Rechtsgüter ab, da deren Schutz in besonderer Weise einen Eingriff in das informationelle Selbstbestimmungsrecht rechtfertigt. Dagegen würde eine generelle Ermächtigung des Einsatzes der Videoüberwachung zur Verhinderung und Verfolgung von Straftaten und Ordnungswidrigkeiten losgelöst vom Schutz bestimmter Rechtsgüter zu weitreichende Eingriffsrechte mit sich bringen. Eine konkrete Aufgabe in Bezug auf ein bestimmtes Rechtsgut muss den Einsatz von Videoüberwachung rechtfertigen. Die Zuständigkeitsabgrenzung zu den Aufgaben der Polizei zur Gefahrenabwehr und Strafverfolgung ist zu beachten. Polizeiliche Aufgaben unterliegen einem anderen datenschutzrechtlichen Regime, nämlich dem der Datenschutzrichtlinie (EU)

680/2016 (JI-Richtlinie) und erlauben ebenfalls nur in begrenztem Umfang Videoüberwachung. Gemäß § 44 Absatz 3 des Polizeigesetzes, das der Umsetzung der JI-Richtlinie dient, können die Ortspolizeibehörden an öffentlich zugänglichen Orten Bild- und Tonaufzeichnungen von Personen anfertigen, wenn sich die Kriminalitätsbelastung dort von der des übrigen Gemeindegebiets deutlich abhebt und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist. Damit ist die Videoüberwachung zu polizeilichen Zwecken auf Fälle starker Kriminalitätsbelastung beschränkt.

(3) Videoüberwachung in nicht öffentlich zugänglichen Bereichen

Seitens der Wissenschaft wird ein Bedürfnis für Videoüberwachung auch in nicht öffentlich zugänglichen Bereichen, wie sie gerade im Universitätskontext, aber auch im Großforschungsbereich bestehen (z. B. aufgrund atomrechtlicher Zugangsbeschränkungen), gesehen. Eine Heranziehung von § 15 Absatz 1 LDSG als Rechtsgrundlage sei nicht zielführend, da sich in den betreffenden Bereich auch zulässigerweise Dienstleister oder Studierende aufhalten können.

Ebenso plädiert die Vermögens- und Hochbauverwaltung des Landes für eine ausdrückliche Regelung im LDSG zur Videoüberwachung von nicht öffentlich zugänglichen Räumen, um an Baustellen Diebstahl und betrügerischer Abrechnung von Zusatzarbeit vorzubeugen. Hierbei sollten auch konkrete Vorgaben zur Speicherdauer u. ä. getroffen werden.

- Bewertung des LfDI (S. 47 bis 51):

Der LfDI weist darauf hin, dass die Rechtslage umstritten sei. Während manche von einer geringeren Eingriffsintensität ausgingen, bestehe aus seiner Sicht in diesen Bereichen ein erhöhter Schutzbedarf im Vergleich zu öffentlich zugänglichen Räumen. Denn in letzteren müsse ohnehin jeder mit Beobachtung rechnen. Mithin sollte sich eine etwa zu schaffende Rechtsgrundlage für die Videobeobachtung auf enge Anwendungsfälle beschränken, quasi nur als Ultima Ratio, vergleichbar den Anforderungen an die Aufklärung von Straftaten durch Beschäftigte, und unter Beachtung des höheren Schutzbedarfs, in Betracht kommen.

Position der Landesregierung:

Die Videoüberwachung ist im LDSG für öffentlich zugängliche Räume geregelt und berücksichtigt die an diesen Orten bestehende Gefährdungslage für den Schutz von Personen und Objekten auf der einen Seite und das Recht auf informationelle Selbstbestimmung auf der anderen Seite, die gegeneinander abzuwägen sind. Die Videoüberwachung im öffentlichen

Raum erfasst, wie bereits ausgeführt, überwiegend unbekannte Personen, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff in ihr informationelles Selbstbestimmungsrecht durch ihr Verhalten nicht veranlasst haben. Dem ist bei der Anwendung des § 18 LDSG Rechnung zu tragen.

Dagegen sind bei der Videoüberwachung in nicht öffentlich zugänglichen Räumen, beispielsweise am Arbeitsplatz (z. B. auf Baustellen) oder im Universitätskontext, je nach den Gegebenheiten weitere Gesichtspunkte in die Interessenabwägung einzustellen. Insbesondere der Beschäftigtendatenschutz verlangt besondere Vorkehrungen. Dies gilt auch, wenn in die Videoüberwachung Dritte wie Dienstleister oder Studierende einbezogen werden sollen, da diese jederzeit identifizierbar sind. Auf der anderen Seite ist gegebenenfalls die besondere Schutzbedürftigkeit bestimmter Anlagen, z. B. im Hochschulbereich, einzubeziehen.

Die Vorschrift des § 18 LDSG ist nicht für diese Anwendungsfälle konzipiert. Aus den genannten Gründen wird es nicht als zulässig angesehen, in Absatz 1 die Beschränkung auf öffentlich zugängliche Räume aufzuheben.

Nach der geltenden Rechtslage kommen folgende Rechtsgrundlagen für eine Videoüberwachung außerhalb des Anwendungsbereichs von § 18 LDSG in Betracht:

- Sofern öffentliche Stellen zum Schutz ihrer Baustelleneinrichtung oder sonstigen Einrichtung Videoüberwachung benötigen, kann dies im Rahmen der Ausübung des Hausrechts auf § 4 LDSG gestützt werden, sofern Beschäftigte nicht erfasst werden, z. B. für die Überwachung außerhalb der Betriebszeiten.

- Die Videoüberwachung von Beschäftigten beurteilt sich nicht nach § 18 LDSG, sondern nach § 15 LDSG. In § 15 Absatz 7 LDSG wird die Überwachung Beschäftigter mittels optisch-elektronischer Einrichtungen zum Zweck der Verhaltens- und Leistungskontrolle ausdrücklich verboten. Ausnahmen bestehen nur bei dem Verdacht auf eine Straftat oder eine schwere Pflichtverletzung gemäß § 15 Absatz 5 LDSG, wobei ein Anfangsverdacht genügt.[99].

- Wenn wie im Fall von sensiblen Forschungseinrichtungen hinzukommt, dass neben Beschäftigten auch noch Dritte betroffen sein können, empfiehlt sich eine spezialgesetzliche Regelung, die die spezifische Situation berücksichtigen kann und entsprechende technische und organisatorische Maßnahmen vorgeben sollte. Wie eine solche Regelung aussehen könnte, zeigt beispielhaft § 32 des Landesglücksspielgesetzes.

[99] Vgl. Maschmann in Kühling/Buchner, BDSG § 26 Rn. 45 mit Verweis auf die Rechtsprechung des Bundesarbeitsgerichts.

Eine eigenständige Vorschrift zur Videoüberwachung in nicht öffentlich zugänglichen Räumen könnte, sofern nicht Spezialregelungen erforderlich sind, die Voraussetzungen klarstellend regeln, insbesondere in Bezug auf den Schutz Beschäftigter und wird daher befürwortet.

(4) Sonderfall: Videoüberwachung zum Einsatz von KI

Es entstehen vermehrt KI-Einsatzgebiete, welche die Überwachung bzw. Aufzeichnung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die, häufig nicht bezweckte, Verarbeitung der dadurch erhobenen personenbezogenen Daten bedingen. Zu nennen sind hier exemplarisch Methoden des autonomen Fahrens, der Bauwirtschaft oder der Pflege und Wartung öffentlicher Einrichtungen und Infrastruktur.

Für deren Einsatz könnten Konflikte mit der Regelung in § 18 Absatz 1 LDSG entstehen, in der Videoüberwachung sehr weit als „die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen“ legal definiert wird. Es sollte daher, um Rechtsunsicherheiten vorzubeugen, in einem Gesetzgebungsverfahren geprüft werden, ob diese KI-Einsatzgebiete im Kontext von § 18 Absatz 1 LDSG entweder ausdrücklich geregelt oder ausgeschlossen werden.

bb) Zu § 18 Absatz 2 LDSG

Informationspflicht

Der LfDI kritisiert zu geringe Informationspflichten in Absatz 2 der Vorschrift. Es sei nicht nachvollziehbar, weshalb für die Datenerhebung durch Videoüberwachung geringere Anforderungen an die Information der Betroffenen gemäß Artikel 13 DSGVO gestellt werden sollten als in den übrigen Fällen der Datenerhebung. Dies sollte korrigiert werden. In der Aufsichtspraxis stoße die erweiterte Information nicht auf Widerstand.

Position der Landesregierung:

Unabhängig davon, ob bereits bei der Videoüberwachung die Informationspflicht nach der DSGVO entsteht, wird die Erweiterung der Informationspflichten befürwortet. Sie ist mit geringem Aufwand machbar und erhöht die Transparenz. Insbesondere der verfolgte Zweck und die Speicherfristen sollten erkennbar sein. Die Informationspflicht kann auch durch Anbringen eines QR-Codes erfüllt werden.

Die Vorschrift des § 18 Absatz 2 LDSG sollte entsprechend ergänzt werden.

cc) Zu § 18 Absatz 4 LDSG

Informationspflicht gegenüber einer bestimmten Person

Die kommunalen Landesverbände schlagen vor, Absatz 4 komplett zu streichen oder zumindest zu überarbeiten. Die Informationspflicht ergebe sich bereits aus Artikel 14 DSGVO, sobald die Daten gespeichert werden. Vorher, also nur bei Aufzeichnungen, die sofort gelöscht würden, bestehe kein Bedarf für eine entsprechende Information, wenn die Person erkannt werde (was in kleineren Gemeinde häufig vorkomme). Dies stelle unnötigen Verwaltungsaufwand ohne Nutzen dar.

- Bewertung des LfDI (S. 54f.):

Nach Auffassung des LfDI hat die Information nach Artikel 13 DSGVO zu erfolgen, und zwar in der Regel in Form eines Hinweisschilds. Der Vorschrift komme nur klarstellende Funktion zu.

Position der Landesregierung:

Eine Streichung der Vorschrift wird als unbedenklich angesehen, da sie wegen der Regelung in Artikel 13 DSGVO selbst entbehrlich ist. In den Fällen, in denen die Aufnahme nicht gespeichert wird, genügt die Information nach Absatz 2.

dd) Zu § 18 Absatz 5 LDSG

Speicherdauer

Der LfDI bemängelt, dass die maximale Speicherdauer von vier Wochen in der Praxis häufig ausgenutzt werde, ohne dass dies sachlich erforderlich sei. Hierin sieht er den Grundsatz der Speicherbegrenzung aus Artikel 5 Absatz 1 Buchst. e DSGVO als verletzt an. Um dies zu vermeiden, schlägt er vor, die Höchstspeicherdauer von vier Wochen zu streichen. Damit würde die Pflicht zur unverzüglichen Löschung normiert werden.

Die kommunalen Landesverbände fordern dagegen die Beibehaltung der Vierwochenfrist als Höchstspeicherdauer. In der Praxis komme es häufig vor, dass Meldungen über Sachbeschädigungen nicht immer sofort erfolgen oder die Videoaufzeichnungen nicht immer unverzüglich durch die zuständigen Personen ausgewertet werden könnten. Eine Verkürzung der Speicherfrist würde daher in zahlreichen Fällen zum Schutz von Straftätern führen.

Seitens der Polizei wird bemerkt, dass die Speicherdauer in der Praxis häufig zu Auseinandersetzungen mit der Datenschutzaufsichtsbehörde führe, da in der Praxis die Vier-Wochen-Frist häufig als Höchstspeicherdauer verstanden werde. Es sei aber klar, dass die Speicherdauer sich an der Erforderlichkeit und dem Grundsatz der Speicherbegrenzung auszurichten habe. Bei richtiger Auslegung besage die Vorschrift nichts Anderes. Sie sei klar im Sinne eines Regel-Ausnahmeverhältnisses formuliert. Sollte unmittelbar nach der Datenerhebung feststehen, dass die Daten nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden, bestehe die Pflicht zur unverzüglichen Löschung. Oftmals könne diese Bewertung aber nicht unmittelbar nach der Datenerhebung getroffen werden. Im Rahmen von polizeilichen Ermittlungen könne sich dieser Bedarf auch erst einige Tage später noch ergeben. Vor diesem Hintergrund erscheine die Pflicht zur Löschung spätestens nach vier Wochen angemessen.

- Bewertung des LfDI (S. 55f.):

Der LfDI weist darauf hin, dass die Datenschutzkonferenz für nichtöffentliche Stellen eine Speicherdauer von maximal 72 Stunden für zulässig halte. Eine davon abweichende Speicherdauer sei nur in Ausnahmefällen zulässig. Für die Videoüberwachung durch öffentliche Stellen sollte nichts anderes gelten. Mit der Speicherdauer nehme auch die Intensität des Eingriffs in die Rechte der gefilmten Personen zu. § 18 Absatz 5 LDSG sollte daher gestrichen oder die Speicherdauer gesetzlich auf 72 Stunden begrenzt werden.

Position der Landesregierung:

Grundsätzlich wird der Aussage zugestimmt, dass sich die Speicherdauer an der Erforderlichkeit und dem Grundsatz der Speicherbegrenzung auszurichten hat. Zugleich können die Gemeinwohlzwecke der Gefahrenabwehr sowie der Strafverfolgung unter Beachtung des Verhältnismäßigkeitsprinzips die Einführung einer Höchstspeicherfrist rechtfertigen.

Mit der Speicherbegrenzung wird die Zweckbindung zum zentralen Anknüpfungspunkt für die Speicherungsdauer. Personenbezogene Daten dürfen nicht länger gespeichert werden, als dies für die Zwecke ihrer Verarbeitung erforderlich ist. Danach sind sie gemäß Artikel 17 DSGVO unverzüglich zu löschen. Der Zweck der Videoüberwachung im öffentlichen Raum besteht, sofern es sich nicht um die Wahrnehmung des Hausrechts handelt, in der Schadensprävention für öffentliche Sachgüter oder im Schutz von Leben und Gesundheit der sich dort befindlichen Personen. Sobald diese Gefahr nicht mehr besteht, hat der Verantwortliche daher die Daten grundsätzlich zu löschen.

Zum anderen ist das Land aber dem Gemeinwohl verpflichtet, das zur Erfüllung der staatlichen Schutzpflicht verlangt, Straftaten zulasten der Bürger zu verhindern und aufzuklären.

115

Daher hat das Land von der Ermächtigung in Artikel 23 DSGVO, die Zweckbindung aus übergeordneten Gründen des öffentlichen Wohls einzuschränken, Gebrauch gemacht. Es ist nämlich vorgesehen, dass die Videoüberwachungsdaten zur Verfolgung von Straftaten und erheblichen Ordnungswidrigkeiten genutzt werden können. Folgerichtig muss den zuständigen Stellen ein gewisser zeitlicher Spielraum zur Auswertung der Videodaten zugestanden werden. Sofern die Daten nicht länger als für die Abwehr und Aufklärung von Straftaten nötig, gespeichert werden, wird der DSGVO Genüge getan. Schließlich kann auch die Löschverpflichtung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, entsprechend Artikel 17 Absatz 3 Buchst. b DSGVO zulässig eingeschränkt werden.

Der Gesetzgeber hat sich für eine Höchstspeicherdauer von vier Wochen entschieden. Damit hat er in zulässiger Weise von dem verfassungsrechtlich eingeräumten Spielraum Gebrauch gemacht. Die Regelung sollte beibehalten werden. Dies wird wie folgt begründet.

Gesetzliche Speicherfristen sind daran zu messen, ob sie in Abwägung mit dem Grundrecht auf Datenschutz als verhältnismäßige Einschränkung gemäß Artikel 52 Absatz 1 GRCh betrachtet werden können. Die Auswertungen der Videodaten sind, sofern es zu einem Schaden gekommen ist, komplex und setzen daher eine gewisse Speicherdauer voraus. Gesetzliche Festlegungen von Höchstspeicherfristen geben hier den Verantwortlichen die erforderlichen Spielräume und sind dadurch gerechtfertigt, dass die Speicherung der Videodaten dem legitimen und bestimmten Zweck der Abwehr und Aufklärung von Straftaten im Interesse der Allgemeinheit dient. Bestimmte Vorkehrungen in Bezug auf Datensicherheit, Datenverwendung und Transparenz (s.o.) können und sollten den Eingriff ggf. minimieren. Andererseits bedarf es auch der Festlegung einer Höchstspeicherdauer. Denn es entspricht der ständigen Rechtsprechung des Bundesverfassungsgerichts, dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich untersagt ist[100].

Die Schwere des Eingriffs wird außerdem dadurch relativiert, dass Videodaten nicht von vornherein einer bestimmten Person zuordenbar sind und nur punktuell an Orten stattfindet, die öffentlich zugänglich sind.

Unter den genannten Voraussetzungen kann die Ausnutzung der Höchstspeicherfrist zur Abwehr von Gefahren für die öffentliche Sicherheit und Aufklärung von Straftaten und Ordnungswidrigkeiten verhältnismäßig sein. Dies sollte aber nicht der Regelfall sein.

[100] Vgl. BVerfGE 65, 1 <46>; 100, 313 <360>; 115, 320 <350>; 118, 168 <187>.

Soweit KI-Systeme außerhalb des Bereichs des Polizei- und Ordnungsrechts künftig umfasst sein sollen, wäre hierfür gegebenenfalls eine gesonderte Speicherdauer festzulegen, da die Dauer von vier Wochen gegebenenfalls zu kurz bemessen sein könnte, um geeignete KI-Systeme in diesem Zeitraum zu trainieren.

16. Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken (§ 19 LDSG)

a) Zum Norminhalt

Mit § 19 LDSG wird von der Spezifizierungsklausel des Artikels 85 Absatz 2 DSGVO Gebrauch gemacht. Die Vorschrift regelt ergänzend zu den Vorschriften im Pressegesetz und im Medienstaatsvertrag für die Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken die eingeschränkte Geltung der Vorschriften der DSGVO. Damit soll ein umfassender Grundrechtsschutz der Kunst- und Meinungsfreiheit auch im öffentlichen Bereich (z. B. für öffentlich-rechtlich organisierte Theaterbetriebe) gewährleistet werden. Die datenschutzrechtliche Kontrolle in Bezug auf die geltenden Vorschriften wird durch den LfDI ausgeübt.

b) Rückmeldungen und Bewertung

Verhältnis zu KunstUrhG

Der LfDI hält eine Überprüfung der Vereinbarkeit mit dem Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) für erforderlich. Die in § 19 LDSG getroffenen Einschränkungen müssten daraufhin untersucht werden, ob sie mit dem nach mehreren Urteilen weiterhin geltenden KunstUrhG vereinbar seien.

- Bewertung des LfDI (S.56):

Der LfDI hält an seinen Ausführungen fest.

Position der Landesregierung:

Das KunstUrhG schützt das Recht am eigenen Bild, eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts. Aus diesem folgt, dass grundsätzlich allein dem Abgebildeten die Befugnis zusteht, darüber zu befinden, ob und in welcher Weise sein Bild der Öffentlichkeit zugänglich gemacht wird. Bildnisse einer Person dürfen nach § 22 KunstUrhG daher in der

Regel nur mit deren Einwilligung verbreitet werden. § 23 KunstUrhG regelt die Fallgestaltungen, in denen ohne Einwilligung Bildnisse verbreitet werden dürfen. Dies betrifft

- Bildnisse aus dem Bereich der Zeitgeschichte,
- Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen,
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben,
- Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

Längere Zeit war streitig, ob die DSGVO die Vorschriften des KunstUrhG verdrängt. Inzwischen hat der BGH entschieden, dass § 22 und § 23 KunstUrhG im Hinblick auf die Beurteilung der Zulässigkeit von Bildveröffentlichungen im journalistischen Bereich als die Öffnungsklausel des Artikels 85 DSGVO ausfüllende Gesetze anzusehen sind[101]. Falls der Bundesgesetzgeber eine andere Beurteilung bevorzugen würde, müsste er eine gesetzliche Klarstellung einfügen.

Es ist nicht ersichtlich, dass an die Verarbeitung von Bildnissen zu künstlerischen und literarischen Zwecken andere Maßstäbe als an die Verarbeitung im journalistischen Bereich anzulegen wären, vor allem da es sich um die Verarbeitung von Bildnissen durch öffentliche Stellen geht.

Wenn man mit der Rechtsprechung davon ausgeht, dass §§ 22 bis 24 KunstUrhG weiter anwendbar sind, ergibt sich in Bezug auf die Darstellung von Bildnissen eine einschränkende Geltung des § 19 LDSG. Eine weitere Klarstellung ist nicht erforderlich, da sich der Vorrang des KunstUrhG bereits aus § 2 Absatz 3 LDSG ergibt.

17. Aufgaben und Befugnisse (§ 25 LDSG)

a) Zum Norminhalt

§ 25 LDSG regelt ergänzend zur DSGVO die Aufgaben und Befugnisse des LfDI als Aufsichtsbehörde gegenüber öffentlichen Stellen. Des Weiteren wird ihm die Aufgabe der Aufsichtsbehörde für nichtöffentliche Stellen zugewiesen.

Absatz 4 enthält Verfahrensvorschriften zur Ausübung der Aufsichtsbefugnisse des LfDI bei öffentlichen Stellen.

[101] BGH, Urteil v. 07.07.2020, Az. VI ZR 250/19, NJW 2020, S. 3715, Rn. 11.

Mit der Regelung des § 25 Absatz 5 LDSG wird die Vorschrift des § 29 Absatz 3 BDSG, die alle nichtöffentlichen Stellen, u. a. Rechtsanwältinnen und Rechtsanwälte, die einer Geheimhaltungsvorschrift unterliegen, von der Kontrolle der Aufsichtsbehörden befreit, auf die Notarinnen und Notare erstreckt, die in Baden-Württemberg als öffentliche Stellen organisiert sind.

b) Rückmeldungen und Bewertung

aa) Zu § 25 Absatz 1 LDSG

Zusammenarbeit mit anderen Aufsichtsbehörden

Das Staatsministerium hat im Rahmen der Evaluation den Südwestrundfunk beteiligt. Aufgrund der Rückmeldung des Südwestrundfunks wird angeregt, folgende Ergänzung des § 25 Absatz 1 LDSG zu prüfen:

„Der Landesbeauftragte für den Datenschutz arbeitet mit anderen Aufsichtsbehörden, auch durch Informationsaustausch, zusammen und leistet ihnen Amtshilfe, um die einheitliche Anwendung der Vorschriften über den Datenschutz zu gewährleisten."

- Bewertung des LfDI (S. 57):

Der LfDI lehnt den Vorschlag ab. Eine Pflicht zur Amtshilfe würde zum einen gegen bestehendes Verfahrensrecht verstoßen, wenn die Hilfeleistung in Handlungen besteht, die der ersuchten Behörde als eigene Aufgabe obliegen. Des Weiteren sieht der LfDI durch eine solche Regelung seine Unabhängigkeit beeinträchtigt, weshalb er sie strikt ablehnt.

Position der Landesregierung:

Es wird keine Notwendigkeit für die vorgeschlagene Regelung gesehen.

bb) Zu § 25 Absatz 4 LDSG

Verfahrensvorschriften

Der LfDI hält die Vorschrift des Absatz 4 für europarechtswidrig, weshalb er sie nicht als für sich bindend ansieht. Die Maßnahmenbefugnisse der Aufsichtsbehörde seien abschließend in Artikel 58 DSGVO geregelt. Die Verpflichtung, vor Durchführung von Maßnahmen eine Stellungnahme einzuholen, hindere den effektiven Schutz der Betroffenen vor fortdauernden

Grundrechtsbeeinträchtigungen, da dieses Verfahren einige Zeit in Anspruch nehme. Im kommunalen Bereich sei die Unterrichtung auch in der Regel überflüssig, da der Bürgermeister die Korrespondenz mit der Aufsichtsbehörde kenne.

- Bewertung des LfDI (S. 58):

Der LfDI empfiehlt die Streichung des § 25 Absatz 4 LDSG. Es solle aber festgehalten werden, dass der LfDI sich bei Bedarf an die Dienst- und Fachaufsichtsbehörde wenden könne. Unabhängig hiervon sollte in § 25 Absatz 4 LDSG auch der Verstoß gegen die Unterstützungspflicht gemäß § 26 LDSG aufgenommen werden.

Position der Landesregierung:

Artikel 58 Absatz 4 DSGVO sieht für die Ausübung der Befugnisse der Aufsichtsbehörde geeignete Verfahrensgarantien vor. Ergänzende verfahrensrechtliche Anforderungen nach dem nationalen Recht sollen, wie sich aus Erwägungsgrund 129 Satz 8 ergibt, nicht ausgeschlossen sein.

Durch die Mitteilung wird insbesondere gewährleistet, dass die zuständige Rechts- oder Fachaufsichtsbehörde Kenntnis von dem Verstoß erhält und vor der Ausübung weiterer Befugnisse durch den LfDI rechtliches Gehör und Gelegenheit erhält, diesem eine etwaige gegenteilige Rechtsauffassung mitzuteilen oder ihrerseits die betroffene Behörde zur Abhilfe aufzufordern. Die Gefahr divergierender Anweisungen zwischen Datenschutzaufsicht und Rechts- oder Fachaufsicht wird hierdurch reduziert. Widersprüchliche Auffassungen der Datenschutzaufsicht und der Rechts- oder Fachaufsicht wären ansonsten letztlich auf dem Gerichtsweg zu klären. Widerspricht die Verfügung des LfDI der Rechtsauffassung der Rechts- oder Fachaufsichtsbehörde, kann diese den Verantwortlichen zur gerichtlichen Klärung anweisen[102]. Auch in der Kommentarliteratur werden keine Bedenken gegen die entsprechende Bundesregelung in § 16 Absatz 1 BDSG vorgebracht[103].

In der Kommentarliteratur ist unter Verweis auf Artikel 4 Absatz 3 des Vertrags über die Europäische Union in der Fassung des Vertrags von Lissabon anerkannt, dass der übergeordnete Äquivalenz- und Effizienzgrundsatz bei der Ausgestaltung des nationalen Verfahrensrechts zu beachten ist[104].

Die Argumentation des LfDI, der effektive Schutz Betroffener werde gehindert, da regelmäßig geraume Zeit vergehe, bis es gegebenenfalls zu einer Löschungsanordnung oder einem

[102] Vgl. LT-Drs. 16/3930, S. 114.
[103] Vgl. BeckOK DatenschutzR/Meltzian BDSG § 16 Rn. 1-5; Bange in Kühling/Buchner, BDSG § 16 Rn. 6 f.
[104] Vgl. Selmayr in Ehmann/Selmayr, Artikel 58 Rn. 5.

sonstigen Verarbeitungsverbot komme, erscheint mit Blick auf die in § 25 Absatz 4 Satz 3 LDSG geregelten Ausnahmen, die in Eilfällen auch ein sofortiges Tätigwerden ermöglichen, aber nicht überzeugend.

Auch aus kommunalrechtlicher Sicht sollte an § 25 Absatz 4 LDSG festgehalten werden. Es erscheint angemessen, dass bei kommunaler Betroffenheit das vertretungsberechtigte Organ unmittelbar eingebunden wird. Der LfDI schreibt in seiner Stellungnahme selbst, dass der Bürgermeister „regelmäßig“ die Korrespondenz mit der Aufsichtsbehörde kennen wird und bringt damit zum Ausdruck, dass dies nicht immer der Fall ist. Die darüber hinaus erfolgende Einbindung der zuständigen Aufsichtsbehörde entspricht dem Verwaltungsaufbau.

Ein Verstoß gegen § 26 LDSG dürfte bereits von § 25 Absatz 4 Satz 1 LDSG erfasst sein, da Verstöße gegen die Vorschriften des LDSG explizit erwähnt werden.

cc) Zu § 25 Absatz 5 LDSG

Aufsicht gegenüber Notarinnen und Notaren

Der LfDI hält die Beschränkung der Aufsichtsbefugnisse gegenüber Notarinnen und Notaren für europarechtswidrig. Sie sei wegen des Vorrangs der DSGVO nicht anwendbar und sollte daher gestrichen werden.

- Bewertung des LfDI (S. 58f.):

Der LfDI hält an seiner Bewertung fest. Die Verweisung auf § 29 Absatz 3 BDSG und die dort genannte Einschränkung nur einzelner Befugnisse werde in der Praxis nicht verstanden. Angeregt wird die Streichung oder eine Klarstellung durch eine eigenständige, von § 29 Absatz 3 BDSG unabhängige Normierung.

Position der Landesregierung:

Die Beschränkung der Aufsichtsbefugnisse gegenüber Notarinnen und Notaren wird von Artikel 90 Absatz 1 DSGVO gestattet, der eine Einschränkung der Untersuchungsbefugnisse der Aufsichtsbehörde zulässt, „soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen.“ Auch Notarinnen und Notare unterliegen einer Verschwiegenheitspflicht (§ 18 BNotO) und werden im Übrigen auch von § 203 Absatz 1 Nummer 3 StGB ausdrücklich erfasst.

121

Der in Bezug genommene § 29 Absatz 3 BDSG wird in der Kommentarliteratur unterschiedlich bewertet. Während teilweise eine vollständige Unterwerfung auch von Berufsgeheimnisträgern unter die Datenschutzaufsicht gefordert wird, wird die Regelung von anderen als verhältnismäßig und den Anforderungen des Artikels 90 Absatz 1 DSGVO genügend beurteilt[105]. Letzteres wird überzeugend damit begründet, dass die Aufsichtsbefugnisse nur eingeschränkt, aber nicht ausgeschlossen sind und damit den besonderen Geheimhaltungspflichten der Berufsgeheimnisträger Rechnung getragen wird. Zudem ist auf die Rechtsprechung des Bundesverfassungsgerichts zu verweisen, die den Schutz von Berufsgeheimnissen vor dem Zugriff von staatlichen Institutionen für verfassungsrechtlich geboten hält.[106]

Eine Ungleichbehandlung im Sinne einer Schlechterstellung der öffentlich-rechtlich bestellten Notarinnen und Notare mit den selbständigen Anwältinnen und Anwälten wird als nicht gerechtfertigt angesehen. Über eine eigenständige Normierung im LDSG (anstelle der Verweisung in § 25 Absatz 5 Satz 1 LDSG auf § 29 Absatz 3 BDSG) kann nachgedacht werden.

18. Pflicht zur Unterstützung (§ 26 LDSG)

a) Zum Norminhalt

Den öffentlichen Stellen wird die Pflicht auferlegt, den LfDI bei der Erfüllung seiner Aufgaben zu unterstützen. Zu diesem Zweck ist dem LfDI unter anderem jederzeit Zutritt zu den Diensträumen zu gewähren.

b) Rückmeldungen und Bewertung

Zutrittsrecht des LfDI in Wohnungen

Die kommunalen Landesverbände weisen im Zusammenhang mit dem verstärkten mobilen Arbeiten bzw. dem Arbeiten im Homeoffice darauf hin, dass in Bezug auf das Zutrittsrecht gemäß § 26 Absatz 1 Nummer 2 LDSG zusätzlich das Grundrecht auf die Unverletzlichkeit der Wohnung gemäß Artikel 13 des Grundgesetzes zu beachten sei. Für den Zutritt des LfDI in Wohnungen zur Ausübung seiner Untersuchungsbefugnisse wird ggf. eine gesetzliche Grundlage für erforderlich gehalten.

[105] Vgl. BeckOK DatenschutzR/Uwer DS-GVO Artikel 90 Rn. 16-19; Gräber/Nolden, in: Paal/Pauly, § 29 BDSG Rn. 18-21.
[106] Vgl. BVerfGE 113, 29.

- Bewertung des LfDI (S. 59):

Die Zugangsrechte des LfDI, die gegenüber den datenschutzrechtlich Verantwortlichen bestehen, könnten sich gemäß Artikel 58 Absatz 1 Buchst. f grundsätzlich auch auf geschäftlich genutzte Räume in Privatwohnungen erstrecken. Der LfDI geht davon aus, dass diese Fallkonstellation keine praktische Anwendung findet.

Position der Landesregierung:

Das LDSG verpflichtet die öffentlichen Stellen als Verantwortliche, der Datenschutzaufsicht in den „Diensträumen einschließlich aller Datenverarbeitungsanlagen und -geräte“ für den Zweck der Datenschutzkontrolle Zutritt zu gewähren. Die Regelung erfolgte zur Umsetzung des Artikels 58 Absatz 1 Buchst. f DSGVO. Der Zugang zu Wohnungen war bei Erlass des LDSG nicht intendiert.

Maßgeblich für die Reichweite der Befugnisse des LfDI ist die DSGVO. Diese räumt in dem genannten Artikel der DSGVO den Aufsichtsbehörden Zugangsrechte zu „den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen“ zur Ausübung ihrer Untersuchungsbefugnisse ein. Von der Regelung der DSGVO sind also auch die für die Dienstausübung in Wohnungen genutzten Geräte des Arbeitgebers erfasst.

Zugleich hat jede Person gemäß Artikel 7 GRCh das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation. Unstreitig ist, dass bei dienstlicher Datenverarbeitung in Wohnungen in Bezug auf die Durchsuchungsbefugnis der Datenschutzaufsicht der Schutzbereich der Wohnung hier ggf. mit dem Grundrecht auf Datenschutz kollidiert.

Im Anwendungsbereich der DSGVO überlagert das europäische Primärrecht die nationalen Grundrechte. Die Reichweite der Untersuchungsbefugnis der Datenschutzaufsicht ist also an Artikel 52 der Grundrechtecharta zu messen. Wesentlich ist danach, dass Einschränkungen nur auf gesetzlicher Grundlage unter Wahrung des Wesensgehalts und der Verhältnismäßigkeit vorgenommen werden. Über ein Zugangsrecht der Datenschutzaufsichtsbehörde auch zu Privaträumen aufgrund der Befugnis gemäß Artikel 58 Absatz 1 Buchst. f DSGVO wurde bisher nicht gerichtlich entschieden. Die Kommentarliteratur äußert sich differenziert[107].

[107] Bejahend Boehm in Kühling/Buchner DS-GVO Artikel 58 Rn, 19; ebenso unter Beachtung des Verhältnismäßigkeitsgrundsatzes und vorbehaltlich einer verfahrensrechtlichen Regelung BeckOK DatenschutzR/Eichler/Matzke DS-GVO Artikel 58 Rn. 15-17; für Richtervorbehalt Körffer in Paal/Pauly DS-GVO, 3. Aufl. 2021, Artikel 58 Rn. 14-16.

Eine Kontrolle in Privaträumen, die dienstlich genutzt werden, gänzlich zu verbieten, ist nach Auffassung der Landesregierung nicht angezeigt, da auch der Grundrechtsschutz der betroffenen Personen, deren Daten verarbeitet werden, nicht vernachlässigt werden darf. Generell und erst recht in Privaträumen sollte eine Vor-Ort-Kontrolle nur stattfinden, wenn kein milderes Mittel zur Verfügung steht. Sie muss außerdem in verhältnismäßiger Weise vorgenommen werden. Dies setzt in der Regel eine Vorankündigung voraus.

Der festgestellten Befugnis der Datenschutzaufsicht korrespondiert die Pflicht des Verantwortlichen, solche Kontrollen zu ermöglichen. Die Regelung des § 26 LDSG stellt diese Pflicht der öffentlichen Stellen klar, berücksichtigt aber bisher nicht Kontrollen in Privaträumen. Dies könnte in den Gesetzestext aufgenommen werden, ergänzt um verfahrensrechtliche Vorschriften zur Wahrung des Verhältnismäßigkeitsgrundsatzes[108]. Auf das Zitiergebot gemäß Artikel 19 GG wird hingewiesen.

Nach der geübten Praxis wird in der Regel Homeoffice nur gewährt, wenn die beschäftigte Person einwilligt, ggf. Kontrollen des LfDI zuzulassen. Allenfalls wegen der möglichen Betroffenheit Dritter, die sich in den Räumlichkeiten aufhalten, könnte einer gesetzlichen Regelung der Vorzug gegeben werden. Nach der Bewertung des LfDI wird für eine solche Regelung aber kein dringendes Bedürfnis gesehen.

19. Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz (§ 27 LDSG)

a) Zum Norminhalt

Der Rundfunkbeauftragte für den Datenschutz wurde als weitere Datenschutzaufsichtsbehörde gemäß Artikel 51 DSGVO eingerichtet. Maßgeblich hierfür ist, die Staatsferne des Rundfunks zu gewährleisten. Hierbei waren wie beim LfDI die Vorgaben der Artikel 51 ff. DSGVO zu beachten. Die materiell-rechtlichen Datenschutzregelungen für den journalistischen Bereich des Rundfunks sind mittlerweile im neuen Medienstaatsvertrag geregelt.

b) Rückmeldungen und Bewertung

Zu § 27 LDSG wurde der Rundfunkbeauftragte für den Datenschutz angehört. Seine Stellungnahme ist als Anlage beigefügt. Der Rundfunkbeauftragte für den Datenschutz schlägt einige Verbesserungen in Bezug auf seine Funktion vor.

[108] Vgl. Erwägungsgrund 129 Satz 6 der DSGVO.

aa) Kontrollmodell

Nach Auffassung des Rundfunkbeauftragten hat sich das datenschutzrechtliche Kontrollmodell beim SWR bewährt. Eines weiteren internen behördlichen Datenschutzbeauftragten bedürfe es daher nicht.

- Bewertung des LfDI (S. 60):

Diesbezüglich ist der LfDI unter Verweis auf Artikel 37 DSGVO anderer Ansicht. Der SWR habe auch einen Datenschutzbeauftragten verpflichtet. Gesetzgeberischer Handlungsbedarf bestehe nicht.

Position der Landesregierung:

Nach der Regelung des § 27 LDSG im Jahr 2018 wurde mit Gesetz vom 6. Dezember 2022 die Anbindung der Aufsichtsbehörde der oder des Rundfunkbeauftragten für den Datenschutz bei der Gremiengeschäftsstelle, die beim MDR in Leipzig angesiedelt ist, eingeführt[109]. Damit einher ging die Bestellung eines eigenen Datenschutzbeauftragten.

bb) Anpassung an den Medienstaatsvertrag

Der Rundfunkbeauftragte weist auf die Aufhebung des Rundfunkstaatsvertrags hin, der durch den Medienstaatsvertrag ersetzt wurde.

Position der Landesregierung:

Die Verweisung auf den Medienstaatsvertrag statt auf § 16c des Rundfunkstaatsvertrags wurde mit dem erwähnten Gesetz in § 27 Absatz 1 Satz 1 LDSG vorgenommen.

cc) Benachteiligungsverbot

Vorgeschlagen wird vom Rundfunkbeauftragten, ein Benachteiligungsverbot auch nach dem Ende der Amtszeit festzulegen, um den Rundfunkbeauftragen vor Benachteiligungen seines Arbeitgebers wegen seiner Aufsichtstätigkeit schützen. Die Erfahrung aus anderen Bundesländern zeige, dass diese Diskriminierungsgefahr bestehe. Eine entsprechende Vorschrift könnte in § 27 Absatz 4 LDSG aufgenommen werden.

[109] Vgl. § 27 Absatz 3 Satz 1 LDSG, eingefügt durch Gesetz vom 6. Dezember 2022 (GBl. S. 622).

- Bewertung des LfDI (S. 60f.):

Der LfDI befürwortet eine entsprechende Regelung. Der Schutzbedarf sei dem eines (behördlichen) Datenschutzbeauftragten vergleichbar, für den sich ein entsprechender Schutz aus Artikel 38 Absatz 3 Satz 2 DSGVO ergebe.

Position der Landesregierung:

Das LDSG regelt die Ausgestaltung des Amtes des Rundfunkbeauftragten für den Datenschutz entsprechend den Vorgaben der DSGVO. Das Arbeitsverhältnis des Rundfunkbeauftragten für den Datenschutz wird insofern durch öffentlich-rechtliche Regelungen überlagert. Die DSGVO enthält jedoch keine Vorschriften zur Ausgestaltung des privatrechtlichen Arbeitsverhältnisses zu seinem Arbeitgeber nach dem Ende der Amtszeit. Dieses Verhältnis richtet sich nach allgemeinen privat- bzw. arbeitsrechtlichen Regelungen. Eine Regelung, wie sie vom Rundfunkbeauftragten für den Datenschutz gefordert wird, in das LDSG aufzunehmen, erscheint aus diesem Grund sachfremd.

dd) Vergütung

Darüber hinaus ist der Rundfunkbeauftragte für den Datenschutz der Auffassung, dass der Gesetzgeber nach Artikel 52 Absatz 4 DSGVO als wesentliche Frage die Vergütung sowie den Status des Rundfunkbeauftragten wie für den LfDI selbst festzulegen habe. Mit der derzeitigen Regelung in § 27 Absatz 3 LDSG werde man seiner unabhängigen Stellung nicht gerecht.

- Bewertung des LfDI (S. 62):

Dem LfDI erscheint die Argumentation des Rundfunkbeauftragten für den Datenschutz grundsätzlich plausibel. Die Unabhängigkeit des Rundfunkbeauftragten solle soweit es die Unabhängigkeit der Organisation des Rundfunks zulasse, geschützt werden.

Position der Landesregierung:

Im Ergebnis wird seitens der Landesregierung kein Erfordernis gesehen, die Regelung des § 27 LDSG entsprechend der Forderung des Rundfunkbeauftragten für den Datenschutz zu ergänzen. Die Grundsätze der Vergütung sind in einer Satzung (Satzung über den Rundfunkbeauftragten für den Datenschutz beim SWR vom 15. Juni 2018) näher geregelt. Auf diese Satzung wird in § 27 Absatz 3 LDSG verwiesen, wo auch normiert ist, dass die Vergütung angemessen zu sein hat. Darüber hinaus wird dort festgehalten, dass ihm „die für die Erfüllung

seiner Aufgaben und Befugnisse notwendige Personal-, Finanz- und Sachausstattung zur Verfügung zu stellen“ ist. Damit sind die Regelungen der DSGVO hinreichend umgesetzt.

Die DSGVO schreibt die Unabhängigkeit der Aufsichtsbehörden vor. Hierzu sind diese gemäß Artikel 52 Absatz 4 mit den personellen, technischen und finanziellen Ressourcen auszustatten, die sie für ihre effektive Aufgabenwahrnehmung benötigen. Es ist zutreffend, dass der Landesgesetzgeber für den Landesdatenschutzbeauftragten in § 23 Absatz 4 LDSG eine Regelung getroffen hat, die die Besoldungsgruppe sowie weitere Gehaltsbestandteile direkt regelt. Eine solche Regelung ist jedoch nicht zwingend erforderlich.

Eine Festlegung des Status und der Höhe der finanziellen Entlohnung des Rundfunkbeauftragten für den Datenschutz würde zudem einen Eingriff in die Finanzautonomie des Südwestrundfunks bedeuten.

Im Übrigen wird darauf hingewiesen, dass auch andere Staatsverträge, die die Rechtsgrundlagen der Landesrundfunkanstalten regeln, sowie diejenigen das ZDF und Deutschlandradio betreffend, entsprechende Vorschriften aufweisen, die die Regelung der Vergütung einer durch die Gremien getroffenen Satzung zuweisen[110].

ee) Tätigkeitsbericht

Nach § 27 Absatz 10 LDSG hat der Rundfunkbeauftragte seinen Tätigkeitsbericht unter anderem dem Landtag zu übermitteln. Vom Rundfunkbeauftragten wird der Sinn dieser Vorschrift hinterfragt.

- Bewertung des LfDI (S. 62):

Der LfDI weist auf die gesetzliche Vorgabe nach Artikel 59 DSGVO hin.

Position der Landesregierung:

Die Regelung in § 27 Absatz 10 LDSG greift die Vorgaben aus Artikel 59 DSGVO auf, welcher festlegt, dass die Aufsichtsbehörde einen Jahresbericht erstellt, der den nationalen Parlamenten, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden übermittelt wird.

[110] Vgl. die Regelungen in Artikel 21 Absatz 5 Bayerisches Rundfunkgesetz, § 38 Absatz 3 MDR-Staatsvertrag; § 44 Absatz 3 NDR-Staatsvertrag, § 16 Absatz 3 DLR-Staatsvertrag, § 16 Absatz 3 ZDF-Staatsvertrag.

ff) Zusammenarbeit mit anderen Aufsichtsbehörden

Der Rundfunkbeauftragte wünscht sich eine stärkere Einbindung des Rundfunkbeauftragten für den Datenschutz in die Datenschutzkonferenz und verweist hierzu auf die Vorschrift des § 14 Absatz 1 Nummer 7 BDSG. § 25 Absatz 1 LDSG sollte um folgenden Satz ergänzt werden:

„Der Landesdatenschutzbeauftragte arbeitet mit allen anderen Aufsichtsbehörden zusammen und unterstützt sie."

- Bewertung des LfDI (S. 57f.):

Der LfDI lehnt den Vorschlag ab. Der Gesetzgeber in Baden-Württemberg könne den LfDI nicht zur Zusammenarbeit mit Gremien außerhalb des Landes verpflichten. Ungeachtet dessen pflege der LfDI einen intensiven Austausch mit spezifischen Aufsichtsbehörden wie dem Rundfunkbeauftragten für den Datenschutz.

Position der Landesregierung:

Entsprechend den Ausführungen zu § 25 Absatz 1 LDSG wird keine Notwendigkeit für die vorgeschlagene Regelung gesehen. Eine Vorschrift zur Zusammenarbeit findet sich u. a. in § 18 BDSG. Damit besteht ein Mechanismus, damit in Angelegenheiten der Europäischen Union zu einer einheitlichen Auslegung gefunden wird.

20. Ordnungswidrigkeiten (§ 28 LDSG)

a) Zum Norminhalt

Entsprechend der Ermächtigung in Artikel 83 Absatz 7 DSGVO wurde die Regelung getroffen, dass gegen öffentliche Stellen keine Geldbußen verhängt werden können. Der zweite Halbsatz stellt klar, dass dies nicht für öffentliche Stellen als Teilnehmer am Wettbewerb gilt. Letzteres betrifft vor allem die fiskalische Tätigkeit von öffentlichen Stellen.

b) Rückmeldungen und Bewertung

aa) Ausnahme Wettbewerbsunternehmen

Folgendes wird vorgebracht: Da öffentliche Stellen, die am Wettbewerb teilnehmen, gemäß § 2 Absatz 6 LDSG bereits vom Anwendungsbereich des LDSG ausgenommen sind, habe die

Vorschrift in § 28 LDSG, 2. Halbsatz nur deklaratorischen Charakter und sei daher überflüssig.

- Bewertung des LfDI (S. 63):

Der LfDI hält die Vorschrift für verständlich und spricht sich gegen eine Streichung aus.

Position der Landesregierung:

Die Vorschrift wäre auch ohne den zweiten Halbsatz eindeutig, da nur die öffentlichen Stellen nach § 2 Absatz 1 und 2 LDSG einbezogen sind. Der Vorschrift kommt daher im zweiten Halbsatz nur klarstellender Charakter zu. Der zweite Halbsatz könnte gestrichen werden. Seine Beibehaltung ist aber ebenfalls unschädlich und macht die Norm auch ohne Kenntnis des § 2 Absatz 6 LDSG verständlich.

bb) Krankenkassen

Das Sozialministerium leitet aus einem Urteil des Europäischen Gerichtshofs vom 11. Juni 2020 ab, dass Krankenkassen nicht als am Markt agierende Unternehmen anzusehen seien. Insbesondere die staatliche Aufsicht und die Verpflichtung auf das Solidarprinzip sprächen gegen die Unternehmereigenschaft. Relevant ist dies in Bezug auf die Frage, inwieweit die Aufsichtsbehörde gegen Krankenkassen Bußgelder verhängen kann. Das Sozialministerium schlägt vor, die Krankenkassen ausdrücklich vom Anwendungsbereich des LDSG auszunehmen. Krankenkassen könnten nur sehr geringfügig frei am Markt agieren. Letztlich müssten Krankenkassen Strafen aus Versichertengeldern bezahlen, da andere Einnahmen nur marginal vorhanden seien. Zudem verweist das Sozialministerium auf den in der 97. Arbeitstagung der Aufsichtsbehörden der Sozialversicherungsträger vom 25. bis 27. November 2020 gefassten Beschluss, nach dem die Aufsichtsbehörden des Bundes und der Länder der Auffassung sind, dass für die Verhängung von Bußgeldern gegenüber Krankenkassen im Rahmen des Sozialdatenschutzes keine Rechtsgrundlage besteht. Hiernach seien gesetzliche Krankenkassen keine „öffentlich-rechtlichen Unternehmen“.

- Bewertung des LfDI (S. 63):

Der LfDI sieht gesetzliche Krankenkassen als öffentliche Stellen im Sinne des § 2 Absatz 2 LDSG, die – sofern sie mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen – grundsätzlich dem möglichen Anwendungsbereich des § 28 LDSG unterfallen.

Position der Landesregierung:

Zur Beurteilung kommt es maßgeblich auf die Auslegung des Unternehmensbegriffs an. Die Aufsichtsbehörden der Sozialversicherungsträger haben in ihrer 97. Arbeitstagung vom 25. bis 27. November 2020 folgenden Beschluss gefasst: „Die Aufsichtsbehörden des Bundes und der Länder sind der Auffassung, dass für die Verhängung von Bußgeldern gegenüber Krankenkassen im Rahmen des Sozialdatenschutzes keine Rechtsgrundlage besteht.“ Begründet wurde der Beschluss im Wesentlichen damit, dass gesetzliche Krankenkassen Körperschaften des öffentlichen Rechts seien und keine „öffentlich-rechtlichen Unternehmen“. Ferner könne die Verhängung von Bußgeldern als Konsequenz zu einer Erhöhung der Beitragszahlungen führen, wodurch im Ergebnis die Versicherten, die keinerlei Einfluss auf die datenschutzrechtlichen Vorkehrungen der Krankenkassen nehmen können, die Bußgelder zu tragen hätten.

Vor dem Hintergrund dieses Beschlusses und dem Urteil des Europäischen Gerichtshofs vom 11. Juni 2020 wird im Ergebnis eine Verhängung von Bußgeldern gegen Krankenkassen als Sanktion für eventuelle Datenschutzverstöße als ausgeschlossen angesehen.

cc) Sanktionen gegen Bedienstete

Nach Auffassung des Regierungspräsidiums Freiburg lasse die Vorschrift Unklarheit über die umstrittene Frage, ob und ggfs. unter welchen Voraussetzungen Bedienstete, die gegen datenschutzrechtliche Bestimmungen verstoßen, zur Verantwortung gezogen werden können. Insoweit wäre eine Klarstellung durch den Gesetzgeber im Interesse der Beschäftigten wünschenswert.

In ihrer gemeinsamen Stellungnahme bitten Gemeindetag und Landkreistag darum, dass die Komplexität des Datenschutzrechts bei der Sanktionierung von Datenschutzverstößen gegen Behördenmitarbeiter und Behörden angemessene Berücksichtigung findet.

- Bewertung des LfDI (S. 63f.):

Nach Auffassung des LfDI ist im Gesetz ausreichend klar geregelt, dass nur öffentliche Stellen, nicht die Mitarbeitenden, Adressaten von Bußgeldern sein können. Damit werde an die Verantwortlichkeit im Sinne des Artikels 4 Nummer 7 DSGVO angeknüpft.

Der LfDI plädiert dafür, Notarinnen und Notare vom Anwendungsbereich des § 28 LDSG auszunehmen, da sie so wie Rechtsanwältinnen und Rechtsanwälte auf eigene Rechnung handelten.

130

Position der Landesregierung:

Zu Sanktionen gegen Bedienstete wurde bereits oben zu § 3 Absatz 2 LDSG ausgeführt. Mitarbeitende, die im Rahmen ihrer Tätigkeit datenschutzwidrig handeln, können nicht sanktioniert werden. Auch ansonsten ist die Vorschrift des § 28 LDSG nicht geeignet, Mitarbeitende zu sanktionieren. Inwieweit der LfDI Sanktionen gemäß Artikel 83 Absatz 2 DSGVO gegen Mitarbeitende verhängen kann, ist – wie unter § 3 Absatz 2 LDSG ausgeführt – umstritten.

Die Einbeziehung von Notarinnen und Notaren wird nach dem Normzweck als fragwürdig angesehen, da von öffentlichen Stellen Rechtstreue erwartet werden kann, ohne dass es eines Bußgelds bedarf. Das öffentliche Recht gewährleistet einen effizienten Rechtsschutz und gewährt die Möglichkeit der Amtshaftung[111].

21. Strafvorschrift (§ 29 LDSG)

a) Zum Norminhalt

Entsprechend dem LDSG a. F. wurde als weitere Sanktion eine Strafvorschrift eingeführt.

b) Rückmeldungen und Bewertung

Seitens des Wissenschaftsministeriums wurde darauf hingewiesen, dass die Vorschrift wie nach dem altem Recht auf einzelne Verarbeitungsschritte abstelle, anstatt sie nach der neuen Systematik durch den Begriff des Verarbeitens zu ersetzen.

- Bewertung des LfDI (S. 64):

Der LfDI stimmt der geäußerten Auffassung zu und hält die Differenzierung für obsolet.

Position der Landesregierung:

Mit der Differenzierung wird zum Ausdruck gebracht, dass nicht jede Form unerlaubter Datenverarbeitung unter Strafe gestellt werden soll. Die unbefugte Datenerhebung soll für den Straftatbestand noch nicht ausreichen[112].

[111] Vgl. Debus in Debus/Sicko, LDSG BW, § 28 Rn. 5.
[112] Vgl. LT-Drs. 16/3930 S. 77.

III. Weiterer Regelungsbedarf

Im Rahmen der Evaluierung wurde das LDSG auch auf seine Vollständigkeit untersucht. Wie oben dargestellt, kann das LDSG wegen des Wiederholungsverbots das allgemeine Datenschutzrecht nicht vollständig abdecken. Dennoch war zu überlegen, ob es weiterer Regelungen für bestimmte Fallgestaltungen bedarf, die bisher fehlen. Teilweise wurden diese bereits unter Teil B II. im Rahmen der jeweiligen Vorschrift abgehandelt. Ergänzend haben sich die folgenden Fragestellungen ergeben.

1. Vorschläge des LfDI

a) Datenübermittlung an ausländische Stellen

Der LfDI schlägt vor, die Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes wie im LDSG a. F.[113] klarstellend zu regeln: Für die Übermittlung an Stellen in anderen Mitgliedstaaten der Europäischen Union, in Vertragsstaaten des Europäischen Wirtschaftsraums oder an Organe und Einrichtungen der Europäischen Union solle § 6 LDSG entsprechend gelten.

Als Absatz 2 könnte nach Auffassung des LfDI hinzugefügt werden: „Die Übermittlung personenbezogener Daten in Staaten außerhalb der Europäischen Union oder an über- oder zwischenstaatliche Stellen ist unter den Voraussetzungen der Artikel 46 bis 49 DSGVO zulässig, soweit keine spezielleren Vorschriften eingreifen."

- Bewertung des LfDI (S. 67):

An diesem Vorschlag hält der LfDI fest.

Position der Landesregierung:

Für die Übermittlung an Stellen in Mitgliedstaaten der EU und sonstige Stellen im Anwendungsbereich der DSGVO könnte eine entsprechende Norm für die Anwender nützlich sein. Für die Übermittlung personenbezogener Daten an Drittländer sind die Voraussetzungen in Artikel 44 ff. DSGVO abschließend geregelt. Sofern diese vorliegen, die Übermittlung personenbezogener Daten also zulässig ist, beurteilen sich die materiell-rechtlichen Voraussetzungen für die Übermittlung nach dem LDSG, sofern keine andere Rechtsgrundlage für die Übermittlung besteht.

[113] Vgl. §§ 16, 20 LDSG a. F.

Gegen den vorgeschlagenen Absatz 2 einer entsprechenden Regelung bestehen insofern Bedenken, als sie nur die bereits aufgrund der DSGVO geltende Rechtslage wiedergibt. Insofern würde sie gegen das Normwiederholungsverbot verstoßen. Dies sollte möglichst vermieden werden.

Zur Vermeidung von Missverständnissen sollte in der Vorschrift des § 2 LDSG wie in § 1 Absatz 5 BDSG der Vorrang der DSGVO geregelt werden. Dies würde klarstellen: Auch sofern im LDSG Wiederholungen der DSGVO zu finden sind, bleibt die unmittelbare Geltung der DSGVO unberührt.

b) Beauftragung der Auftragsverarbeitung durch die Fachaufsichtsbehörde

Der LfDI schlägt unter Verweis auf § 7 Absatz 1 Satz 5 des LDSG a. F. die Aufnahme einer Bestimmung zur Beauftragung der Auftragsverarbeitung durch die Fachaufsichtsbehörde mit Wirkung für die ihrer Aufsicht unterliegende Stellen des Landes vor.

- Bewertung des LfDI (S. 67f.):

An diesem Vorschlag hält der LfDI fest. Er weist ergänzend darauf hin, dass der Gesetzgeber für den Schulbereich inzwischen in § 115 Absatz 3e des Schulgesetzes eine entsprechende Regelung getroffen habe.

Position der Landesregierung:

Für eine entsprechende Regelung wird insbesondere ein Bedürfnis gesehen, wenn besondere Eilbedürftigkeit für eine Auftragsverarbeitung für alle nachgeordneten Dienststellen besteht, wie dies beispielsweise während der Corona-Pandemie der Fall war. Ferner könnte ein Bedürfnis für einheitliche Regelungen hinsichtlich OZG-Maßnahmen, Beschaffungen für den nachgeordneten Bereich und IT-Vereinheitlichungsmaßnahmen bestehen. Dies wird auch anhand des Geltungsbereichs und Regelungsumfangs von § 8a OZG zu prüfen sein.

Um eine gemeinsame Verantwortlichkeit aller das Verfahren nutzenden Stellen zu vermeiden, sollte hierbei klargestellt werden, dass die Verantwortlichkeit jeweils nur zwischen der nutzenden Stelle und dem Auftragsverarbeiter konstituiert wird[114]. Die Verantwortlichkeit entscheidet nämlich darüber, wer die Verpflichtungen nach der DSGVO zu erfüllen hat.

[114] Vgl. Corona-Verordnung Auftragsverarbeitung vom 16. Juni 2020 (GBl. 2020, 415).

Sofern ein Bedürfnis für einheitliche inhaltliche Regelungen besteht, könnte sich die gesetzliche Regelung der Auftragsverarbeitung oder die Vorgabe bestimmter Nutzungsbedingungen anbieten[115].

c) Teilnahme des Personals des LfDI an der Personalrotation

Der LfDI schlägt vor, in den bestehenden § 20 Absatz 2 LDSG eine Regelung zu integrieren, die die Teilnahme des Personals des LfDI an der Personalrotation der Landesverwaltung gewährleiste. Der Personalaustausch schaffe das notwendige Verwaltungsverständnis innerhalb des Personalkörpers des LfDI und sorge dafür, dass die Behörden der Innenverwaltung mit datenschutzrechtlich versiertem Personal versorgt würden.

- Bewertung des LfDI (S. 3, 67):

An diesem Vorschlag hält der LfDI fest.

Position der Landesregierung:

Im LDSG a. F. existierte hinsichtlich der Mitarbeiter des damals beim Landtag eingerichteten Landesbeauftragten für den Datenschutz in § 26 Absatz 4 Satz 5 folgende Regelung: „Ihre Einbeziehung in den allgemeinen Personalaustausch der Landesverwaltung wird von der Landesregierung gewährleistet.“ Im aktuellen LDSG ist keine derartige Regelung enthalten.

Das Anliegen des LfDI ist dem Grunde nach nachvollziehbar. In Anlehnung an die alte Regelung sollte eine Teilnahme am Personalaustausch der Landesverwaltung insgesamt vorgesehen werden und keine Einschränkung auf die Innenverwaltung vorgenommen werden.

d) Effektivität und Durchsetzbarkeit von Anordnungen gegenüber Behörden

Der LfDI weist darauf hin, dass er zwar befugt sei, gemäß Artikel 58 Absatz 2 DSGVO auch Behörden zu einem datenschutzkonformen Verhalten anzuhalten. Mangels Umsetzung des Artikels 58 Absatz 5 DSGVO stünden ihm aber weder gerichtliche Rechtsmittel zu, noch sei ihm die Vollstreckung bestandskräftiger Verwaltungsakte gegen Behörden und juristische Personen des öffentlichen Rechts erlaubt. Die Möglichkeit der Vollstreckung solle in § 25 LDSG aufgenommen werden, um ihm entsprechend seiner unabhängigen Stellung eine effektive Durchsetzung zu ermöglichen. Er führt aus, dass gerade die Möglichkeit, Zwangsgelder zu verhängen insbesondere im kommunalen Bereich die Bereitschaft erhöhen könnte, den Anweisungen der Aufsichtsbehörde Folge zu leisten.

[115] Hierzu wird unten unter 2f) ausgeführt.

134

Soweit der LfDI die Umsetzung des Artikels 58 Absatz 5 DSGVO bemängelt, sieht er darin einen Verstoß gegen europäisches Recht. Hierzu führt er die Rechtsprechung des Europäischen Gerichtshofs an, der noch unter der Geltung der Datenschutz-Richtlinie ein Klagerecht für die Aufsichtsbehörde gefordert hätte. Auch in der Kommentarliteratur werde eine entsprechende Klagemöglichkeit befürwortet.

- Bewertung des LfDI (S. 3, 67):

An diesem Vorschlag hält der LfDI fest.

Position der Landesregierung:

Es ist zutreffend, dass eine Einleitung eines Gerichtsverfahrens durch die Aufsichtsbehörde im Landesrecht nicht ausdrücklich vorgesehen ist.

Die Landesregierung erkennt ausdrücklich an, dass es das Anliegen der DSGVO ist, die Aufsichtsbehörden mit effektiven Befugnissen auszustatten; Erwägungsgrund 129 erläutert dies eingehend. Einer landesrechtlichen Regelung bedarf es hierfür jedoch nach Auffassung der Landesregierung nicht. Die verwaltungsprozessualen Rechte bestimmen sich nach der VwGO. Gegebenenfalls kann auf das Instrument der Feststellungklage zurückgegriffen werden.

Die vom LfDI zitierte Rechtsprechung des Europäischen Gerichtshofs bezog sich im Zusammenhang mit der Überprüfung einer Angemessenheitsentscheidung der Kommission auf das in Artikel 28 Absatz 3 der damals geltenden Datenschutz-Richtlinie erwähnte „Klagerecht“ der Kontrollstelle[116]. Der Europäische Gerichtshof hält es für die „Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen“. Ein entsprechendes Klagerecht ist in § 21 BDSG umgesetzt.

Die Vorschrift des Artikels 58 Absatz 5 DSGVO ist unter anderem auch in § 13 Absatz 6 BDSG umgesetzt, der in Verbindung mit Absatz 4 Satz 7 ein Anzeigerecht für den LfDI bei festgestellten Datenschutzverstößen normiert.

Zur Durchsetzung seiner Anordnungen dem LfDI die Verwaltungsvollstreckung gegenüber Behörden zu erlauben, besteht nach Auffassung der Landesregierung aus den folgenden – bereits im Rahmen der Gesetzesbegründung angeführten – Gründen kein Anlass.

[116] Vgl. EuGH, Urteil vom 06.10.2015, C-362/14, abrufbar unter CURIA - Dokumente (europa.eu).

135

Während der LfDI gegenüber nichtöffentlichen Stellen seine Anordnungen mittels Verwaltungsvollstreckung unmittelbar durchsetzen kann, steht ihm dieser Weg gegenüber Behörden nicht offen. Nach geltender Rechtslage kann gegen Behörden und juristische Personen des öffentlichen Rechts nur vollstreckt werden, soweit dies durch Rechtsvorschriften ausdrücklich gestattet ist (§ 22 des Landesverwaltungsvollstreckungsgesetzes). Dieser Gesetzesvorbehalt dient der Einhaltung des allgemein anerkannten Grundsatzes - welcher sich ebenfalls im Verwaltungsvollstreckungsgesetz des Bundes in § 17 wiederfindet -, wonach in der Regel kein Hoheitsträger gegen einen anderen Träger hoheitlicher Befugnisse mit Mitteln des Verwaltungszwangs vorgehen darf. Ein solches Vorgehen ist mit dem grundsätzlich koordinationsrechtlich geprägten Verhältnis zwischen Hoheitsträgern und mit dem Ansehen der Behörden nicht vereinbar. Es darf vielmehr davon ausgegangen werden, dass eine Behörde die ihr obliegenden Pflichten auch ohne Anwendung von Zwangsmitteln erfüllt, da von ihr aufgrund ihrer Bindung an Gesetz und Recht (Artikel 20 Absatz 3 des Grundgesetzes und Artikel 25 Absatz 2 der Verfassung des Landes Baden-Württemberg) grundsätzlich Rechtstreue erwartet werden kann.

Sowohl im Bundes- als auch im Landesrecht[117] werden nur sehr vereinzelt gesetzliche Ausnahmen von der grundsätzlichen Unzulässigkeit des Verwaltungszwangs gegen Hoheitsträger geschaffen. Diese restriktive Normierung spezialgesetzlicher Ausnahmeregelungen ist angezeigt, um den genannten Grundsatz nicht zu konterkarieren.

Hinsichtlich der Durchsetzung von datenschutzrechtlichen Anordnungen des LfDI gegenüber Behörden sind keine Gründe ersichtlich, die eine gesetzliche Ausnahmeregelung von der grundsätzlichen Unzulässigkeit des Verwaltungszwangs gegen Hoheitsträger rechtfertigen würden. Vielmehr ist mit der Einschaltung der Rechts- oder Fachaufsicht bereits ein milderes Mittel vorhanden, mit dem die Erfüllung der datenschutzrechtlichen Verpflichtungen effektiv durchgesetzt werden kann. Es ist zu erwarten, dass im Falle von Zweifeln an der Rechtmäßigkeit der Anordnung des LfDI die betroffene Behörde selbst ein gerichtliches Verfahren einleitet. Durch die Beteiligung des LfDI an diesem Verfahren entsprechend § 18a des Gesetzes zur Ausführung der Verwaltungsgerichtsordnung (AGVwGO) dürfte eine hinreichende Durchsetzungsmöglichkeit im Sinne von Artikel 58 Absatz 5 DSGVO bestehen. Sollte es doch einmal erforderlich werden – bislang ist, soweit ersichtlich, dieser Fall nicht eingetreten – wäre ein gerichtliches Vorgehen des LfDI, etwa im Wege einer Feststellungsklage, aber durchaus denkbar.

Erwähnt werden soll in diesem Zusammenhang die Regelung in § 19 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes. Die Vorschrift lautet wie folgt:

[117] Vgl. z. B. § 123 Gemeindeordnung für Baden-Württemberg

„§ 19 Gerichtlicher Rechtsschutz
…
„(5) Behörden und sonstige öffentliche Stellen des Landes können unbeschadet anderer Rechtsbehelfe gerichtlich gegen sie betreffende verbindliche Entscheidungen der oder des Hessischen Datenschutzbeauftragten vorgehen. Wenn die Behörde oder öffentliche Stelle eine verbindliche Entscheidung der oder des Hessischen Datenschutzbeauftragten nicht beachtet und nicht innerhalb eines Monats nach Bekanntgabe gerichtlich gegen diese vorgeht, kann die oder der Hessische Datenschutzbeauftragte die gerichtliche Feststellung der Rechtmäßigkeit der getroffenen verbindlichen Entscheidung beantragen."

Begründet wurde diese Vorschrift im hessischen Gesetzentwurf folgendermaßen:
„Absatz 5 Satz 1 statuiert - auch in Verbindung mit § 56 - die Zulässigkeit eines Insichprozesses zwischen einer Behörde oder anderen öffentlichen Stelle des Landes einerseits und der oder dem Hessischen Datenschutzbeauftragten andererseits. Satz 2 sieht für die oder den Hessischen Datenschutzbeauftragten die Möglichkeit zur gerichtlichen Feststellung der Rechtmäßigkeit seiner getroffenen verbindlichen Entscheidung vor, sofern die Behörde oder sonstige öffentliche Stelle des Landes nicht innerhalb eines Monats nach Bekanntgabe der verbindlichen Entscheidung Klage hiergegen erhoben hat. Damit wird erreicht, dass den Justizbehörden auch im Innenverhältnis des Landes Verstöße gegen das Datenschutzrecht zur Kenntnis gebracht werden."

Während der erste Satz der hessischen Regelung § 18a AGVwGO entspricht, geht Satz 2 darüber hinaus, indem er dem hessischen Datenschutzbeauftragten eine eigene Klagebefugnis zuweist. Mit einer entsprechenden Regelung könnte eine Klarstellung in Bezug auf die Klagemöglichkeiten des LfDI bewirkt werden.

e) Aufsichtszuständigkeit im Telemedienbereich

Der LfDI regte in seiner Stellungnahme vom 6. November 2020 an, die Sonderzuständigkeit des Regierungspräsidiums Karlsruhe für datenschutzrechtlich geprägte Ordnungswidrigkeiten nach dem Telemediengesetz gemäß § 4 Absatz 2 Nummer 4 der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten (OWiZuVO) aufzuheben und auf ihn zu übertragen.

- Bewertung des LfDI (S. 4, 64ff, 67f.):

Nachdem die Übertragung der Zuständigkeit für die relevanten Ordnungswidrigkeiten zwischenzeitlich in Umsetzung des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) vom 23. Juni 2021

geschehen sei, solle ihm auch die Zuständigkeit übertragen werden, die Einhaltung der Vorgaben des TTDSG zu überwachen und abseits von Bußgeldern durchzusetzen.

Position der Landesregierung:

Der Bundesgesetzgeber hat das Datenschutzrecht der Telekommunikation und der Telemedien mit dem TTDSG neu geregelt. Das Gesetz ist am 1. Dezember 2021 in Kraft getreten. Im Gesetz wurden die Ordnungswidrigkeiten neu geregelt, u. a. auch neue Tatbestände eingeführt. Mittlerweile wurde das TTDSG in das Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz - TDDDG) überführt.

Nach Erlass des TTDSG war es notwendig, die zuständige Verwaltungsbehörde für die Verfolgung der Ordnungswidrigkeiten neu zu bestimmen. Eine entsprechende Neuregelung ist im Zuge der Novellierung des Landesmediengesetzes zwischenzeitlich erfolgt, wobei die Abgrenzung so vorgenommen wurde, dass der LfDI für die datenschutzrechtlich geprägten Ordnungswidrigkeiten des § 28 Absatz 1 Nummer 10, 11 und 13 TTDSG die zuständige Verwaltungsbehörde ist [118], soweit nicht der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig ist. Für die nicht datenschutzrechtlich geprägten Ordnungswidrigkeiten bleibt gemäß § 4 Absatz 2 Nummer 4 OWiZuVO das Regierungspräsidium Karlsruhe zuständig, sofern nicht eine Sonderzuständigkeit der Landesanstalt für Kommunikation eingeführt wurde.

Seitens der Landesregierung wird ebenfalls ein Gleichlauf von Aufsicht und Sanktionsbefugnis für sinnvoll gehalten. Wie der LfDI zutreffend erwähnt, haben einige Länder, zuletzt Hamburg, die Aufsichtszuständigkeit explizit geregelt[119]. Andere Länder sind dagegen wie Baden-Württemberg bisher der Auffassung, dass bereits eine ausreichende Regelung besteht. Die Zuständigkeit für die Aufsicht über nichtöffentliche Stellen wie auch die Befugnisse sowohl nach der DSGVO als auch nach § 40 BDSG können auch im Anwendungsbereich des TDDDG über § 1 Absatz 1 Nummer 8 TDDDG, § 40 BDSG, § 25 Absatz 1 LDSG hergeleitet werden, weil die letztgenannte Regelung § 40 BDSG umfassend in Bezug nimmt und dieser über § 1 Absatz 1 Nummer 8 TDDDG weiterhin (wie schon bisher, bevor die Datenschutzrichtlinie für elektronische Kommunikation[120] umgesetzt wurde) auch Cookies erfasst. Daneben besteht die Zuständigkeit nach § 113 MStV, der die Aufsicht über die Telemedien den nach dem Landesrecht zuständigen Datenschutzaufsichtsbehörden zuweist. Demnach wäre

[118] Vgl. § 3 a OWiZuVO.
[119] Vgl. § 19 Absatz 7 Hamburgisches Datenschutzgesetz.
[120] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

der LfDI gemäß § 25 Absatz 1 LDSG die zuständige Aufsichtsbehörde, ohne dass es einer weiteren Regelung bedarf.

Soweit es der Klarstellung dient, könnte die vom LfDI vorgeschlagene Regelung in die Vorschriften des LDSG zur Aufsichtszuständigkeit des LfDI aufgenommen werden.

f) Umsetzungsdefizit im LDSG-JB

Der LfDI bemängelt, dass im LDSG-JB eine ausdrückliche gesetzliche Bestimmung zur Umsetzung der JI-Richtlinie fehle, wonach der LfDI uneingeschränkt bei der Ausarbeitung von Gesetzen und untergesetzlichen Regelungen des Landes, die die Verarbeitung personenbezogener Daten betreffen, zu beteiligen sei (S. 3f., 76). Eine § 26 Absatz 2 LDSG entsprechende Regelung solle auch in das LDSG-JB eingefügt werden.

Position der Landesregierung:

Das LDSG-JB ist nicht Gegenstand der Evaluierung. Es bietet sich aber an, eine Regelung entsprechend dem Vorschlag des LfDI aufzunehmen.

2. Vorschläge der Ressorts

Aus den Ressorts wurde um die Prüfung folgender bisher nicht berücksichtigter Bedarfe gebeten.

a) Regelung zur Datenschutzfolgenabschätzung

Artikel 35 DSGVO verlangt für Datenverarbeitungen mit hohem Risiko für die Rechte und Freiheiten natürlicher Personen vorab eine Einschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten.

Seitens des Kultusministeriums wird angemerkt, dass die Durchführung einer Datenschutzfolgenabschätzung (DSFA) sehr komplex sei, vor allem, da es bisher die Liste der Verarbeitungen, für die keine DSFA durchzuführen sei, nicht gebe. Aufgrund dieses „datenschutzrechtlichen Orientierungsvakuums“ werde vorgeschlagen, eine klarstellende Regelung wie in § 9 des Landesdatenschutzgesetzes Rheinland-Pfalz[121] zu treffen. Dies käme insbesondere den Schulen zugute. Seitens eines Staatlichen Schulamts wurde dementsprechend vorgebracht, dass unklar sei, wie die DSFA durchzuführen sei bzw. ob sie in bestimmten Fällen als nicht verpflichtend anzusehen sei.

- Bewertung des LfDI (S. 72ff.):

Der LfDI sieht die Regelung von Rheinland-Pfalz als problematisch an. Eine Öffnungsklausel hierfür sei nicht ersichtlich. Artikel 35 Absatz 1 Satz 2 und Absatz 10 DSGVO würden bereits Erleichterungen vorsehen; hierauf könne, ggf. auch konkretisierend, verwiesen werden.

[121] § 9 LDSG Rheinland-Pfalz
Datenschutz-Folgenabschätzung
(1) Eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der Datenschutz-Grundverordnung durch den Verantwortlichen kann unterbleiben, soweit
1.eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Ministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird oder
2.der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine Datenschutz-Folgenabschätzung erfolgt ist, es sei denn, dass in der Rechtsvorschrift etwas anderes bestimmt ist.
Die Ministerien stellen den öffentlichen Stellen die Ergebnisse der von ihnen und der von ihnen ermächtigten öffentlichen Stellen durchgeführten Datenschutz-Folgenabschätzungen zur Verfügung.
(2) Entwickelt eine öffentliche Stelle ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, so kann sie, sofern die Voraussetzungen des Artikels 35 Absatz 1 der Datenschutz-Grundverordnung bei diesem Verfahren vorliegen, die Datenschutz-Folgenabschätzung nach den Artikeln 35 und 36 der Datenschutz-Grundverordnung durchführen. Soweit das Verfahren von öffentlichen Stellen im Wesentlichen unverändert übernommen wird, kann eine weitere Datenschutz-Folgenabschätzung durch die übernehmenden öffentlichen Stellen unterbleiben.
Gleichlautende Regelung in Artikel 14 des Bayerischen Datenschutzgesetzes.

Wenn mehrere Verantwortliche sich auf eine DSFA stützen wollten, sei es entscheidend, dass die Maßnahmen umgesetzt würden und eine Begründung vorgelegt werden könne, warum eine einzige DSFA ausreichend sei. Denn es stehe mit der vorgeschlagenen Regelung zu befürchten, dass die DSFA unkritisch übernommen werde, obwohl sie für den konkreten Anwendungsfall nichtzutreffend sei.

Position der Landesregierung:

Artikel 35 Absatz 10 DSGVO regelt bereits die vorgezogene DSFA bei Erlass der Rechtsgrundlage. Der Gesetzgeber übernimmt in diesen Fällen die Verantwortlichkeit für die Durchführung und entlastet damit die Verantwortlichen und Regelungsadressaten des Gesetzes von der Durchführungspflicht. Allerdings wird die DSFA im Gesetzgebungsverfahren eher die Ausnahme darstellen, sollte aber, soweit möglich, mitbedacht werden.

Die vorgeschlagene Regelung würde es erlauben, dass nachgeordnete Stellen die DSFA der obersten Landesbehörden oder von ihr ermächtigter Stellen oder die DSFA anderer Stellen, die für dasselbe automatisierte Verfahren eine DSFA durchgeführt haben, übernehmen. Die Erstellung einer eigenen DSFA durch die nachnutzenden Stellen kann in diesen Fällen unterbleiben.

Von der Normierung wie vorgeschlagen wird eher abgeraten. Zum einen enthält die DSGVO keine Öffnungsklausel für diesbezügliche landesgesetzliche Regelungen. Zum anderen sieht Artikel 35 Absatz 1 Satz 2 DSGVO ausdrücklich vor, dass für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken eine einzige Abschätzung vorgenommen werden kann. Gemäß Erwägungsgrund 92 kann die DSFA vernünftigerweise zur Schonung von Ressourcen thematisch breiter angelegt werden, beispielsweise für eine gemeinsame Anwendung oder Verarbeitungsplattform von Behörden oder für mehrere Verantwortliche bei gleicher Verarbeitungsumgebung. Dies dürfte vor allem für den Schulbereich Entlastung versprechen.

Grundsätzlich bleibt der Verantwortliche in der Pflicht, wenn der Gesetzgeber die DSFA noch nicht vorgenommen hat. Dies kann auch durch unterschiedliche Gegebenheiten vor Ort gerechtfertigt sein. Allerdings sind die verantwortlichen öffentlichen Stellen nicht gehindert, bei der Übernahme gleichgelagerter Verfahren sich die DSFA der anderen öffentlichen Stelle zu eigen zu machen, sofern die Ausgangslage die gleiche ist.

141

b) Regelungen zum Schutz der Daten von Behördenmitarbeiterinnen und -mitarbeitern

Im Hinblick auf Unsicherheiten bei der Herausgabe von Daten der Behördenmitarbeiterinnen und -mitarbeiter, z. B. bei der Auslegung von Planunterlagen in förmlichen Verwaltungsverfahren, Veröffentlichung von Protokollen im Internet etc., wird vom Umweltministerium eine klarstellende Regelung angeregt. In der Praxis auftretende Unsicherheiten fänden sich insbesondere in förmlichen Verwaltungsverfahren, da dort der Bedarf, große Mengen an Dokumenten unter Zeitnot zu veröffentlichen, besonders groß sei.

- Bewertung des LfDI (S. 38ff.):

Der LfDI ist der Auffassung, dass eine klarstellende Regelung nicht zwingend notwendig sei. Namen von Beschäftigten sollten grundsätzlich nicht ins Internet gestellt werden. Dies sei nicht erforderlich, da Dritte den zuständigen Beschäftigten auch über das Sachgebiet, Funktionspostfächer oder die Telefondurchwahl erreichen können. Ausnahmsweise könne die Veröffentlichung von Ansprechpersonen in Behörden gemäß § 15 Absatz 1 Satz 1 LDSG im Internet zulässig sein. Dies treffe z. B. zu auf Personen, deren Tätigkeit nach außen wirke (wie Behördenleitung, Abteilungs- und Referatsleitungen, Pressesprecherinnen und Pressesprecher, Ansprechpersonen für Projekte mit Bürgerbeteiligung). Ohne deren Einwilligung können folgende Daten veröffentlicht werden: Name, Vorname, Tätigkeitsbereich, Adresse der Dienststelle, dienstliche Telefonnummer sowie dienstliche E-Mail-Adresse. Im Übrigen bedürfe die Bekanntgabe von personenbezogenen Daten sonstiger Mitarbeitender im Internet der Abwägung im Einzelfall. Zeitnot sei jedenfalls keine rechtfertigende Grundlage für die Veröffentlichung.

Position der Landesregierung:

Die Auffassung des LfDI an, dass die Namensnennung von Behördenmitarbeitern nach außen in der Regel nicht zulässig, weil nicht erforderlich ist, wird geteilt. Eine ähnliche Wertung nimmt § 5 Absatz 3 LIFG in Bezug auf die beantragte Herausgabe von Unterlagen vor. Eine gesetzliche klarstellende Regelung ist möglich, sollte aber nicht zu detaillierte Regelungen treffen.

c) Regelungen zum Datenschutzbeauftragten

Aus dem Hochschulbereich wurde angeregt, in Bezug auf die Ernennung eines Datenschutzbeauftragten und zum Umfang seiner Aufgabenwahrnehmung Regelungen aufzunehmen, insbesondere folgenden Inhalts:

- Regelungen für die Freistellung, gestaffelt nach der Größe der Körperschaft,

- Regelungen bezüglich einer Beratung der Verfassten Studierendenschaft und des Personalrats durch den Datenschutzbeauftragten,
- Regelungen zu den dem Datenschutzbeauftragten zur Verfügung zu stellenden Ressourcen,
- Beschwerderecht bei der Aufsichtsbehörde
- Vorlagepflicht der Berichte an den LfDI,
- Regelungen zu Ausschreibungsverfahren und Mindestqualifikationen.

- Bewertung des LfDI (S. 68f.):

Der LfDI befürwortet eine Regelung von Mindestkapazitäten und Mindestressourcen von Datenschutzbeauftragten, damit diese ihre Aufgaben ordnungsgemäß wahrnehmen können. Dagegen wird ein explizites Recht zur Vorlage von Vorgängen an den LfDI oder gar eine Vorlagepflicht für Datenschutzbeauftragte nicht für erforderlich gehalten. Die verantwortlichen Stellen hätten sicherzustellen, dass die Datenschutzbeauftragten ihrer Aufgabe nachkommen könnten. Die Pflicht zur Datenpannenmeldung und Beratungsangebote garantierten ausreichend die Beteiligung des LfDI.

Position der Landesregierung:

Das LDSG enthält im Hinblick auf die Vorschriften der DSGVO in den Artikeln 37 ff. zu den Datenschutzbeauftragten keine eigenen Regelungen zu den behördlichen Datenschutzbeauftragten. Das Wiederholungsverbot verbietet gleichlautende Regelungen. Im Übrigen sind Spezifizierungen nur sehr eingeschränkt erlaubt. Im Wesentlichen gilt nach der DSGVO für Datenschutzbeauftragte Folgendes:

- Die DSGVO schließt innerorganisatorische (ggf. durch Satzung) oder spezial- oder untergesetzliche Regelungen für den nachgeordneten Bereich, z. B. zur Freistellung oder zur Bestellung externer Datenschutzbeauftragter, nicht aus.
- Da die Aufzählung der Aufgaben des Datenschutzbeauftragten in Artikel 39 Absatz 1 DSGVO nicht abschließend ist, ist die Festlegung weiterer Aufgaben möglich, sofern hierdurch kein Interessenkonflikt entsteht[122]. Dies könnte z. B. im Universitätsbereich die Beratung der Verfassten Studierendenschaft und des Personalrats umfassen.
- Gemäß Artikel 38 DSGVO sind dem Datenschutzbeauftragten die zur Erfüllung seiner Aufgaben erforderlichen Ressourcen zur Verfügung zu stellen. Diese sind, abhängig von den spezifischen Anforderungen in der verantwortlichen Stelle, von dieser festzulegen.

[122] Vgl. Artikel 38 Absatz 6 DSGVO.

- Die Benennung des Datenschutzbeauftragten ist in Artikel 37 DSGVO geregelt, der auch Anforderungen an die Qualifikation stellt.
- Der Datenschutzbeauftragte hat gemäß Artikel 39 Absatz 1 Buchst. d und e DSGVO auch die Aufgabe, mit der Datenschutzaufsichtsbehörde zusammenzuarbeiten sowie für diese als Ansprechpartner für alle im Zusammenhang mit der Datenverarbeitung zusammenhängenden Fragen zu fungieren. Darüberhinausgehende Regelungen zu weiteren Aufgaben müssen die Unabhängigkeit des LfDI berücksichtigen, dem vom Gesetzgeber keine weiteren Aufgaben zugewiesen werden dürfen.

Zusammenfassend kann festgehalten werden, dass das LDSG nicht geeignet ist, spezifische Anforderungen an den Datenschutzbeauftragten festzulegen, die im jeweiligen Fachbereich angemessen sind. Ggf. sind hierzu spezifische Regelungen, auch untergesetzlicher Art, zu prüfen.

d) Diskriminierungsschutz und Erweiterung sensibler Daten

Es wurden aus dem Sozialministerium Vorschläge gemacht, im Datenschutzrecht einen stärkeren Antidiskriminierungsschutz zu verankern, z. B. durch Vorgaben bei der Verwendung von Algorithmen oder die Einbeziehung weiterer sensibler Daten in den Schutz nach Artikel 9 DSGVO.

- Bewertung des LfDI (S. 45):

Der LfDI sieht für die generelle Gleichsetzung zusätzlicher Arten personenbezogener Daten mit den in Artikel 9 DSGVO geregelten besonderen Kategorien personenbezogener Daten mangels Öffnungsklausel keinen Raum. Denkbar und wünschenswert sei es allerdings, im Rahmen der Öffnungsklauseln nach Artikel 6 Absatz 1 Buchst. c und e, Absatz 2 und 3 DSGVO spezifischere Anforderungen für die Verarbeitung weiterer sensibler Datenarten zur Aufgabenerfüllung zu regeln.

Position der Landesregierung:

Regelungen zum Profiling finden sich bereits in Artikel 22 DSGVO. Entscheidungen aufgrund automatisierter Verarbeitung einschließlich Profiling sind außer aufgrund einer Rechtsvorschrift verboten. Für die Verarbeitung besonders geschützter Kategorien personenbezogener Daten ist dies noch weiter eingeschränkt auf die Fälle ausdrücklicher Einwilligung oder aus Gründen eines erheblichen öffentlichen Interesses.

Artikel 9 DSGVO zählt besonders sensible Daten auf, deren Verarbeitung in besonderem Maße das Risiko einer diskriminierenden Verwendung birgt. Wegen des Anwendungsvorrangs der DSGVO können die aufgezählten Daten nicht erweitert werden.

Im Rahmen der Öffnungsklauseln nach Artikel 6 Absatz 1 Buchst. c und e, Absatz 2 und 3 DSGVO sollten Regelungen zu besonderen Anforderungen für die Verarbeitung weiterer sensibler Datenarten in erster Linie der spezifischen Gesetzgebung vorbehalten bleiben, wie sie z. B. in Bezug auf den Mieterschutz, Behindertenschutz, Arbeitnehmerschutz, den Schutz ausländischer Mitbürger oder Menschen mit Migrationshintergrund bereits bestehen. Im Entwurf zur Ersten Änderung des Bundesdatenschutzgesetzes wurde eine eigene Regelung zu Scoring aufgenommen, um für die Prüfung der Kreditwürdigkeit die Verwendung bestimmter diskriminierender Merkmale auszuschließen[123]. Darüber hinaus ist im Gesetzgebungsverfahren zu prüfen, ob und ggf. welche weiteren Anforderungen für die Verarbeitung solcher sensiblen Datenarten neben den Regelungen in spezifischen Gesetzen möglich und erforderlich sind.

Zur Vermeidung von Diskriminierung werden auch zunehmend auf europäischer Ebene Regelungen vorgeschlagen und erlassen. Beispiele hierfür sind der Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit[124] sowie der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung[125]. Der Einsatz von KI in der Verwaltung wird im Besonderen auf den Schutz vor Diskriminierung zu achten haben. Ggf. ist hier an spezifische Regelungen zu denken, soweit die KI-Verordnung hierzu noch Spielräume lässt und weiterer Schutz aus Sicht des Landes erforderlich ist.

e) Widerspruchsrecht aus Gründen der Verletzung höherwertiger Rechtsgüter

Des Weiteren wurde zurückgemeldet, dass eine Regelung vergleichbar dem früheren § 5 Absatz 1 Nummer 4 in Verbindung mit § 4 Absatz 6 LDSG a.F. notwendig wäre. Es fehle an einer Regelung, die es dem Betroffenen ermögliche, der Datenverarbeitung zu widersprechen, wenn eine fortgesetzte Verarbeitung zu einer Verletzung höherwertiger Rechtsgüter führen würde. Die DSGVO sehe ein Widerspruchsrecht nur teilweise vor. Eine ausdrückliche Regelung eines Betroffenenrechts, aus Gründen der Verletzung höherrangiger Rechte die Einschränkung der Verarbeitung verlangen zu können, sei erforderlich. Anderenfalls könne von der durch eine Rechtsgrundlage legitimierten Verarbeitung personenbezogener Daten nur aufgrund der Anwendung des Verhältnismäßigkeitsgrundsatzes abgesehen werden.

[123] Vgl. § 37a BDSG-Entwurf lt. Bundesrat Drs. 72/24.
[124] Vgl. Bundesrat Drs. 846/21.
[125] Vgl. Bundesrat Drs. 826/21.

- Bewertung des LfDI (S. 71):

Aus Sicht des LfDI ist nicht ersichtlich, dass insoweit eine Öffnungsklausel in der DSGVO zur Verfügung stünde. Das Widerspruchsrecht aus Artikel 21 DSGVO gelte unmittelbar.

Position der Landesregierung:

Die DSGVO enthält in Artikel 21 ein Widerspruchsrecht der betroffenen Person aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen Verarbeitungen auf der Grundlage von Artikel 6 Absatz 1 Buchst. e und f DSGVO. Dieses Recht wurde im LDSG, anders als im Bundesdatenschutzgesetz (vgl. § 36 BDSG), nicht eingeschränkt. Ein Bedürfnis nach einem weitergehenden Widerspruchsrecht wird wegen der Bindung der Verwaltung an Recht und Gesetz nicht gesehen. Die öffentlichen Stellen haben bei der Gesetzesanwendung insbesondere den Vorrang des Verfassungsrechts, besonders der Grundrechte des Grundgesetzes, und der Grundrechtecharta zu beachten. Mit den Einwendungen der Bürgerinnen und Bürger hat sich die Verwaltung im Übrigen auch ohne die Normierung eines speziellen Widerspruchsrechts auseinanderzusetzen. Dem Bürger steht grundsätzlich der Rechtsweg offen.

f) Auftragsverarbeitung gesetzlich regeln

Es wurde vorgeschlagen, die Betrauung eines Dienstleisters der Verwaltung, statt durch Vertrag, gesetzlich zu regeln. Ein solches Vorgehen wird vor allem in den Fällen für sinnvoll gehalten, in denen die Verwaltung verpflichtet sei, einen bestimmten Dienstleister zu beauftragen; eine entsprechende Verpflichtung ist z. B. in § 3 des Gesetzes zur Errichtung der Landesoberbehörde IT Baden-Württemberg (BITBWG) genannt. Mit einer gesetzlichen Regelung in einem Spezialgesetz oder im LDSG könnte der Aufwand der individuellen Vertragsvereinbarung unterbleiben. Auch für fakultativ zu beauftragende Dienstleister, z. B. des Logistikzentrums Baden-Württemberg bei Vergabeverfahren, wird dieser Weg vorgeschlagen, soweit sie eine öffentliche Stelle darstellten bzw. besitzanteilig überwiegend einer öffentlichen Stelle angehören würden.

- Bewertung des LfDI (S. 69f.):

Aus Sicht des LfDI könne eine Normierung wie vorgeschlagen die Praxis sinnvoll entlasten. Die Corona-Verordnung Auftragsdatenvereinbarung stelle ein entsprechendes Beispiel dar. Allerdings sei fraglich, ob eine einheitliche Regelung die mutmaßlich sehr unterschiedlichen Leistungen der BITBW abdecken könne. Insbesondere die zu vereinbarenden technischen und organisatorischen Maßnahmen oder die Einbeziehung von Unterauftragnehmern erforderten möglicherweise eine auf die unterschiedlichen Auftragssituationen angepasste Regelung.

Diese Frage solle mit der BITBW geklärt werden. Gegebenenfalls könnte eine Regelung sachnäher im BITBWG getroffen werden. Auch dürfte eine Ausgestaltung durch eine oder mehrere Rechtsverordnungen praktikabler sein als eine Normierung unmittelbar im Parlamentsgesetz.

Position der Landesregierung:

Es ist zutreffend, dass Artikel 28 Absatz 3 Satz 1 DSGVO die Auftragsverarbeitung nicht nur auf der Grundlage eines Vertrags legitimiert, sondern auch auf der Grundlage eines anderen Rechtsinstruments, das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Die Vorschrift der DSGVO zählt des Weiteren enumerativ alle zu treffenden Regelungen auf.

Eine entsprechende Grundlage für die Auftragsverarbeitung könnte daher auch ein Gesetz oder eine Verordnung auf der Grundlage eines Gesetzes sein. Für letzteres bedürfte es noch einer landesgesetzlichen Verordnungsermächtigung. Entsprechende Regelungen zur Datenverarbeitung im Auftrag finden sich teilweise in anderen Ländern[126].

Alternativ kann der Gesetzgeber für das Zustandekommen eines Auftragsverarbeitungsvertrags durch staatliche Stellen Vorgaben machen sowie allgemeine Nutzungsbedingungen verbindlich vorschreiben. Eine entsprechende gesetzliche Regelung wurde im Freistaat Bayern gewählt[127], wobei eine abweichende Individualvereinbarung möglich ist.

Der Vorteil entsprechender gesetzlicher Regelungen ist die Bindung der gesamten staatlichen Verwaltung an einheitliche Vorgaben. Die Rechtmäßigkeit wird dadurch in verstärktem Maße sichergestellt. Nachteil könnte sein, dass eine gesetzliche Regelung nicht flexibel genug ist, um ggf. kurzfristige Änderungen zu ermöglichen. Abweichungen durch individualvertragliche Regelungen sollten jedenfalls möglich sein, soweit dies erforderlich ist.

g) Datenschutzaufsichtsbehörde für die Justiz

Seitens des Justizministeriums wird unter Verweis auf Erwägungsgrund 20 der DSGVO die Frage gestellt, durch welchen Rechtsakt Stellen mit der Aufsicht über die Einhaltung der

[126] Vgl. z. B. die saarländische „Verordnung zur Regelung der Rechtsbeziehungen bei der ‚Datenverarbeitung im Auftrag' zwischen den Dienststellen und Einrichtungen des Landes (Dienststellen der öffentlichen Hand) und dem Auftragsverarbeiter (IT-DLZ)" vom 28. April 2021 (Amtsblatt I 2021, 1418), abrufbar unter https://recht.saarland.de/bssl/document/jlr-AuftrVVSLrahmen.
[127] Vgl. Artikel 38 Bayerisches Digitalgesetz vom 22. Juli 2022.

DSGVO in der Justiz betraut werden könnten. Denn zur Wahrung der Unabhängigkeit der Justiz sollten, wie Erwägungsgrund 20 ausführt, „die eingerichteten Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein. Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollten besondere Stellen im Justizsystem des Mitgliedstaats betraut werden können, die insbesondere die Einhaltung der Vorschriften dieser Verordnung sicherstellen."

- Bewertung des LfDI (S. 75):

Der LfDI schließt sich der Forderung nach einer Aufsichtsbehörde für die Justiz ausdrücklich an. Sie entspreche einer Forderung, die durch die Datenschutzkonferenz bereits mit Schreiben vom April 2022 an die Justizministerkonferenz herangetragen wurde.

Position der Landesregierung:

In seinem Urteil vom 2. März 2023 hat der Europäische Gerichtshof entschieden, dass Zivilgerichte bei der Vorlage von Dokumenten als Beweismittel an Artikel 6 Absatz 3 und 4 DSGVO gebunden sind und unter Beachtung des Verhältnismäßigkeitsgrundsatzes und des Grundsatzes der Datenminimierung (nach Artikel 5 DSGVO) im Einzelfall die Interessen der betroffenen Personen zu berücksichtigen und abzuwägen haben[128].

Die festgestellte materiell-rechtliche Verpflichtung zur Einhaltung der DSGVO durch die Gerichte sollte mit der Beschwerdemöglichkeit bei einer Aufsichtsbehörde korrelieren. Anderenfalls bleibt den betroffenen Personen nur der Rechtsweg zum Schutz ihrer personenbezogenen Daten.

Artikel 55 Absatz 3 DSGVO stellt die Justiz entsprechend dem genannten Erwägungsgrund von der Aufsicht durch die eingerichteten Aufsichtsbehörden frei. Damit müssen an die datenschutzrechtliche Aufsicht über die Justiz nicht dieselben Anforderungen wie an die Aufsichtsbehörden nach der DSGVO gestellt werden. Im Hinblick auf die richterliche Unabhängigkeit sollten der betrauten Stelle auch nicht dieselben Befugnisse verliehen werden wie den unabhängigen Aufsichtsbehörden nach der DSGVO.

Eine Betrauung setzt einen hoheitlichen Betrauungsakt voraus. Die Einrichtung sollte durch Gesetz erfolgen, da der Gesetzgeber wesentliche Entscheidungen zu treffen hat, nämlich wie den Bürgerinnen und Bürgern ein effizientes Recht auf Beschwerde entsprechend Artikel 79

[128] Vgl. Urteil des EuGH vom 2. März 2023, Rechtssache C-268/21, abrufbar unter CURIA - Dokumente (europa.eu).

DSGVO eingeräumt und zugleich die Unabhängigkeit der Justiz gewahrt werden kann. Welche Aufgaben und Befugnisse einer solchen Aufsichtsbehörde zugewiesen werden sollen, bedarf näherer Untersuchung, die nicht Gegenstand der Evaluierung sein kann.

3. Vorschläge anderer Stellen

Seitens eines Staatlichen Schulamts wird vorgebracht, dass die vom Gesetzgeber verlangten Funktionen bei digitaler Umsetzung einer Internetseite nur schwer durchzuführen seien. Insbesondere sogenannte SSL/TLS Zertifikate für eine HTTPS Verbindung, aber auch die häufig zu erweiternden Cookie Richtlinien, die über Banner auf der Startseite abgefragt werden müssten, könnten Schulen nicht immer realisieren. Eine Befreiung davon für reine „Visitenkartenseiten“ ohne Kontakt- und Abfrageformular würde für überlegenswert gehalten.

Ebenso wird angemerkt, dass objektive Kriterien für Schulleitungen bei der Suche nach datenschutzkonformen Lösungen, z. B. für Fernlernunterricht und zur Nutzung von cloudbasierter Software fehlten. Dies sei für die Schulen unbefriedigend.

- Bewertung des LfDI (S. 72):

Der LfDI entgegnet, dass die angeführten Anforderungen an Websites grundlegende Standards der IT-Sicherheit sowie zum Schutz von Endgeräten vor einer ungewünschten Speicherung von Informationen seien. Diese Standards seien nicht verhandelbar und auch nicht unverhältnismäßig.

Den geschilderten Aufwand für die Prüfung der Datenschutzkonformität digitaler Werkzeuge durch die Schulen hält der LfDI für nachvollziehbar. Die digitale Bildungsplattform, die das Kultusministerium den Schulen anbiete, schaffe hier zum großen Teil Abhilfe. Vorgaben enthielten auch die jüngsten Änderungen im Schulgesetz, die sich mit dem Einsatz digitaler Medien und digitaler „Lehr- und Lernformen“ beschäftigten. Das LDSG sei jedenfalls nicht der richtige Ort für die erbetenen Regelungen. Neben der Unterstützung durch die Datenschutzbeauftragten und das Kultusministerium stehe auch der LfDI beratend und mit angebotenen Fortbildungen den Schulen zur Unterstützung zur Seite.

Position der Landesregierung:

Die Landesregierung sieht das LDSG ebenfalls nicht als den geeigneten Standort für spezifische, den Schulbereich betreffende Regelungen. In das Schulgesetz hat bereits in gewissem Umfang eine spezifische Regelung Eingang gefunden. Weitere Rechtsetzungsverfahren werden sich anschließen. Außerdem steht das Kultusministerium in stetigem Austausch mit dem LfDI und kann daher die Schulen gut unterstützen.

4. Vorschläge des Landtags

a) Fotografien

Der Landtag bittet um Prüfung, ob bei entsprechender Ankündigung der Veranstaltung, bei der fotografiert werden soll, ein Opt-Out-Verfahren zugelassen werden könnte, bei dem diejenigen Personen, die nicht fotografiert werden möchten, dies mitteilten und dann bei den Fotos ausgespart würden, etwa über dezidierte Sitzplätze außerhalb des fotografierten Bereichs. Dies würde es ersparen, aufwändig von jedem Teilnehmer oder jeder Teilnehmerin das Einverständnis abzufragen.

- Bewertung des LfDI (S. 17):

Der LfDI hält ein Opt-Out in diesem Rahmen für keine zulässige Regelung. Von den Anforderungen der DSGVO an die Einwilligung könne nicht abgewichen werden. Die Veranstaltungsfotografie bedürfe auch nicht per se der Einwilligung der betroffenen Personen. In bestimmten Konstellationen, angelehnt an die Regelungen des KunstUrhG könne eine solche auch im Rahmen der Aufgabenerfüllung mit entsprechendem Widerspruchsrecht der betroffenen Personen erfolgen.

Position der Landesregierung:

Wie oben unter § 19 LDSG behandelt, erlaubt § 23 KunstUrhG die Ablichtung auf öffentlichen Veranstaltungen, wenn Personen nur als „Beiwerk“ oder im Rahmen von Übersichtsaufnahmen abgebildet werden. Sofern sich die Veranstaltungsleitung auf die nach dem KunstUrhG zulässigen Fotos beschränkt, bedarf es daher keiner Einwilligung, so dass nur Gelegenheit zum Widerspruch gegeben werden muss.

Dagegen bedürfen Einzelporträts der Einwilligung der betroffenen Person. Hiervon kann auch nicht abgewichen werden.

In dem dazwischenliegenden Spektrum kommt es in Anwendung der Generalklausel des § 4 LDSG jeweils darauf an, ob die Veröffentlichung des Fotos für die Öffentlichkeitsarbeit erforderlich ist oder wegen Eingriffs in die Persönlichkeitsrechte unterbleiben sollte. Hierfür bedarf es der Abwägung im Einzelfall. Das Widerspruchsrecht muss gewahrt bleiben. Im Ergebnis wird eine gesetzliche Regelung für nicht opportun angesehen.

b) Schulungen zur Informationssicherheit

Der Landtag bittet um Berücksichtigung folgenden Sachverhalts: Bei Fortbildungs- und Sensibilisierungsveranstaltungen, die im Interesse der Informationssicherheit regelmäßig durchgeführt werden sollten und müssten, sei es notwendig, für das Informationssicherheitsmanagement Nachweise über die Durchführung und den Erfolg der Maßnahmen zu erzeugen und für ein Sicherheits-Audit bei den Akten vorzuhalten. Betroffen seien neben den Mitarbeitenden der Landtagsverwaltung und solcher aus Fraktionen und Abgeordnetenbüros auch Abgeordnete. Im Einzelfall, etwa zur Vorbereitung und Durchführung von gezielten realitätsnahen Sensibilisierungsmaßnahmen gegenüber Angriffen mit Spear-Phishing-E-Mails, könne auch die Erhebung weiterer personenbezogener Daten im Internet sowie die Übertragung an einen Dienstleister für Sensibilisierungsmaßnahmen erforderlich sein. Der Landtag regt an, für solche der Informationssicherheit dienenden Maßnahmen eine geeignete Rechtsgrundlage zu schaffen.

- Bewertung des LfDI (S. 17f.):

Der LfDI nimmt eine differenzierte Betrachtung nach Nutzergruppen vor. Für Beschäftigte der Landtagsverwaltung könnten die Maßnahmen der Schulungen und Kontrollen auf § 15 Absatz 1 LDSG gestützt werden. Denn als Teil der kritischen Infrastruktur sei der Landtag gemäß Artikel 32 DSGVO zur Gewährleistung angemessener Sicherheit personenbezogener Daten verpflichtet und dürfe die Maßnahmen auch dokumentieren. Für die Gruppe der nicht beim Landtag direkt beschäftigten Nutzerinnen und Nutzer könne eine gesetzliche Grundlage erwogen werden, ebenso wie für Sensibilisierungsmaßnahmen generell.

Position der Landesregierung:

In Bezug auf die Beschäftigten der Landtagsverwaltung wird ebenfalls § 15 LDSG als einschlägig angesehen, da entsprechende Veranstaltungen als Maßnahmen zur Durchführung des Beschäftigungsverhältnisses im Interesse des Dienstherrn, hier der Landtagsverwaltung, erforderlich sein können.

Für die übrigen aufgeführten Personen (Beschäftigte der Fraktionen und Abgeordnete) steht derzeit als Rechtsgrundlage nur die Generalklausel des § 4 in Verbindung mit § 5 LDSG zur Verfügung. Eine Rechtsgrundlage zur Verarbeitung personenbezogener Daten für die Durchführung sicherheitstechnischer Maßnahmen fehlt bisher im Landesrecht. Wie für Maßnahmen zur Öffentlichkeitsarbeit unter § 4 LDSG ausgeführt, ist eine spezielle Rechtsgrundlage vorzuziehen. Diese könnte unter Berücksichtigung der schutzwürdigen Belange der betroffenen

Personen geschaffen werden für Maßnahmen einschließlich Sensibilisierungsmaßnahmen, die aus sicherheitstechnischen Gründen erforderlich sind.

c) Nutzung biometrischer Daten

Der Landtag thematisiert die Absicherung des Zugangs zu informationsverarbeitenden Geräten durch biometrische Methoden wie Fingerabdrucksensor oder Gesichtserkennung. Diese würden derzeit auf freiwilliger Basis optional ergänzend oder als Alternative zur klassischen Authentisierung über Benutzerkennung und Passwort eingesetzt. Es sei zu erwarten, dass in naher Zukunft die Authentifizierung mittels Passwort aus Sicherheitsgründen voraussichtlich nicht mehr zu vertreten sei. Deshalb werde angeregt zu prüfen, ob die rechtlichen Voraussetzungen geschaffen werden könnten, damit biometrische Methoden zur Absicherung des Zugangs zulässig seien, zumindest, soweit damit ein höheres Sicherheitsniveau als mit alternativen Methoden erreicht werden könne, welches aus Sicht des Verantwortlichen angemessen sei.

- Bewertung des LfDI (S. 42):

Der LfDI hält die vorgeschlagene Regelung nicht für erforderlich. Eine Verarbeitung biometrischer Daten komme nur in Betracht, wenn kein gleich wirksames Mittel vorhanden sei, welches das Persönlichkeitsrecht der Beschäftigten weniger stark beeinträchtige. In einer Zwei-Faktor-Authentifizierung sieht der LfDI eine geeignete Alternative, um ohne biometrische Daten hohe Sicherheit zu erreichen. Wenn biometrische Daten entwendet würden, ginge von diese eine höhere Gefahr für die betroffene Person als bei entwendeten Passwörtern aus, da biometrische Daten unveränderbar seien. An eine Verwendung aufgrund Einwilligung, wie in § 15 Absatz 6 LDSG vorgesehen, seien hohe Anforderungen in Bezug auf die Freiwilligkeit der Einwilligung zu stellen.

Position der Landesregierung:

Biometrische Daten unterfallen den besonderen Kategorien personenbezogener Daten, deren Verarbeitung nach Artikel 9 Absatz 1 DSGVO grundsätzlich untersagt ist. Eine Verarbeitung ist nur aufgrund der Ausnahmetatbestände des Artikels 9 Absatz 2 DSGVO in Verbindung mit einer landesrechtlichen Vorschrift zulässig.

Das LDSG regelt in § 15 Absatz 6 als Teil des Beschäftigtendatenschutzes die Verarbeitung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken. Danach ist die Verarbeitung aufgrund einer Einwilligung oder einer Dienst- oder Betriebsvereinbarung zulässig, wenn für beide Alternativen jeweils ein „dringendes dienstliches Bedürfnis“ besteht. Letzteres

ist bei erhöhten Sicherheitsanforderungen nur zu bejahen, wenn derselbe Zweck nicht mit einer Maßnahme erreicht werden kann, die denselben Zweck mit geringerer Eingriffstiefe erfüllt. In die Abwägung wird auch die Schutzbedürftigkeit der mittels der informationsverarbeitenden Geräte oder in speziellen Räumen verarbeiteten Daten einzubeziehen sein. Darüber hinaus sind ggf. spezifische technische und organisatorische Maßnahmen hinsichtlich der Verarbeitung der biometrischen Daten zu treffen.

§ 15 LDSG findet keine Anwendung für die Verarbeitung biometrischer Daten anderer als beschäftigter Personen. Diesbezüglich kann die Verarbeitung biometrischer Daten nach der geltenden Rechtslage nur unter den in § 17 Absatz 2 LDSG genannten engen Voraussetzungen im öffentlichen Interesse zulässig sein[129]. Eine allgemeine Zulassung über die in § 17 Absatz 2 LDSG geregelten Voraussetzungen hinaus wird zum Schutz der betroffenen Personen nicht für zulässig gehalten. Artikel 9 Absatz 4 DSGVO ermächtigt zwar die Mitgliedstaaten, zusätzliche Bedingungen für die Verarbeitung biometrischer Daten einzuführen. Nach Auffassung der überwiegenden Kommentarliteratur ist hier aber an weitere Anforderungen und Beschränkungen, nicht an die Ausdehnung der Verarbeitung gedacht[130].

d) Audio- und Videoüberwachungssysteme

Für die Sicherung von Informationen und informationsverarbeitenden Systemen könnten Audio- und Videoüberwachungssysteme eingesetzt werden, um etwa Rechnerräume oder Serverschränke in Rechnerräumen zu überwachen. Damit könnte überwacht werden, ob eigenes oder fremdes Personal, das für einzelne Komponenten eingesetzt wird, versucht, sich rechtwidrig unberechtigten Zugang zu Informationen oder informationsverarbeitenden Systemen zu verschaffen. Der Landtag bittet um Prüfung der Zulässigkeit einer derartigen Kontrolle im Interesse der Sicherheit.

- Bewertung des LfDI (S. 50):

Der LfDI sieht eine Videoüberwachung für den Schutz von Serverräumen nicht als erforderlich an. Externen sollte der Schutz durch technische Maßnahmen verwehrt werden; im Übrigen könne Zutritt nur unter Aufsicht erlaubt werden. Der Nutzen von Audioaufnahmen sei aus praktischer Sicht nicht zu erkennen. Das Mithören von Gesprächen sei regelmäßig ein unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Personen, wie die Vorschriften über den Lauschangriff im Strafgesetzbuch zeigten.

[129] Vgl. hierzu aber die Ausführungen unter § 17 LDSG.
[130] Vgl. BeckOK DatenschutzR/Albers/Veit DS-GVO Art. 9 Rn. 109-113.

Position der Landesregierung:

Auf die Ausführungen unter § 18 LDSG zur Videoüberwachung in nicht öffentlich zugänglichen Räumen wird verwiesen. Wie dort ausgeführt, steht der Beschäftigtendatenschutz dem generellen Einsatz von Audio- und Videoüberwachungssystemen entgegen. Für fremdes Personal ist eine entsprechende Überwachung im LDSG bisher ebenfalls nicht vorgesehen. Vorab steht aber das Instrument der Zuverlässigkeitsüberprüfung nach § 17 Absatz 1 LDSG zur Verfügung.

Wie bereits ausgeführt, könnte erwogen werden, für sicherheitstechnisch erforderliche Maßnahmen eine Ermächtigungsgrundlage zu schaffen. Der Beschäftigtendatenschutz muss unberührt bleiben.

e) Öffentlichkeitsarbeit

Es wird angeregt, die Öffentlichkeitsarbeit von Behörden explizit gesetzlich zu erlauben, damit das Veranstaltungsmanagement des Landtags sich für die Speicherung von Adressen von Interessenten für die Teilnahme an Veranstaltungen bzw. die Landtagspräsidenten für ihre Weihnachtspost darauf stützen könne.

Dieser Punkt wurde bei den Ausführungen zu § 4 und § 5 LDSG vertieft.

f) Verwendung von Kontaktdaten

In Bezug auf § 15 LDSG regt der Landtag an, eine geeignete Rechtsgrundlage für eine Kommunikation über Parlaments- und Behördengrenzen hinweg und das Vorhalten entsprechender Kontaktdaten zu entwickeln. Wer die Kontaktdaten angebe, willige zwar konkludent in die Kontaktaufnahme ein, aber eine Rechtsgrundlage sei besser als eine Einwilligung.

- Bewertung des LfDI (S. 43):

Der LfDI führt aus, dass ihm die genaue Intention und Stoßrichtung des Vorschlags nicht nachvollziehbar sei. Die Zugänglichmachung sämtlicher Adressbücher von Beschäftigten im öffentlichen Dienst sei schon wegen ihres Umfangs von über 500.000 Personen bedenklich sowie wegen der Verwechslungsgefahr nicht zielführend. Es sei nicht ersichtlich, dass ein Beschäftigter eines Bürgeramts Zugang zu den Kontaktdaten Parlamentsangehöriger haben sollte. Der Grundsatz der Datenminimierung stehe einer derartigen Datenverarbeitung entgegen. Das Vorhalten von Kontaktdaten von Bürgerinnen und Bürgern könne im Umfang der Erforderlichkeit zur Aufgabenerfüllung von § 4 LDSG gedeckt sein.

155

Position der Landesregierung:

Dem LfDI ist zuzustimmen, dass in einer entsprechenden Regelung der Zweck und die Grenzen der Verarbeitung von Kontaktdaten bestimmt werden müssten. Für die an die Verwaltungsnetze angeschlossenen Verwaltungsbehörden und Stellen stehen gemäß § 6 des Landesverwaltungsgesetzes elektronische Verzeichnisse mit den erforderlichen personenbezogenen Daten zu den Bediensteten der Landesverwaltung zur Verfügung. Es bedarf der näheren Prüfung, für welche Aufgaben der Landtag welche Verzeichnisse der Landtag benötigt. Denn eine Datenverarbeitung kommt nur in Frage, soweit diese erforderlich ist.

E. Gesamtbewertung und Schlussfolgerungen

Ziel der Evaluierung war die Untersuchung, ob die im LDSG getroffenen Regelungen den Regelungs- und Gestaltungsspielraum der DSGVO im Hinblick auf Zweckmäßigkeit und Praktikabilität sinnvoll ausnutzen. Dabei waren zum einen die praktischen Bedürfnisse der öffentlichen Stellen zur Verarbeitung personenbezogener Daten, zum anderen die schutzwürdigen Interessen der betroffenen Personen zu berücksichtigen.

Nachfolgend werden die Änderungs- und Ergänzungsvorschläge zusammengefasst aufgeführt:

I. Änderungs- und Ergänzungsvorschläge zum LDSG[131]

- § 2 Absatz 1: Die Definition der verantwortlichen öffentlichen Stelle könnte präzisiert werden.

- § 2 Absatz 3: Der Vorrang der DSGVO sollte zur Klarstellung in das Gesetz aufgenommen werden.

- § 2 Absatz 5: Die Regelung sollte hinsichtlich des Landtags aufgehoben und insoweit eine Neuregelung dem Landtag anheimgestellt werden. Hinsichtlich der Gerichte sollte der Anwendungsbereich erweitert werden.

- § 3 Absatz 1: Die Verpflichtung zu technischen und organisatorischen Maßnahmen ist zur Sicherstellung des Datenschutzes herauszustellen. Zur Verarbeitung besonderer Kategorien personenbezogener Daten bedarf es spezifischer Regelungen.

- §§ 4 bis 6: Die Systematik der Vorschriften könnte klarer gestellt werden.

- § 4: Zulässigkeit der Verarbeitung personenbezogener Daten:
  - Das LDSG sollte um eine Rechtsgrundlage für die Öffentlichkeitsarbeit ergänzt werden.
  - § 4 sollte für eine Regelung zur Verwendung und zum Training von KI einschließlich der Verwendung vorhandener Daten hierfür erweitert werden.

- § 5 Absatz 1 Nummer 1: Der Gemeinwohlbegriff sollte präzisiert werden.

[131] Die in diesem Abschnitt genannten Paragrafen beziehen sich ohne Gesetzesbezeichnung auf das LDSG.

- § 5 Absatz 1 Nummer 3: Die Vorschrift sollte präziser gefasst werden sowie die Verfolgung von Ordnungswidrigkeiten generell ermöglicht werden.

- § 5: Ein weiterer Zweckänderungstatbestand wird vorgeschlagen für die Verwendung von Daten, insbesondere Adressdaten für politische Arbeit.

- § 6: Für die Übermittlung personenbezogener Daten an den Landtag sollte eine spezifische Rechtsgrundlage angefügt werden.

- § 6: Für die Übermittlung personenbezogener Daten an ausländische Stellen innerhalb der EU sowie des Europäischen Wirtschaftsraums und an die Organe der EU könnte klarstellend eine Norm eingefügt werden.

- § 6 Absatz 1 Nummer 1: Hier sollte klargestellt werden, dass auch die Übermittlung an nichtöffentliche Stellen erfasst ist.

- § 6 Absatz 1 Nummer 2, zweiter Halbsatz: Zur sprachlichen Bereinigung wird die Streichung vorgeschlagen.

- § 6 Absatz 1: Als dritte Variante könnte zur Klarstellung eine Rechtsgrundlage für die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche eingefügt werden.

- § 6 Absatz 2: Die Regelung sollte gestrichen werden. Die Übermittlung von Daten auf Ersuchen sollte in Absatz 3 integriert werden.

- § 6 Absatz 3: Eine Regelung zu den Voraussetzungen für Abrufverfahren und regelmäßige Datenübermittlungen sollte die Einführung solcher Verfahren auf eine sichere Grundlage stellen.

- § 8: Die Einfügung spezifischer Vorschriften gemäß Artikel 23 Absatz 2 DSGVO wird für notwendig erachtet. Hierfür wird eine Regelung entsprechend § 32 Absatz 2 und 3 BDSG empfohlen.

- § 13: Zur Angleichung an die Regelung im Bundesdatenschutzgesetz sollte die „Erforderlichkeit“ als Tatbestandsvoraussetzung eingeführt werden, um die gemeinsame Forschung mit Einrichtungen des Bundes und der Länder, die sich am Bund orientiert haben, zu erleichtern.

- § 13: Vorhandene Daten sowie allgemein zugängliche Daten sollten für Zwecke gemeinwohlorientierter Forschung (weiter-)verarbeitet werden dürfen, soweit dies für den Forschungszweck erforderlich ist.

- § 13: Die Forschungsregelung könnte um einen Katalog der vereinbaren Zwecke ergänzt werden, um die Gemeinwohlorientierung herauszustellen.

- § 13: In der Regelung sollte außerdem klargestellt werden, dass zu Gemeinwohlzwecken auch die Übermittlung an privatwirtschaftliche Empfänger zur Weiterverarbeitung zu Forschungszwecken zulässig ist.

- § 13 Absatz 3: Die Zulässigkeit der Veröffentlichung könnte um eine Regelung erweitert werden, mit der die Veröffentlichung personenbezogener Daten, sofern sie zur Einhaltung der guten wissenschaftlichen Praxis erforderlich ist, zugelassen wird. Dabei dürfen schutzwürdige Interessen der betroffenen Person nicht erheblich beeinträchtigt werden.

- § 15 Absatz 2: Die Zwecke der Gesundheitsvorsorge und der Arbeitsmedizin sollten zusätzlich aufgenommen werden.

- § 15 Absatz 6: Es werden Klarstellungen empfohlen, um zu verdeutlichen, dass die Verarbeitung biometrischer Daten zur Authentifizierung nur zulässig sein sollte, wenn keine milderen Mittel zur Verfügung stehen.

- § 16: Die Nichtanwendbarkeit bei einem vorliegenden Widerspruch könnte klarstellend eingefügt werden.

- § 17 Absatz 2: Zur Sicherstellung des Datenschutzes sind für die Verarbeitung besonderer Kategorien personenbezogener Daten im öffentlichen Interesse spezifische Regelungen zu treffen. Ggf. sollte die Vorschrift in eine eigene Vorschrift überführt werden.

- § 18 Absatz 1: Es wird vorgeschlagen, die Videoüberwachung als generell geeignetes Mittel zuzulassen, wenn andere Mittel einen unverhältnismäßigen Aufwand erfordern würden oder für die Aufgabenerfüllung nicht geeignet sind. Damit würde die Vorrangprüfung anderer Mittel erleichtert. Die Einbeziehung oder der Ausschluss von KI-Systemen auf Basis von Videotechnologie im öffentlichen Raum, die nicht primär Polizei- oder Ordnungsrecht dienen, ist zu prüfen.

- § 18 Absatz 2: Durch Präzisierung der Informationspflicht sollte für mehr Transparenz gesorgt werden.

- § 18 Absatz 4: Die Regelung sollte gestrichen werden. Die Informationspflicht richtet sich nach der DSGVO.

- § 26: Die Regelung könnte um Untersuchungsbefugnisse des LfDI in Privaträumen unter strengen Voraussetzungen ergänzt werden.

Zur Ergänzung des LDSG werden folgende Regelungen vorgeschlagen:

- Die Möglichkeit zur Beauftragung der Auftragsverarbeitung durch die Fachaufsichtsbehörde wird für sinnvoll erachtet.

- Zur Erleichterung und Vereinheitlichung von Auftragsverarbeitungen sollte für eine gesetzliche Grundlage für die Beauftragung eines Dienstleisters oder in anderer Weise für standardisierte Bedingungen anstelle individueller vertraglicher Vereinbarungen gesorgt werden.

- Eine Regelung zur Videoüberwachung in nicht öffentlich zugänglichen Bereichen würde zur Klarstellung beitragen.

- Möglich wäre die Einführung eines Rechtsbehelfs für den LfDI, und zwar in Form der Zulassung eines In-Sich-Prozesses zwischen einer öffentlichen Stelle und dem LfDI.

- Für eine Ermächtigungsgrundlage für sicherheitstechnisch erforderliche Maßnahmen wurde ein Bedarf festgestellt.

- Die Einbeziehung des Personals des LfDI in den allgemeinen Personalaustausch der Landesverwaltung sollte Berücksichtigung finden.

- Die Aufsichtszuständigkeit des LfDI in Bezug auf die Überwachung der datenschutzrechtlichen Pflichten nach dem TDDDG könnte explizit aufgenommen werden.

II. Schlussfolgerungen

Die Landesregierung legt dem Landtag den Abschlussbericht zur Evaluierung des LDSG mit den Stellungnahmen des LfDI und der kommunalen Landesverbände vor.

Soweit ein Änderungsbedarf festgestellt oder Klarstellungen und Ergänzungen empfohlen wurden, schlägt die Landesregierung ein Gesetzgebungsverfahren zur Modernisierung des LDSG vor.

160

Anlagen

Anlage 1:	Landesdatenschutzgesetz
Anlage 2:	Stellungnahme des LfDI vom 6. November 2020
Anlage 3:	Stellungnahme des LfDI vom 13. Februar 2024
Anlage 4:	Stellungnahme des Rundfunkbeauftragten für den Datenschutz vom 30. Oktober 2020
Anlage 5:	Gemeinsame Stellungnahme des Gemeindetags und des Landkreistags vom 29. Oktober 2021

Literaturverzeichnis

Debus / Sicko (Hrsg.)	Landesdatenschutzgesetz Baden-Württemberg, 1. Auflage 2022
Ehmann / Selmayr	Datenschutz-Grundverordnung, 2017
Gola / Heckmann	Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022 in beck-online
Kühling / Buchner	Datenschutz-Grundverordnung – BDSG, 3. Auflage 2020
Beck´scher Online-Kommentar, Wolff / Brink / v. Ungern-Sternberg	Datenschutzrecht 47. Edition
Paal / Pauly	Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Auflage 2018

Anlage 2

Gesamtes Gesetz

Amtliche Abkürzung:	LDSG	**Quelle:**	
Ausfertigungsdatum:	12.06.2018		
Gültig ab:	21.06.2018	**Fundstelle:**	GBl. 2018, 173
Dokumenttyp:	Gesetz	**Gliederungs-Nr:**	2040

Landesdatenschutzgesetz (LDSG)

Vom 12. Juni 2018 *)

Zum 10.02.2022 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: letzte berücksichtigte Änderung: § 23 geändert durch Art. 3 des Gesetzes vom 18. Dezember 2018 (GBl. S. 1549, 1551)

Fußnoten

* Verkündet als Artikel 1 des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 vom 12. Juni 2018 (GBl. S. 173)

INHALTSÜBERSICHT

ABSCHNITT 1
Allgemeine Bestimmungen

§ 1
Zweck des Gesetzes

Dieses Gesetz trifft ergänzende Regelungen zur Durchführung der 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) (ABl. L 119 vom 4. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) in der jeweils geltenden Fassung sowie Regelungen für die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

§ 2
Anwendungsbereich

(1) Dieses Gesetz gilt nach Maßgabe von Absatz 2 bis 7 für die Verarbeitung personenbezogener Daten durch Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen). Die öffentliche Stelle ist zugleich Verantwortlicher nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit dieses Gesetz nichts anderes bestimmt. Dieses Gesetz gilt nicht für die Verarbeitung personenbezogener Daten

1. durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes,

2. beim Vollzug des Landessicherheitsüberprüfungsgesetzes,

3. durch die Polizei sowie die Gerichte, Staatsanwaltschaften, das Justizministerium und die Justizvollzugsbehörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit und

4. durch andere für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständige Stellen,

soweit besondere Rechtsvorschriften keine abweichenden Regelungen treffen. § 30 gilt auch für die Verarbeitung personenbezogener Daten nach Satz 3.

(2) Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts nach Satz 1 an einer weiteren Vereinigung des privaten Rechts, findet Satz 1 entsprechende Anwendung. Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

(3) Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Vorschriften dieses Gesetzes gehen denen des Landesverwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) Soweit die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit stattfindet, die nicht in den sachlichen Anwendungsbereich der Verordnung (EU) 2016/679 oder der 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 (ABl. L 119 vom 4. Mai 2016, S. 89) fällt, gelten die Regelungen der Verordnung (EU) 2016/679 und dieses Gesetz entsprechend, sofern die Verarbeitung nicht in besonderen Rechtsvorschriften geregelt ist. Die Artikel 30, 35 und 36 der Verordnung (EU) 2016/679 gelten nur, soweit die Verarbeitung personenbezogener Daten automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Auf die Prüfungstätigkeit des Rechnungshofs und der staatlichen Rechnungsprüfungsämter finden Artikel 30 und Kapitel VI der Verordnung (EU) 2016/679 sowie §§ 25 und 26 dieses Gesetzes keine Anwendung.

(5) Dieses Gesetz gilt für den Landtag sowie unbeschadet des Absatz 1 Nummer 3 für die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(6) Soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, sind die für nichtöffentliche Stellen geltenden datenschutzrechtlichen Vorschriften entsprechend anzuwenden. Satz 1 gilt nicht für Zweckverbände.

(7) Die Vorschriften dieses Gesetzes gelten nicht für die Verarbeitung personenbezogener Daten zur Ausübung des Begnadigungsrechts.

§ 3
Sicherstellung des Datenschutzes

(1) Bei der Datenverarbeitung sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Zu den Maßnahmen können insbesondere gehören:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung [EU] 2016/679 erfolgt,

2. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind,

3. die Sensibilisierung und Schulung der an Verarbeitungsvorgängen Beteiligten,

4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern,

5. die Pseudonymisierung personenbezogener Daten,

6. die Verschlüsselung personenbezogener Daten,

7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und

9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung [EU] 2016/679 sicherstellen.

(2) Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Das Datengeheimnis besteht nach Beendigung ihrer Tätigkeit fort.

ABSCHNITT 2
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 4
Zulässigkeit der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist.

§ 5
Datenverarbeitung zu anderen Zwecken

(Ergänzung zu Artikel 6 Absatz 3 und 4 der Verordnung [EU] 2016/679)

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist unbeschadet der Bestimmungen der Verordnung [EU] 2016/679 zulässig, wenn

1. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,

2. sie zum Schutz der betroffenen Person oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist,

3. sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung ergeben und die Unterrichtung der für die Verhütung, Verfolgung oder Vollstreckung zuständigen Behörden erforderlich ist oder

4. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

soweit die Verarbeitung notwendig und verhältnismäßig ist.

(2) Eine Verarbeitung gilt als mit den ursprünglichen Zwecken vereinbar, wenn sie

1. für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen benötigt wird oder

2. der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen oder der Prüfung und Wartung von automatisierten Verfahren dient.

Dies gilt auch für die Verarbeitung zu eigenen Aus- und Fortbildungszwecken, soweit schutzwürdige Belange der betroffenen Person nicht entgegenstehen.

(3) Abweichend von Artikel 13 der Verordnung [EU] 2016/679 erfolgt eine Information der betroffenen Person über die Datenverarbeitung nach Absatz 1 Nummern 1 bis 4 nicht, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde und die Interessen der öffentlichen Stelle an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

(4) Personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage verarbeitet werden, dürfen nur für diesen Zweck und hiermit in Zusammenhang stehende Maßnahmen gegenüber Beschäftigten verarbeitet werden oder soweit dies zur Verhütung oder Verfolgung von Straftaten gegen Leib, Leben oder Freiheit einer Person erforderlich ist.

§ 6
Übermittlung personenbezogener Daten

(1) Die Übermittlung personenbezogener Daten zu anderen als ihren Erhebungszwecken ist zulässig, wenn

1. sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 5 zulassen würden oder

2. der Empfänger eine nichtöffentliche Stelle ist, die ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; dies gilt auch, soweit die Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden, übermittelt werden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde öffentliche Stelle. Erfolgt die Übermittlung an eine öffentliche Stelle im Geltungsbereich des Grundgesetzes auf deren Ersuchen, trägt diese die Verantwortung und erteilt die Informationen nach Artikel 14 der Verordnung [EU] 2016/679. Die übermittelnde öffentliche Stelle hat im Falle des Satzes 2 lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden öffentlichen Stelle liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht.

(3) Erfolgt die Übermittlung aufgrund eines automatisierten Verfahrens, welches die Übermittlung personenbezogener Daten durch Abruf ermöglicht, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Dritte, an den übermittelt wird. Die übermittelnde Stelle prüft die Zulässigkeit des Abrufs nur, wenn dazu Anlass besteht. Sie hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

§ 7
Datenverarbeitung in der gemeinsamen Dienststelle

(1) Die örtlich zuständige öffentliche Stelle darf personenbezogene Daten nur den in einer gemeinsamen Dienststelle nach § 16 Absatz 1 des Landesverwaltungsgesetzes beschäftigten eigenen Bediensteten zur Verarbeitung für eigene Aufgaben überlassen. Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass ein Zugriff auf die Daten nach Satz 1 durch Bedienstete anderer Behörden nicht möglich ist. Soweit dies zur Sicherstellung einer sachgerechten Erledigung der eigenen Aufgaben erforderlich ist, darf die örtlich zuständige öffentliche Stelle auch Bediensteten anderer Behörden, die in der gemeinsamen Dienststelle beschäftigt sind, personenbezogene Daten zur Verarbeitung überlassen. Im Rahmen einer solchen Datenverarbeitung unterliegen die Bediensteten anderer Behörden den Weisungen der örtlich zuständigen öffentlichen Stelle. Hinsichtlich der Daten, die sie im Rahmen ihrer Tätigkeit für die fremde Behörde zur Kenntnis nehmen, haben sie das Datengeheimnis gegenüber ihrer ei-

genen Dienststelle zu wahren. Das Nähere ist durch gemeinsame interne Dienstanweisungen zu regeln. Verantwortlicher bleibt die örtlich zuständige öffentliche Stelle.

(2) Für gemeinsame Dienststellen nach § 27 des Gesetzes über kommunale Zusammenarbeit gilt Absatz 1 entsprechend.

ABSCHNITT 3
Rechte der betroffenen Person

§ 8
Beschränkung der Informationspflicht

(Ergänzung zu Artikel 13 und 14 der Verordnung [EU] 2016/679)

(1) Eine Pflicht zur Information der betroffenen Person besteht nicht, soweit und solange

1. die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

2. die Information die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung gefährden würde,

3. die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde,

4. die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte und Freiheiten anderer Personen geheim gehalten werden müssen oder

5. die Information voraussichtlich die Verwirklichung des wissenschaftlichen oder historischen Forschungszwecks unmöglich macht oder ernsthaft beeinträchtigt

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

(2) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten an Staatsanwaltschaften, Polizeibehörden oder den Polizeivollzugsdienst, Verfassungsschutzbehörden und, soweit sie in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung personenbezogene Daten speichern, an Behörden der Finanzverwaltung, ist diesen Behörden vorab Gelegenheit zur Stellungnahme zu geben. Satz 1 findet auch Anwendung auf die Übermittlung personenbezogener Daten an den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, an andere Behörden des Bundesministers der Verteidigung. Satz 1 und 2 gelten entsprechend für die Information über die Herkunft der Daten von den genannten Behörden.

(3) Die Gründe für das Absehen von der Information sind zu dokumentieren.

§ 9
Beschränkung des Auskunftsrechts

(Ergänzung zu Artikel 15 der Verordnung [EU] 2016/679)

(1) Die Auskunftserteilung kann aus den in § 8 Absatz 1 Nummern 1 bis 4 genannten Gründen abgelehnt werden. Die betroffene Person kann ferner keine Auskunft verlangen, soweit und solange die personenbezogenen Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

(2) Sofern die öffentliche Stelle eine große Menge von Informationen über die betroffene Person verarbeitet, kann sie sich auf die Benennung der Verarbeitungsvorgänge und der Art der verarbeiteten Daten beschränken, wenn sie im Übrigen von der betroffenen Person eine Präzisierung verlangt, auf welche In-

formation oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht. Kommt die betroffene Person dem Verlangen nicht nach, kann die Auskunft verweigert werden, soweit die Auskunftserteilung einen unzumutbaren Aufwand auslösen würde.

(3) § 8 Absatz 2 gilt entsprechend.

(4) Die Ablehnung der Auskunftserteilung ist zu begründen, es sei denn, durch die Mitteilung der Gründe würde der mit der Auskunftsverweigerung verfolgte Zweck gefährdet. In diesem Fall sind die Gründe der Auskunftsverweigerung zu dokumentieren. Die betroffene Person ist auf die Möglichkeit der Beschwerde bei der oder dem Landesbeauftragten für den Datenschutz hinzuweisen.

(5) Wird der betroffenen Person keine Auskunft erteilt, ist sie auf ihr Verlangen der oder dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Landesbeauftragten für den Datenschutz an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand der öffentlichen Stelle zulassen, sofern diese nicht einer weiter gehenden Auskunft zustimmt.

§ 10
Beschränkung des Rechts auf Löschung

(Ergänzung zu Artikel 17 der Verordnung [EU] 2016/679)

(1) Die Bestimmungen des Landesarchivgesetzes zur Anbietungspflicht sowie sonstige gesetzliche oder satzungsmäßige Dokumentations- und Aufbewahrungspflichten bleiben unberührt.

(2) Die Pflicht zur Löschung personenbezogener Daten nach Artikel 17 der Verordnung [EU] 2016/679 besteht nicht, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel 18 der Verordnung [EU] 2016/679. Die öffentliche Stelle unterrichtet die betroffene Person über das Absehen von der Löschung und die Einschränkung der Verarbeitung. Widerspricht die betroffene Person dem Absehen von der Löschung, sind die Daten zu löschen.

(3) Ist eine Löschung im Falle nichtautomatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht der öffentlichen Stelle zur Löschung personenbezogener Daten nicht. In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel 18 der Verordnung [EU] 2016/679. Satz 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

§ 11
Beschränkung der Benachrichtigungspflicht

(Ergänzung zu Artikel 34 der Verordnung [EU] 2016/679)

Die öffentliche Stelle kann von der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person absehen, soweit und solange

1. die Benachrichtigung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

2. die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte anderer Personen geheim gehalten werden müssen oder

3. die Benachrichtigung die Sicherheit von Systemen der Informationstechnologie gefährden würde

und deswegen das Interesse der betroffenen Person an der Benachrichtigung zurücktreten muss.

ABSCHNITT 4

Besondere Verarbeitungssituationen

§ 12
Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die der öffentlichen Stelle in Ausübung einer Berufs- oder Amtspflicht übermittelt worden sind, dürfen von der öffentlichen Stelle nur für den Zweck verarbeitet werden, für den sie die Daten erhalten hat. Artikel 9 der Verordnung (EU) 2016/679 bleibt unberührt.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet werden, wenn

1. die Änderung des Zwecks durch besonderes Gesetz zugelassen ist oder

2. die Voraussetzungen des § 5 Absatz 1 Nummern 1 bis 3, § 13 Absatz 1 oder § 14 Absatz 1 vorliegen und die zur Verschwiegenheit verpflichtete Stelle zugestimmt hat.

§ 13
Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Öffentliche Stellen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können und die Interessen der öffentlichen Stelle an der Durchführung des Forschungs- oder Statistikvorhabens die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. Besondere Kategorien personenbezogener Daten sind die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 genannten Daten.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis zur Anonymisierung sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(3) Die wissenschaftliche oder historische Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten außer bei Einwilligung nur veröffentlichen, soweit dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(4) Die in Artikel 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der jeweiligen Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der jeweiligen Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

§ 14
Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist.

(2) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben

gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(3) Das Recht auf Berichtigung der betroffenen Person gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

(4) Die in Artikel 18, 19, 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

(5) Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, ist eine Löschung erst zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten und von diesem nicht als archivwürdig übernommen worden sind oder über die Übernahme nicht innerhalb der gesetzlichen Frist entschieden worden ist.

§ 15
Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Personenbezogene Daten von Bewerberinnen und Bewerbern sowie Beschäftigten dürfen verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des jeweiligen Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlich planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich oder in einer Rechtsvorschrift, einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung (Kollektivvereinbarung) vorgesehen ist. Die Verarbeitung ist auch zulässig, wenn sie zur Ausübung oder Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

(2) Besondere Kategorien personenbezogener Daten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit die Verarbeitung erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen oder der betroffenen Person, auch aufgrund von Kollektivvereinbarungen, auf dem Gebiet des Dienst- und Arbeitsrechts sowie des Rechts der sozialen Sicherheit und des Sozialschutzes zu genügen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

(3) Im Zusammenhang mit der Begründung eines Dienst- oder Arbeitsverhältnisses ist die Erhebung personenbezogener Daten einer Bewerberin oder eines Bewerbers bei dem bisherigen Dienstherrn oder Arbeitgeber nur zulässig, wenn die betroffene Person eingewilligt hat. Satz 1 gilt entsprechend für die Übermittlung personenbezogener Daten an künftige Dienstherren oder Arbeitgeber.

(4) Auf die Verarbeitung von Personalaktendaten von Arbeitnehmerinnen und Arbeitnehmern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis finden die für Beamtinnen und Beamte geltenden Vorschriften des § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbeamtengesetzes entsprechende Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor.

(5) Zur Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat oder schwerwiegende Pflichtverletzung begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(6) Die Verarbeitung biometrischer Daten von Beschäftigten zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, die betroffene Person hat ausdrücklich eingewilligt oder sie ist durch Dienst- oder Betriebsvereinbarung geregelt und für die Datenverarbeitung besteht jeweils ein dringendes dienstliches Bedürfnis.

(7) Eine Überwachung von Beschäftigten mit Hilfe optisch-elektronischer Einrichtungen zum Zwecke der Verhaltens- und Leistungskontrolle ist unzulässig. Absatz 5 bleibt unberührt. Für sonstige technische Einrichtungen gilt Absatz 1 entsprechend; die öffentliche Stelle muss geeignete Maßnahmen treffen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(8) Beschäftigte sind alle bei öffentlichen Stellen beschäftigten Personen unabhängig von der Rechtsform des Beschäftigungsverhältnisses. Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

§ 16
Öffentliche Auszeichnungen und Ehrungen

(1) Zur Entscheidung über öffentliche Auszeichnungen und Ehrungen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten verarbeitet werden; die öffentlichen Stellen sind insofern nicht zur Informations- und Auskunftserteilung gemäß Artikel 13 bis 15 der Verordnung (EU) 2016/679 verpflichtet.

(2) Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden, es sei denn, sie werden für protokollarische Zwecke benötigt.

§ 17
Verarbeitung personenbezogener Daten im öffentlichen Interesse

(1) Für die Überprüfung der Zuverlässigkeit von Besuchern, Mitarbeitern von Unternehmen und anderen Organisationen sowie sonstigen Personen, die in sicherheits- oder sicherheitstechnisch relevante Bereiche gelangen sollen, für die öffentliche Stellen Verantwortung tragen, gilt § 15 Absatz 1 Satz 1 entsprechend mit der Maßgabe, dass zusätzlich die Einwilligung der betroffenen Person erforderlich ist. Besondere Kategorien personenbezogener Daten sowie Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln dürfen nur aufgrund einer ausdrücklichen Einwilligung verarbeitet werden.

(2) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, wenn die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses oder zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist und die Interessen der öffentlichen Stelle an der Datenverarbeitung die Interessen der betroffenen Person überwiegen.

§ 18
Videoüberwachung öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist,

1. um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich in öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder

2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen

zu schützen und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.

(2) Die Videoüberwachung ist durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen; dabei ist der Verantwortliche mitzuteilen.

(3) Für einen anderen Zweck dürfen die Daten nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, besteht die Pflicht zur Information der betroffenen Person über diese Verarbeitung nach Artikel 13 und 14 der Verordnung (EU) 2016/679. § 8 gilt entsprechend.

(5) Die Videoaufzeichnungen und daraus gefertigte oder sich auf die Videoüberwachung beziehende Unterlagen sind unverzüglich, spätestens jedoch vier Wochen nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.

(6) Öffentliche Stellen haben ihren jeweiligen Datenschutzbeauftragten unbeschadet des Artikels 35 Absatz 2 der Verordnung (EU) 2016/679 rechtzeitig vor dem erstmaligen Einsatz einer Videoüberwachungseinrichtung den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, den betroffenen Personenkreis, die Maßnahmen nach Absatz 2 und die vorgesehenen Auswertungen mitzuteilen und ihm Gelegenheit zur Stellungnahme zu geben.

§ 19
Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken

(1) Werden personenbezogene Daten zu künstlerischen und literarischen Zwecken verarbeitet, gelten neben Absatz 2 und 3 nur Artikel 5 Absatz 1 Buchstabe f in Verbindung mit Absatz 2, Artikel 24 und 32, sowie Kapitel I, VI, VIII, X und XI der Verordnung (EU) 2016/679. Artikel 82 der Verordnung (EU) 2016/679 gilt mit der Maßgabe, dass nur für unzureichende Maßnahmen nach Artikel 5 Absatz 1 Buchstabe f, Artikel 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird. Den betroffenen Personen stehen nur die in Absatz 2 und 3 genannten Rechte zu.

(2) Führt die künstlerische oder literarische Offenlegung oder Verbreitung personenbezogener Daten zu hierauf bezogenen Maßnahmen wie Gegendarstellungen, Verpflichtungserklärungen, Gerichtsentscheidungen oder Widerrufen sind diese Maßnahmen zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst und bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

(3) Wird jemand durch die künstlerische oder literarische Offenlegung oder Verbreitung personenbezogener Daten in seinem Persönlichkeitsrecht beeinträchtigt, kann er Auskunft über die zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen.

ABSCHNITT 5
Unabhängige Aufsichtsbehörden

§ 20
Errichtung

(1) Die oder der Landesbeauftragte für den Datenschutz ist eine unabhängige, nur dem Gesetz unterworfene oberste Landesbehörde. Der Dienstsitz ist Stuttgart.

(2) Die oder der Landesbeauftragte für den Datenschutz ist Dienstvorgesetzte oder Dienstvorgesetzter der Beamtinnen und Beamten der Behörde. Die Beschäftigten der oder des Landesbeauftragten für den Datenschutz sind ausschließlich an ihre oder seine Weisungen gebunden.

(3) Die oder der Landesbeauftragte für den Datenschutz kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Landes übertragen, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist. Die Aufgabenübertragung nach Satz 1 kann nur im Einvernehmen mit der anderen Stelle erfolgen.

§ 21
Unabhängigkeit

(1) Die oder der Landesbeauftragte für den Datenschutz handelt bei der Erfüllung ihrer oder seiner Aufgaben und bei der Ausübung ihrer oder seiner Befugnisse völlig unabhängig.

(2) Die oder der Landesbeauftragte für den Datenschutz unterliegt der Rechnungsprüfung durch den Rechnungshof, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

(3) Die Abgeordneten des Landtags sind berechtigt, Anfragen an die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz zu richten, zu deren Beantwortung diese oder dieser nur verpflichtet ist, soweit hierdurch nicht ihre oder seine Unabhängigkeit beeinträchtigt wird.

§ 22
Ernennung und Amtszeit

(1) Der Landtag wählt ohne Aussprache auf Vorschlag der Landesregierung mit der Mehrheit seiner Mitglieder die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz. Diese oder dieser soll neben der erforderlichen Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten die Befähigung zum Richteramt oder zum höheren Verwaltungsdienst haben oder für eine andere Laufbahn des höheren Dienstes befähigt sein.

(2) Die oder der Gewählte wird von der Landtagspräsidentin oder dem Landtagspräsidenten ernannt. Sie oder er wird vor dem Landtag auf das Amt verpflichtet.

(3) Die Amtszeit der oder des Landesbeauftragten für den Datenschutz beträgt sechs Jahre. Die zweimalige Wiederwahl ist zulässig.

§ 23
Amtsverhältnis

(1) Die oder der Landesbeauftragte für den Datenschutz steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis zum Land.

(2) Die Landtagspräsidentin oder der Landtagspräsident kann die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz ihres oder seines Amtes entheben, wenn diese oder dieser eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Die Amtsenthebung bedarf der Zustimmung von zwei Dritteln der Mitglieder des Landtags. Die Amtsenthebung wird mit der Zustellung der Urkunde durch die Landtagspräsidentin oder den Landtagspräsidenten wirksam.

(3) Die Leitende Beamtin oder der Leitende Beamte der Dienststelle der oder des Landesbeauftragten für den Datenschutz nimmt die Rechte und Pflichten der oder des Landesbeauftragten für den Datenschutz wahr, wenn die oder der Landesbeauftragte für den Datenschutz an der Ausübung ihres oder seines Amtes verhindert ist oder wenn ihr oder sein Amtsverhältnis geendet hat. § 21 Absatz 1 gilt in den genannten Fällen entsprechend.

(4) Die oder der Landesbeauftragte für den Datenschutz erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, Bezüge in Höhe des Grundgehalts der Besoldungsgruppe B 6. Daneben werden der Familienzuschlag sowie sonstige Besoldungsbestandteile, Trennungsgeld, Reisekostenvergütung, Umzugskostenvergütung und Beihilfen in Krankheits-, Geburts- oder Todesfällen in sinngemäßer Anwendung der für Beamtinnen und Beamte geltenden Vorschriften gewährt.

(5) Die oder der Landesbeauftragte für den Datenschutz erhält nach dem Ausscheiden aus dem Amt Versorgungsbezüge in sinngemäßer Anwendung der für Beamtinnen und Beamte geltenden Vorschriften.

§ 24
Rechte und Pflichten

(1) Die oder der Landesbeauftragte für den Datenschutz hat von allen mit den Aufgaben ihres oder seines Amtes nicht zu vereinbarenden Handlungen abzusehen und während ihrer oder seiner Amtszeit keine andere mit ihrem oder seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit auszuüben. Insbesondere darf die oder der Landesbeauftragte für den Datenschutz neben ihrem oder seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung, dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Sie oder er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(2) Die oder der Landesbeauftragte für den Datenschutz hat der Landtagspräsidentin oder dem Landtagspräsidenten Mitteilung über Geschenke zu machen, die sie oder er in Bezug auf das Amt erhält. Die Landtagspräsidentin oder der Landtagspräsident entscheidet über die Verwendung der Geschenke; sie oder er kann Verfahrensvorschriften erlassen.

(3) Die oder der Landesbeauftragte für den Datenschutz ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die oder der Landesbeauftragte für den Datenschutz entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie oder er oder ihre oder seine Beschäftigten über solche Angelegenheiten vor Gericht oder außergerichtlich aussagen oder Erklärungen abgeben. Wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Landesbeauftragten für den Datenschutz erforderlich. Satz 1, 2 und 4 gelten entsprechend für die Beschäftigten der oder des Landesbeauftragten für den Datenschutz nach Beendigung ihrer Tätigkeit bei ihrer oder seiner Dienststelle.

(4) Die oder der Landesbeauftragte für den Datenschutz hat für die Dauer von zwei Jahren nach der Beendigung ihrer oder seiner Amtszeit von allen mit den Aufgaben ihres oder seines früheren Amtes nicht zu vereinbarenden Handlungen und entgeltlichen oder unentgeltlichen Tätigkeiten abzusehen.

(5) Die oder der Landesbeauftragte für den Datenschutz darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde dem Wohle des Bundes oder eines Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder ihre Beziehungen zu anderen Staaten, oder Grundrechte verletzen. Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Landesregierung zuzurechnen sind oder sein könnten, darf die oder der Landesbeauftragte für den Datenschutz nur im Benehmen mit der Landesregierung aussagen.

§ 25
Aufgaben und Befugnisse

(1) Die oder der Landesbeauftragte für den Datenschutz ist zuständige Aufsichtsbehörde im Sinne des Artikels 51 Absatz 1 der Verordnung (EU) 2016/679 im Geltungsbereich dieses Gesetzes, es sei denn, besondere Vorschriften regeln eine andere Zuständigkeit. Sie oder er ist zugleich Aufsichtsbehörde für den Datenschutz für nichtöffentliche Stellen nach § 40 des Bundesdatenschutzgesetzes.

(2) Die oder der Landesbeauftragte für den Datenschutz nimmt auch im Anwendungsbereich des § 2 Absatz 4 die Aufgaben gemäß Artikel 57 der Verordnung (EU) 2016/679 wahr und übt die Befugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 aus. Bei den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie bei den in § 2 Absatz 2 genannten Stellen ist das vertretungsberechtigte Organ der Verantwortliche.

(3) Jede oder jeder kann sich an die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz wenden, wenn sie oder er der Ansicht ist, bei der Verarbeitung ihrer oder seiner personenbezogenen Daten durch eine öffentliche Stelle in ihren oder seinen Rechten verletzt worden zu sein. Wer von seinem Recht nach Satz 1 Gebrauch gemacht hat, darf aus diesem Grund nicht benachteiligt oder gemaßregelt werden.

(4) Stellt die oder der Landesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, teilt sie oder er dies bei den öffentlichen Stellen des Landes der zuständigen Rechts- oder Fachaufsichtsbehörde mit und gibt dieser vor Ausübung der Befugnisse des Artikels 58 Absatz 2 Buchstaben b bis g und j der Verordnung (EU) 2016/679 Gelegenheit

zur Stellungnahme innerhalb einer angemessenen Frist. Bei den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie den in § 2 Absatz 2 genannten Stellen tritt an die Stelle der Rechts- und Fachaufsichtsbehörde das vertretungsberechtigte Organ; zugleich unterrichtet die oder der Landesbeauftragte für den Datenschutz die zuständige Aufsichtsbehörde. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Landesbeauftragten für den Datenschutz getroffen worden oder beabsichtigt sind.

(5) § 29 Absatz 3 des Bundesdatenschutzgesetzes bleibt unberührt und gilt entsprechend für die Notarinnen und Notare des Landes. Im Übrigen erstreckt sich die Kontrolle der oder des Landesbeauftragten für den Datenschutz auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Erlangt die oder der Landesbeauftragte für den Datenschutz im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht unterliegen, gilt die Geheimhaltungspflicht auch für die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz.

§ 26
Pflicht zur Unterstützung

(1) Die öffentlichen Stellen sind verpflichtet, die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz und ihre oder seine Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihnen ist im Rahmen ihrer gesetzlichen Befugnisse insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen und

2. jederzeit Zutritt zu den Diensträumen einschließlich aller Datenverarbeitungsanlagen und -geräte zu gewähren.

(2) Die Ministerien beteiligen die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz rechtzeitig bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften, welche die Verarbeitung personenbezogener Daten betreffen.

§ 27
Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz

(1) Der Südwestrundfunk ernennt für die Dauer von sechs Jahren eine Rundfunkbeauftragte für den Datenschutz oder einen Rundfunkbeauftragten für den Datenschutz, die oder der für alle Tätigkeiten des Südwestrundfunks und seiner Beteiligungsunternehmen nach § 16c Absatz 3 Satz 1 des Rundfunkstaatsvertrages an Stelle der oder des Landesbeauftragten für den Datenschutz zuständige Aufsichtsbehörde nach Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 ist. Die Ernennung erfolgt durch den Rundfunkrat mit Zustimmung des Verwaltungsrats. Die zweimalige Wiederernennung ist zulässig.

(2) Die oder der Rundfunkbeauftragte für den Datenschutz muss über die für die Erfüllung der Aufgaben und Ausübung der Befugnisse erforderliche Qualifikation, nachgewiesen durch ein abgeschlossenes Hochschulstudium, sowie über Erfahrung und Sachkunde, insbesondere im Bereich des Schutzes personenbezogener Daten, verfügen.

(3) Die Dienststelle der oder des Rundfunkbeauftragten für den Datenschutz wird bei der Geschäftsstelle des Rundfunk- und Verwaltungsrats eingerichtet. Die oder der Rundfunkbeauftragte für den Datenschutz ist angemessen zu vergüten. Nähere Bestimmungen, insbesondere die Grundsätze der Vergütung, trifft der Rundfunkrat mit Zustimmung des Verwaltungsrats in einer Satzung. Ihr oder ihm ist die für die Erfüllung ihrer oder seiner Aufgaben und Befugnisse notwendige Personal-, Finanz- und Sachausstattung zur Verfügung zu stellen. Die hierfür vorgesehenen Mittel sind jährlich, öffentlich und gesondert im Haushaltsplan des Südwestrundfunks auszuweisen und der oder dem Rundfunkbeauftragten für den Datenschutz im Haushaltsvollzug zuzuweisen. Die oder der Rundfunkbeauftragte für den Daten-

schutz ist in der Wahl ihrer oder seiner Mitarbeiterinnen oder Mitarbeiter frei. Sie unterstehen allein ihrer oder seiner Leitung.

(4) Das Amt der oder des Rundfunkbeauftragten für den Datenschutz kann nicht neben anderen Aufgaben innerhalb des Südwestrundfunks und seiner Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt der oder des Rundfunkbeauftragten für den Datenschutz zu vereinbaren sein und dürfen ihre oder seine Unabhängigkeit nicht gefährden. Das Amt endet mit Ablauf der Amtszeit, mit Rücktritt vom Amt oder mit Erreichen des gesetzlichen oder tarifvertraglich geregelten Renteneintrittsalters. Die oder der Rundfunkbeauftragte für den Datenschutz kann ihres oder seines Amtes nur enthoben werden, wenn sie oder er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Dies geschieht durch Beschluss des Rundfunkrats auf Vorschlag des Verwaltungsrats; die oder der Rundfunkbeauftragte für den Datenschutz ist vor der Entscheidung zu hören.

(5) Die oder der Rundfunkbeauftragte für den Datenschutz ist in Ausübung ihres oder seines Amtes völlig unabhängig und nur dem Gesetz unterworfen. Sie oder er unterliegt keiner Dienst-, Rechts- und Fachaufsicht. Der Finanzkontrolle des Verwaltungsrats unterliegt sie oder er nur insoweit, als ihre oder seine Unabhängigkeit dadurch nicht beeinträchtigt wird. Die Mitglieder des Rundfunkrats und des Verwaltungsrats sind berechtigt, Anfragen an die Rundfunkbeauftragte für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz zu richten, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

(6) Jeder kann sich an die Rundfunkbeauftrage für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz wenden, wenn sie oder er der Ansicht ist, bei der Verarbeitung ihrer oder seiner personenbezogenen Daten durch den Südwestrundfunk oder eines seiner Beteiligungsunternehmen nach Absatz 1 Satz 1 in seinen Rechten verletzt worden zu sein.

(7) Die oder der Rundfunkbeauftragte für den Datenschutz hat die Aufgaben und Befugnisse entsprechend Artikel 57 und Artikel 58 Absatz 1 bis 5 der Verordnung (EU) 2016/679. Gegen den Südwestrundfunk dürfen keine Geldbußen verhängt werden. § 25 Absatz 4 gilt entsprechend mit der Maßgabe, dass die Mitteilung an die Intendantin oder den Intendanten unter gleichzeitiger Unterrichtung des Verwaltungsrats zu richten ist. Dem Verwaltungsrat ist auch die Stellungnahme der Intendantin oder des Intendanten zuzuleiten. Von einer Beanstandung und Unterrichtung kann abgesehen werden, wenn es sich um unerhebliche Mängel handelt oder wenn ihre unverzügliche Behebung sichergestellt ist.

(8) Die oder der Rundfunkbeauftragte für den Datenschutz hat auch für die Dauer von zwei Jahren nach der Beendigung ihrer oder seiner Amtszeit von allen mit den Aufgaben ihres oder seines früheren Amtes nicht zu vereinbarenden Handlungen und entgeltlichen oder unentgeltlichen Tätigkeiten abzusehen.

(9) Die oder der Rundfunkbeauftragte für den Datenschutz ist während und nach Beendigung ihres oder seines Amtsverhältnisses verpflichtet, über die ihr oder ihm amtlich bekannt gewordenen Angelegenheiten und vertraulichen Informationen Verschwiegenheit zu bewahren. Bei der Zusammenarbeit mit anderen Aufsichtsbehörden ist, soweit die Datenverarbeitung zu journalistischen Zwecken betroffen ist, der Informantenschutz zu wahren.

(10) Die oder der Rundfunkbeauftragte für den Datenschutz erstattet den Organen des Südwestrundfunks jährlich einen Tätigkeitsbericht nach Artikel 59 der Verordnung (EU) 2016/679. Der Bericht wird den Landtagen und den Landesregierungen der unterzeichnenden Länder des Staatsvertrags über den Südwestrundfunk übermittelt. Der Bericht wird veröffentlicht.

ABSCHNITT 6
Sanktionen

§ 28
Ordnungswidrigkeiten

(Ergänzung zu Artikel 83 Absatz 7 der Verordnung [EU] 2016/679)

Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 dürfen keine Geldbußen verhängt werden, es sei denn, die öffentlichen Stellen nehmen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teil.

§ 29

Strafvorschrift

(Ergänzung zu Artikel 84 der Verordnung [EU] 2016/679)

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. unbefugt von diesem Gesetz oder der Verordnung (EU) 2016/679 geschützte personenbezogene Daten, die nicht allgemein zugänglich sind,
   a) speichert, nutzt, verändert, übermittelt oder löscht,

   b) zum Abruf mittels automatisierten Verfahrens bereithält oder

   c) abruft oder sich oder einem anderen aus Dateien verschafft oder

2. durch unrichtige Angaben personenbezogene Daten, die durch dieses Gesetz oder die Verordnung (EU) 2016/679 geschützt werden und nicht allgemein zugänglich sind, erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, die öffentliche Stelle, der Auftragsverarbeiter, die oder der Landesbeauftragte für den Datenschutz, die oder der Rundfunkbeauftragte für den Datenschutz und die Aufsichtsbehörden.

ABSCHNITT 7
Übergangsbestimmungen

§ 30
Polizeibehörden und Polizeivollzugsdienst, Justizbehörden, Landesamt für Verfassungsschutz und Vollzug des Landessicherheitsüberprüfungsgesetzes

(1) Für die Verarbeitung personenbezogener Daten durch die Polizeibehörden und den Polizeivollzugsdienst gilt, soweit sie nicht die Verordnung (EU) 2016/679 anzuwenden haben, das Landesdatenschutzgesetz in der am 20. Juni 2018 geltenden Fassung weiter, bis die Regelungen des Landes Baden-Württemberg zur Umsetzung der Richtlinie (EU) 2016/680 für den Bereich der Polizei in Kraft treten.

(2) Für die Verarbeitung personenbezogener Daten zu den in Artikel 2 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679 genannten Zwecken durch das Justizministerium und die Justizvollzugsbehörden sowie durch die ordentlichen Gerichte und die Staatsanwaltschaften des Landes, soweit sie zu diesen Zwecken in Verwaltungsangelegenheiten tätig werden, sowie für die Behörden des Landes, die personenbezogene Daten zur Verfolgung und Ahndung von Ordnungswidrigkeiten verarbeiten, gilt das Landesdatenschutzgesetz in der am 20. Juni 2018 geltenden Fassung weiter, bis das Gesetz des Landes Baden-Württemberg zur Anpassung des besonderen Datenschutzrechts an die Verordnung und zur Umsetzung der Richtlinie (EU) 2016/680 für den Geschäftsbereich des Justizministeriums sowie für die zur Ahndung von Ordnungswidrigkeiten zuständigen Behörden des Landes in Kraft tritt.

(3) Für die Verarbeitung personenbezogener Daten durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes und beim Vollzug des Landessicherheitsüberprüfungsgesetzes gilt das Landesdatenschutzgesetz in der am 20. Juni 2018 geltenden Fassung weiter, bis das Gesetz des Landes Baden-Württemberg zur Änderung des Landesverfassungsschutzgesetzes und anderer Gesetze in Kraft tritt.

§ 31
Überleitungsvorschriften

(1) Der zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Amt befindliche Landesbeauftragte für den Datenschutz gilt ab dem Tag des Inkrafttretens dieses Gesetzes als in ein Amt nach § 23 Absatz 1 beru-

fen. Mit der Berufung in dieses Amt endet sein Beamtenverhältnis auf Zeit. Seine Amtszeit endet am 31. Dezember 2022.

(2) Mit Inkrafttreten dieses Gesetzes sind die Angehörigen des öffentlichen Dienstes bei dem Landesbeauftragten für den Datenschutz vom Landtag zu dem Landesbeauftragten für den Datenschutz versetzt.

(3) Der Personalrat bei der Dienststelle des Landesbeauftragten für den Datenschutz besteht ab Inkrafttreten dieses Gesetzes bis zu seiner Neuwahl als Personalrat bei dem Landesbeauftragten für den Datenschutz fort.

Anlage 3

Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

6. November 2020

EVALUIERUNG DES LANDESDATENSCHUTZGESETZES BADEN-WÜRTTEMBERG

I. Sicherstellung des Datenschutzes, § 3

1. § 3 Absatz 1 S. 3 Nr. 1 LDSG liest sich derzeit so, als seien technische und organisatorische Maßnahmen ein „Kann", kein „Muss". Das widerspricht dem Wortlaut des Artikel 32 Absatz 1 HS 1 DS-GVO, wonach (unter Berücksichtigung des Stands der Technik usw.) der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Erst im zweiten Halbsatz zählt Artikel 32 Absatz 1 in den Buchstaben a) bis d) auf, welche Maßnahmen „gegebenenfalls" zu den TOMs gehören.

   Handlungsempfehlung:

   § 3 LDSG sollte klarstellen, dass TOMs stets zu treffen sind, indem § 3 Absatz 1 S. 3 Nr. 1 „vor die Klammer" gezogen wird.

2. In der bisherigen Praxis der Bußgeldbehörde werden Behördenmitarbeiter, die ihre gesetzlichen Datenverarbeitungsbefugnisse überschreiten und damit gegen das Datengeheimnis des § 3 Abs. 2 LDSG verstoßen, wie Privatpersonen nach DS-GVO und BDSG behandelt. Klarer wäre es, dies ausdrücklich im LDSG zu regeln. Es ist nicht nachvollziehbar, weshalb öffentlich Bedienstete sanktionslos gegen Datenschutzbestimmungen verstoßen können sollten.

   Handlungsempfehlung:
   Der Verstoß gegen das Datengeheimnis gemäß § 3 Absatz 2 LDSG sollte bußgeldbewehrt werden.

Königstraße 10 a · 70173 Stuttgart · Telefon 0711 615541-0 · Telefax 0711 615541-15 · poststelle@lfdi.bwl.de · poststelle@lfdi.bwl.de-mail.de
www.baden-wuerttemberg.datenschutz.de · PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

II. Zulässigkeit der Verarbeitung personenbezogener Daten, § 4

Das LDSG enthält keine spezielle Norm zur Datenverarbeitung im Rahmen von **Öffentlichkeitsarbeit**. Es kann immer lediglich auf die Generalklausel des § 4 zurückgegriffen werden.

Wie bereits in der Broschüre „Wesentliche Anforderungen an die behördliche Nutzung Sozialer Netzwerke“ gefordert, ist die Schaffung einer Norm, die Umfang und Grenzen von Öffentlichkeitsarbeit in sozialen Medien regelt, dringend erforderlich, um die Arbeit der Behörden in diesem Bereich zu legitimieren. Nur so können rechtsklare und bestimmte Vorgaben für den immer wichtiger werdenden öffentlichen Auftritt von Behörden und anderen öffentlichen Stellen in sozialen Netzwerken geschaffen werden, während der Schutz personenbezogener Daten gewährleistet wird. Insoweit wird eine Änderung von § 4 und eine Ergänzung durch einen neuen § 4a gefordert:

Handlungsempfehlung:

Erweiterung der landesrechtlichen Rechtsgrundlage um die Öffentlichkeitsarbeit

Formulierungsvorschlag:

§ 4

Zulässigkeit der Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist.

(2) Als Aufgabe der öffentlichen Stelle gilt auch deren Öffentlichkeitsarbeit. Findet die Öffentlichkeitsarbeit durch Nutzung eines sozialen Netzwerks statt, ist die öffentliche Stelle für die Verarbeitung personenbezogener Daten gemäß Artikel 26 der Datenschutz-Grundverordnung gemeinsam mit dem Anbieter des sozialen Netzwerks verantwortlich. Sie hat die Einrichtung und Einhaltung geeigneter technischer und organisatorischer Maßnahmen nach der Datenschutz-Grundverordnung zu gewährleisten.

III. Erweiterung der Möglichkeit einer Zweckänderung, § 5

Eine Erweiterung der Regelung zur zulässigen Zweckänderung aus polizeilichen oder politischen Gründen ist empfehlenswert.

1. § 5 Absatz 1 LDSG ist nach den praktischen Erfahrungen der Aufsichtsbehörde zu eng gefasst. Insbesondere die fehlende Möglichkeit, Daten zweckändernd auch für Strafverfolgungszwecke weiter zu verarbeiten (nach § 18 Absatz 3 LDSG ist dies bei Videoaufnahmen möglich), ist nicht praxisgerecht und führt dazu, im Einzelfall den Anwendungsbereich der Nummer 1 („Wahrung erheblicher Belange des Gemeinwohls““) bis an die Grenze des Vertretbaren und unter Aufgabe jeglicher Normbestimmtheit auszudehnen.

   Handlungsempfehlung:

   Es wird empfohlen, sich an der Fassung des § 23 Absatz 1 BDSG zu orientieren.

2. Auch im Bereich der „politischen“ Arbeit wäre eine Erweiterung denkbar, um z.B. Kontaktdaten zur Einladung zu einer öffentlichen Anhörung oder eines Erfahrungsaustausches zu verwenden.

   Handlungsempfehlung:

   Wichtig ist, dass bei der Schaffung einer geeigneten Rechtsgrundlage der Grundsatz der Datenminimierung eingehalten wird und die Verarbeitung der Daten an die Voraussetzung der Erforderlichkeit geknüpft wird.

IV. Ausnahmen von den Informationspflichten des Artikel 13 DS-GVO, § 8

§ 8 LDSG ist in seiner aktuellen Fassung mit den Vorgaben der DS-GVO nicht vereinbar.

In § 8 Absatz 1 LDSG ist weitgehend eine Wiederholung der Ziele aus der einschlägigen Öffnungsklausel in Artikel 23 Absatz 1 DS-GVO enthalten. Es fehlt aber an zusätzlichen konkretisierenden Angaben in Sinne von Artikel 23 Absatz 2 DS-GVO. Artikel 23 Absatz 2 DS-GVO stellt die Einhaltung des Bestimmtheitsgrundsatzes sicher. Da dessen Anforderungen nicht eingehalten sind, ist § 8 LDSG zu unbestimmt und muss unter Berücksichtigung der oben genannten Konkretisierungsvorschläge grundsätzlich überarbeitet werden.

V. Beschränkung des Auskunftsrechts, § 9

Zur Klarstellung sollte die Bezugnahme auf Artikel 15 DS-GVO nicht nur in der Überschrift, sondern – wie in Gesetzen sonst üblich – auch im Normtext selbst erfolgen.

Eine Einschränkung für Behörden ist sinnvoll, aber die praktische Anwendung/Umsetzung erscheint problematisch:

- Die Norm ist zu unkonkret – in der Praxis gibt es viele Rückfragen zum Anwendungsbereich.
- Eine Erläuterung des Begriffs „große Mengen von Informationen“ ist erforderlich, ebenso eine Erläuterung des Begriffs „unzumutbarer Aufwand“.
- Es ist eine Klarstellung erforderlich, ob bei der Betrachtung die jeweilige Einzelbehörde entscheidend ist oder ob es auch auf Kommunikationsvorgänge mit anderen Behörden ankommt.

VI. Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, § 14

Die Beschränkungen, die § 14 LDSG hinsichtlich der Rechte der betroffenen Personen vornimmt, sind zu weitgehend und stehen damit im Widerspruch zur Öffnungsklausel des Artikels 89 Abs. 3 DS-GVO. Dieser erlaubt Ausnahmen nur, wenn die Betroffenenrechte voraussichtlich die Verwirklichung der spezifischen Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind. § 14 LDSG geht aber über diese Einschränkungsmöglichkeiten hinaus: In Abs. 2 wird das Recht auf Auskunft aus Gründen des Verwaltungsaufwands eingeschränkt. Der Absatz 3 schließt das Recht auf Berichtigung bei Datenverarbeitungen zu im öffentlichen Interesse liegenden Archivzwecken generell aus und gesteht den Betroffenen nur ein Recht auf Gegendarstellung zu. Damit berücksichtigt die Norm nicht hinreichend, dass es auch Fälle geben kann, in denen ein gewichtiges Interesse an einer Richtigstellung besteht (bspw. zu Rehabilitationszwecken), ohne dass hierdurch die Archivzwecke unmöglich gemacht oder ernsthaft beeinträchtigt werden. Absatz 4 erscheint schließlich im Hinblick auf den Bestimmtheitsgrundsatz und die insofern von Artikel 23 Absatz 2 DS-GVO formulierten Anforderungen problematisch, da er den Wortlaut des Art. 89 Abs. 3 DS-GVO lediglich wiederholt.

Handlungsempfehlung:
Neufassung des § 14 unter Beachtung des grundrechtsverkürzenden Charakters der Einschränkungen der Betroffenenrechte – nur restriktiver Gebrauch der Öffnungsklausel des Artikels 89 Abs. 3 DS-GVO unter Beachtung des Verhältnismäßigkeits- und des Bestimmtheitsgrundsatzes.

VII. Datenverarbeitung bei Dienst- und Arbeitsverhältnissen - § 15

§ 15 Absatz 6 HS 2 ist, wie an dem folgenden Normauszug zu erkennen ist, nicht normenklar:

„(6) Die Verarbeitung biometrischer Daten von Beschäftigten zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, die betroffene Person hat ausdrücklich eingewilligt oder sie ist durch Dienst- oder Betriebsvereinbarung geregelt und für die Datenverarbeitung besteht jeweils ein dringendes dienstliches Bedürfnis."

Wenn man den Wortlaut ganz genau nimmt, müsste sich „sie" auf „die betroffene Person" beziehen, was aber keinen Sinn ergibt. Daher sollte das ersetzt werden durch „*die Verarbeitung*". Davon abgesehen wäre es sinnvoll, bei der Aufzählung der Alternativen zuerst die Regelung durch Dienst- oder Betriebsvereinbarung zu nennen und erst dann die Einwilligung, da die Einwilligung mit ihren hohen Anforderungen und mit Blick auf bestehende Über-/Unterordnungsverhältnisse, welche der Freiwilligkeit der Einwilligung zuwiderlaufen, nur restriktiv als Verarbeitungsgrundlage zu verwenden ist.

VIII. Videoüberwachung öffentlich zugänglicher Räume, § 18

1. In der Praxis wird die Höchstspeicherdauer des § 18 Abs. 5 LDSG meist ausgenutzt, ohne dass eine sachliche Erforderlichkeit nachweisbar ist. Dies widerspricht dem Grundsatz der Speicherbegrenzung (Artikel 5 Absatz 1 Buchstabe e DS-GVO).

   Handlungsempfehlung:

   Streichung der Wörter „spätestens jedoch vier Wochen nach der Datenerhebung" in § 18 Absatz 5 LDSG.

2. § 18 Absatz 2 und 4 LDSG entsprechen nicht den Transparenzgeboten der DS-GVO. Es ist insbesondere nicht nachvollziehbar, weshalb für die Datenerhebung durch Videoüberwachung geringere Anforderungen an die Information der Betroffenen gem. Artikel 13 DS-GVO gestellt werden sollten als in den übrigen Fällen der Datenerhebung. In der Praxis führt das dazu, dass wir im Rahmen von Beratungen und Kontrollen die Anforderungen im Wege der europarechtskonformen Auslegung der Vorschrift definieren, was unnötigen Aufwand bedeutet, ohne dass dies auf Ablehnung stößt.

IX. Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken - § 19

§ 19 LDSG enthält eine Einschränkung dahingehend, dass nur bestimmte Normen/Kapitel der DS-GVO (sowie § 19 LDSG) anwendbar sind. Diese Einschränkung muss darauf überprüft werden, ob sie mit der Tatsache vereinbar ist, dass das KUG, insbesondere §§ 21-23 KUG, nach wie vor nicht aufgehoben wurden und laut bisher ergangenen Urteilen weiter Anwendung finden.

X. Aufgaben und Befugnisse, § 25

1. Die Maßnahmenbefugnisse der Aufsichtsbehörde sind abschließend in Artikel 58 DS-GVO geregelt. Artikel 6 Abs. 2 und 3 DS-GVO eröffnen keinen Spielraum des Landesgesetzgebers, die Durchführung dieser Maßnahmen von weiteren Voraussetzungen abhängig zu machen. Fraglich ist ohnehin, ob hier der Vorrang europarechtlicher Regelungen die Unanwendbarkeit dieser Maßgabe zur Folge hat – wovon der LfDI ausgeht. Abgesehen hiervon hindert die Verpflichtung, vor Durchführung von Maßnahmen eine Stellungnahme einzuholen, den effektiven Schutz der Betroffenen vor fortdauernden Grundrechtsbeeinträchtigungen, da regelmäßig geraume Zeit vergeht, bis es bspw. zu einer Löschungsanordnung oder einem sonstigen Verarbeitungsverbot kommt. Insbesondere auch bei kommunalen Verantwortlichen ist die Unterrichtung des Bürgermeisters regelmäßig überflüssig, da dieser die Korrespondenz mit der Aufsichtsbehörde regelmäßig bereits kennen wird.

   Handlungsempfehlung:

   Streichung des § 25 Absatz 4 LDSG

2. Die Beschränkung der Aufsichtsbefugnisse gegenüber Notaren ist europarechtswidrig. Sie ist wegen des Vorrangs der DS-GVO nicht anwendbar und sollte der Klarheit wegen gestrichen werden.

   Handlungsempfehlung:

   Streichung des § 25 Absatz 5 Satz 1

XI. Spezielle Norm für die Übermittlung von Daten an (ausländische) Behörden

Die alte Fassung des LDSG regelte in § 16 bzw. § 20 spezifisch die Übermittlung von Daten an andere deutsche sowie ausländische Behörden. Um den Austausch zwischen Behörden zu vereinfachen, wäre die Wiederaufnahme dieser Vorschriften wünschenswert:

§ xx

Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,
2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder
3. der Organe und Einrichtungen der Europäischen Gemeinschaften

gilt § 6 dieses Gesetzes entsprechend.

(2) Die Übermittlung personenbezogener Daten in Staaten außerhalb der Europäischen Union oder an über- oder zwischenstaatliche Stellen ist unter den Voraussetzungen der Artikel 46 bis 49 der Verordnung [EU] 2016/679 zulässig, soweit keine spezielleren Vorschriften eingreifen.

XII. Aufnahme einer Bestimmung zur Beauftragung der Auftragsverarbeitung durch die Fachaufsichtsbehörde

Die Regelung in § 7 Absatz 1 Satz 5 LDSG alt sah vor, dass ein Auftrag zur Datenverarbeitung im Auftrag auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegende Stellen des Landes erteilt werden konnte. Eine Aufnahme einer solchen Regelung auch unter Geltung der DS-GVO wäre sinnvoll, nicht zuletzt vor dem Hintergrund der Erfahrungen bei der CoronaVO-Auftragsverarbeitung.

XIII. Teilnahme des Personals des LfDI an der Personalrotation der Innenverwaltung

Früher war der LfDI als Behörde im Verwaltungsaustausch ausdrücklich mit aufgenommen. In § 26 Absatz 4 Satz 4 der alten Fassung des LDSG war festgelegt, dass bezüglich der Beschäftigten des Landesbeauftragten die „Einbeziehung in den allgemeinen Personalaustausch der Landesverwaltung […] von der Landesregierung gewährleistet [wird]“. Heute fehlt eine entsprechende Regelung. Die Möglichkeit eines solchen Austauschs wäre wegen der Eigenschaft des LfDI als oberste Landesbehörde jedoch wünschenswert und könnte in den bestehenden § 20 Absatz 2 LDSG integriert werden. Der Personalaustausch schafft das notwendige Verwaltungsverständnis innerhalb des Personalkörpers des LfDI und sorgt dafür, dass die Behörden der Innenverwaltung mit datenschutzrechtlich versiertem Personal versorgt werden.

XIV. Effektivität und Durchsetzbarkeit von Anordnungen gegenüber Behörden

Nach Artikel 58 Absatz 2 DS-GVO ist die Aufsichtsbehörde befugt, auch Behörden durch förmliche Entscheidung (Verwaltungsakt) zu einem datenschutzkonformen Verhalten anzuhalten. Wirksame Befugnisse, diese Entscheidungen durchzusetzen,

gibt es nicht nur wegen der bisher nicht erfolgten Umsetzung des Artikels 58 Absatz 5 DS-GVO nicht, sondern auch, weil das LDSG die Vollstreckung gegen Behörden und juristische Personen des öffentlichen Rechts nicht regelt (§ 22 des Landesvollstreckungsgesetzes). Eine Ermöglichung der Vollstreckung fehlt im LDSG und sollte beispielsweise in § 25 integriert werden, um die datenschutzrechtlichen Abhilfemaßnahmen des LfDI auch Behörden und anderen öffentlichen Stellen gegenüber effektiv durchsetzbar zu machen und seine in § 21 LDSG normierte Unabhängigkeit zu gewährleisten. Gerade die Möglichkeit, Zwangsgelder zu verhängen, könnte insbesondere im kommunalen Bereich die Bereitschaft erhöhen, den Anweisungen der Aufsichtsbehörde Folge zu leisten.

Das Versäumen der Umsetzung des Regelungsbefehls in Art. 58 Abs. 5 DS-GVO ist ein klarer Verstoß gegen europäisches Recht. Hierzu hatte der EuGH noch unter der Geltung der Datenschutz-Richtlinie geurteilt:

„Hält die Kontrollstelle die Rügen der Person, die sich mit einer Eingabe zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten an sie gewandt hat, dagegen für begründet, ***muss sie*** *nach Art. 28 Abs. 3 Unterabs. 1 dritter Gedankenstrich der Richtlinie 95/46 im Licht insbesondere von Art. 8 Abs. 3 der Charta* ***ein Klagerecht haben****. Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen“* (EuGH, Urteil vom 06.10.2015, C-362/14, Celex-Nr. 62014CJ0362).

Dies entspricht auch der herrschenden Auffassung in der Literatur; bspw.: „Art. 58 Abs. 5 verlangt als obligatorische Spezifizierungsklausel von den Mitgliedstaaten, in nationalen Rechtsvorschriften vorzusehen, dass ihre Datenschutz-Aufsichtsbehörden befugt sind, Verstöße gegen die DS-GVO den Justizbehörden zur Kenntnis zu bringen, entweder durch Einleitung eines gerichtlichen Verfahrens oder durch sonstige Beteiligung an diesem, um die Bestimmungen der DS-GVO erforderlichenfalls gerichtlich durchzusetzen.“ (Ehmann/Selmayr/Selmayr, 2. Aufl. 2018, DS-GVO Art. 58 Rn. 41)

XV. Sonderzuständigkeit bei Ordnungswidrigkeiten im Telemedien-Bereich

Aufgrund einer gesonderten Zuständigkeitsnorm in der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten Baden-Württemberg (OWiZuVO BW) entsteht in spezifischen Einzelfällen bei Ordnungswidrigkeiten im Telemedien-Bereich eine kuriose Sonderzuständigkeit des Regierungspräsidiums Karlsruhe. Während sich die Zuständigkeit des Landesbeauftragten für den Datenschutz aus § 25 LDSG allein für Verstöße gegen DS-GVO und BDSG ergibt, ist für Verstöße gegen das TMG keine Zuständigkeit begründet. Grundsätzlich sind gemäß § 2 Absatz 1 OWiZuVO BW für die Verfolgung und Ahndung von Ordnungswidrigkeiten die unteren Verwaltungsbehörden zuständig. In § 4 Absatz 2 Nr. 4

ist jedoch eine Spezialzuständigkeit des Regierungspräsidiums Karlsruhe vorgesehen, für Ordnungswidrigkeiten nach § 16 Absatz 2 Nr. 2 bis 5 TMG. Dass selbst bei den dort genannten datenschutzrechtlich geprägten Verstößen im Telemedien-Bereich zum einen nicht wie üblich die unteren Verwaltungsbehörden zuständig sind, zum anderen aber vor allem auch nicht der LfDI, ist nicht nachvollziehbar. Es wäre wünschenswert, den § 4 Absatz 2 Nr. 4 OWiZuVO BW zu streichen und stattdessen eine entsprechende Sonderzuständigkeit des LfDI für solche Fälle zu schaffen.

Anlage 4

Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg
Referat 25
Postfach 103465
70029 Stuttgart

Per E-Mail:
poststelle@im.bwl.de

Datum 13. Februar 2024
Name Prof. Dr. Keber/
Durchwahl 0711/615541-0
Aktenzeichen 0557.0-1/1/3
(Bitte bei Antwort angeben)

Stellungnahme zur Evaluierung des Landesdatenschutzgesetzes
Ihr Schreiben vom 16.11.2021
Anlage: Stellungnahme zur Evaluierung des Landesdatenschutzgesetzes

sehr geehrte Damen und Herren,

wir bedanken uns für die Gelegenheit zur Stellungnahme und bitten die zeitliche Verzögerung bei der Rückäußerung zu entschuldigen.

Gerne nehmen wir zur Evaluierung des Landesdatenschutzgesetzes wie folgt Stellung. Wir geben dabei – gegliedert nach den aktuellen Paragraphen des Landesdatenschutzgesetzes (LDSG), ggf. auch noch weiter untergliedert – zunächst den wesentlichen Inhalt der in den Evaluationen der verschiedenen Ressorts geäußerten Kritik wieder – einschließlich unserer eigenen Stellungnahme vom 6. November 2020 im Rahmen der Evaluation – und nehmen sodann zu diesen aus aktueller Sicht Stellung. Gelegentlich fügen wir darüber hinaus aus unserer Sicht aktuell erforderlichen Änderungsbedarf an.

Dabei gehen wir zunächst auf Einzelanmerkungen zu Vorschriften des LDSG ein. Anschließend folgt ein Abschnitt mit Anregungen zur Aufnahme weiterer Vorschriften

Lautenschlagerstraße 20 · 70173 Stuttgart · Telefon 0711 615541-0 · Telefax 0711 615541-15
poststelle@lfdi.bwl.de · poststelle@lfdi.bwl.de-mail.de
www.baden-wuerttemberg.datenschutz.de · PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

in das LDSG bzw. zu Anregungen, die sich nicht an einer bestimmten Vorschrift des LDSG in der aktuellen Fassung festmachen lassen. Schließlich gehen wir auf Änderungsbedarf von Vorschriften ein, die zwar mit dem LDSG in einem Zusammenhang stehen, sich aber außerhalb des LDSG befinden. Zur besseren Lesbarkeit und einer schnellen Erfassung der wesentlichen Punkte aus unserer Sicht finden Sie zu Beginn des Dokuments eine kurze Zusammenfassung.

Gerne stehen wir für weitere Rückfragen oder Beratungen zur Verfügung.

Mit freundlichen Grüßen

gez. Prof. Dr. Tobias Keber
Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Stellungnahme zur Evaluierung des Landesdatenschutzgesetzes

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Zusammenfassung

Im Zuge der Evaluation sind aus den Ressorts und unserer Dienststelle unterschiedliche Anregungen vorgetragen worden, an welchen Stellen das Landesdatenschutzgesetz zu überarbeiten sei. Die Anregungen wurden überwiegend damit begründet, dass die geltende Rechtslage unklar sei oder dass deren Vorgaben für die praktischen Bedürfnisse der datenverarbeitenden Stellen zu eng seien. Teils wurde aber auch moniert, dass die Regelungen mit den europäischen Vorschriften der Datenschutz-Grundverordnung nicht vereinbar seien.

Wir haben diese Anregungen geprüft und einer Bewertung unterzogen. Teilweise halten wir die bisherige Rechtslage entgegen den Anregungen für ausreichend; zum Teil waren die vorgeschlagenen Regelungen auch mit der Datenschutz-Grundverordnung nicht zu vereinbaren oder stellten einen zu weitgehenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.

In verschiedenen Hinsichten halten wir aber eine Novellierung des Landesdatenschutzgesetzes für erforderlich. Wesentlichen Änderungsbedarf sehen wir insbesondere in den folgenden Punkten:

- Vor dem Hintergrund insbesondere einer neuen Entscheidung des EuGH vom Januar 2024 besteht Anlass zu Prüfung, inwieweit die Begrenzung der Gültigkeit des LDSG für den Landtag gemäß § 2 Abs. 5 LDSG Bestand haben kann. Insoweit sollte zur Wahrung des Prinzips der Gewaltenteilung die Einrichtung einer unabhängigen Kontrollstelle beim Landtag erwogen werden, die dort die Datenschutzaufsicht übernimmt und bei deren Ausgestaltung die parlamentarischen Besonderheiten berücksichtigt werden.
- Die zentrale Vorschrift des § 3 LDSG zur „Sicherstellung des Datenschutzes“ ist dringend zu überarbeiten. Sie vermengt verschiedene Aspekte (technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und spezifische Anforderungen nach Art. 6 Absatz 2 und 3 sowie nach Art 9 Absatz 2 Buchstabe g DS-GVO), deren Normierung durch nationales Recht die Datenschutz-

Grundverordnung nur zum Teil oder nur bei entsprechend spezifischer Ausgestaltung der Regelung zulässt. Die Mehrfachfunktion der Vorschrift führt in der Praxis zu Unklarheiten. Zugleich ist die Norm zu wenig spezifisch ausgestaltet, um den Anforderungen der Öffnungsklauseln aus Art. 6 und 9 DS-GVO zu genügen. Dies gilt in besonderem Maße, soweit die Vorschrift – im Zusammenspiel mit der ebenfalls dringend überarbeitungsbedürftigen Regelung in § 17 Absatz 2 LDSG – gemäß Art. 9 Absatz 2 Buchstabe g DS-GVO die spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person bei der Verarbeitung besonderer Kategorien personenbezogener Daten regeln soll.

- Die Systematik der §§ 4-6 LDSG (Generalklausel, Zweckänderung und Übermittlung) sollte im Interesse der besseren Verständlichkeit einer Überprüfung unterzogen werden. Die Regelungen zur Zweckänderung und Übermittlung bedürfen der Konkretisierung. Die Verschiebung der datenschutzrechtlichen Übermittlungsverantwortung bei Anforderung von Daten (§ 6 Absatz 2 Satz 2-4 LDSG) hat sich nicht bewährt und sollte dringend abgeschafft werden. Im Übrigen sollten Regelungen zur Übermittlung an öffentliche Stellen außerhalb des Landes Baden-Württemberg und Deutschlands geschaffen werden.
- Zur Vereinfachung für die Praxis empfehlen wir die Aufnahme einer Regelung, dass ein Vertrag zur Auftragsverarbeitung auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegende Stellen des Landes erteilt werden kann (vgl. neuerdings § 115 Absatz 3e des Schulgesetzes oder früher § 7 Absatz 1 Satz 5 LDSG a. F.).
- An mehreren Stellen werden die Informationspflicht der datenverarbeitenden Stellen (aus Art. 13 und 14 DS-GVO) oder die Betroffenenrechte (u. a. auf Auskunft, Berichtigung oder Löschung) europarechtswidrig verkürzt. Dies gilt z. B. für die Regelung in § 8 LDSG zu Ausnahmen von der Informationspflicht aus Art. 13 und 14 DS-GVO, für die Einschränkungen des Auskunftsrechts in § 9 Absatz 1 Satz 2 und Absatz 2 LDSG, für die Beschränkung der Betroffenenrechte bei der Verarbeitung zu im öffentlichen Interessen liegenden Archivzwecken (§ 14 LDSG) und aufgrund der auch aus anderen Gründen kritikwürdigen Norm über die Verarbeitung zur Entscheidung über öffentliche Auszeichnungen und Ehrungen (§ 16 LDSG).
- Die Vorschrift zur Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (§ 13 LDSG) sollte dringend überarbeitet und dabei auch auf ihre Anschlussfähigkeit zu Parallelvorschriften in Bund und Ländern hin überprüft werden. Zwischenzeitlich zur Thematik ergangene Positionierungen der Datenschutzkonferenz (DSK) sollten

hierbei ebenso berücksichtigt werden, wie über die Aufnahme bisher nicht geregelter technisch-organisatorischer Maßnahmen nachzudenken wäre, die den Schutz der von einer Datenverarbeitung betroffener Personen gewährleisten, ohne die in Ausgleich zu bringenden Forschungsinteressen außer Verhältnis zu setzen.

- In Bezug auf die Regelungen zur Videoüberwachung (§ 18 LDSG) besteht ein Regelungsbedarf mit Blick auf die unklare Rechtslage in Bezug auf nicht öffentlich zugängliche Räume. Hier empfehlen wir die Schaffung einer Rechtsgrundlage, die an die Regelung für öffentlich zugängliche Räume anknüpft, aber den typischerweise höheren Schutzbedarf vor Überwachung in nicht öffentlich zugänglichen Räumen berücksichtigt. Auch sollte die in der Praxis oftmals missverstandene Regelung zu einer vierwöchigen Speicherhöchstdauer (§ 18 Absatz 5 LDSG) entweder gestrichen werden oder diese Höchstdauer explizit auf die auch für nicht öffentliche Stellen allgemein angenommene 72-Stunden-Frist beschränkt werden.
- Die Regelung zur Errichtung des LfDI (§ 20 LDSG) und zu seinen Aufgaben und Befugnissen (§ 25 LDSG) sollte in mehrfacher Hinsicht überarbeitet werden:
    - Wir bitten darum, in das LDSG – etwa in dessen § 20 – eine der früheren Regelung in § 26 Absatz 4 Satz 4 LDSG a. F. entsprechende Norm aufzunehmen, dass die Einbeziehung des Personals des LfDI in den allgemeinen Personalaustausch der Landesverwaltung gewährleistet wird.
    - Die in § 25 Absatz 4 LDSG europarechtswidrig normierte Pflicht des LfDI, vor einer Abhilfemaßnahme gegen eine öffentliche Stelle die Fachaufsichtsbehörde anzuhören (§ 25 Absatz 4 LDSG), ist zu streichen. Stattdessen sollte eine Befugnis des LfDI zu einer solchen Anhörung geregelt werden.
    - Die europarechtswidrige Beschränkung der Aufsichtsbefugnisse gegenüber Notaren (§ 25 Absatz 5 LDSG) ist zu streichen.
    - Es sind effektive Möglichkeiten der Vollstreckung von Abhilfeentscheidungen des LfDI zu normieren. Außerdem sind gemäß Art. 58 Absatz 5 DS-GVO Rechtsvorschriften zu erlassen, über die Beteiligung des LfDI an gerichtlichen Verfahren und die Einleitung solcher Verfahren durch den LfDI.
    - Es fehlt (außerhalb des Polizeigesetzes) eine ausdrücklich gesetzliche Bestimmung zur Umsetzung der JI-Richtlinie, dass der LfDI auch in de-

ren Anwendungsbereich uneingeschränkt bei der Ausarbeitung von Gesetzen und untergesetzlichen Regelungen des Landes, die die Verarbeitung personenbezogener Daten betreffen, zu beteiligen ist.
    - Dem LfDI sollten auch verwaltungsrechtliche Aufsichtsbefugnisse für die Überwachung und Durchsetzung des zum 01.12.2021 in Kraft getretenen Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) zugewiesen werden. Insoweit ist der LfDI bislang nur für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständig, die (regelmäßig milderen) Mittel verwaltungsrechtlicher Aufsichtsmaßnahmen kann er bisher dagegen nicht ergreifen.
- Die Anregungen des Rundfunkbeauftragten für den Datenschutz, seine durch § 27 LDSG normierte Stellung insbesondere durch ein Benachteiligungsverbot und durch eine nähere gesetzliche Ausgestaltung der Regelungen zu seiner Vergütung zu stärken, halten wir für nachvollziehbar.

I. Zur Evaluation einzelner Vorschriften des LDSG

§ 1 LDSG

Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration (Innenministerium) vom 28.06.2021:
(3.1) Verwenden der Bezeichnung „Datenschutz-Grundverordnung“ statt „Verordnung (EU) 2016/679“ im LDSG BW (wie bspw. im NDSG geschehen).

***LfDI**: Wir teilen die Einschätzung, dass sich die Lesbarkeit durch die Änderung der Bezeichnung verbessern lassen könnte. Die Norm des § 1 LDSG führt den Begriff der Datenschutz-Grundverordnung bereits derart ein, dass dieser im Folgenden ohne die Notwendigkeit weiterer Erläuterungen verwendet werden könnte.*

§ 2 LDSG

Gemeinsame Stellungnahme des Gemeinde- und Landkreistags Baden-Württemberg vom 29.10.2021:
(S. 3 Abs. 3 Spiegelstrich 1) § 2 Abs. 1 S. 2 LDSG solle zur weiteren Verständlichkeit

um folgenden, kursiv gestellten Einschub (unter Streichung des hier durchgestrichenen Worts) ergänzt werden:
„[…] soweit dieses *oder ein anderes Gesetz nichts ~~anderes~~ abweichendes bestimmt.“*
Der Einschub sei trotz der Regelung in § 2 Abs. 3 LDSG sinnvoll, um bereits in der Definition den Hinweis auf Spezialregelungen wie die des § 67 Abs. 4 SGB X zu lenken.

LfDI: *Die vorgeschlagenen Änderungen halten wir nicht für erforderlich und unsystematisch. Wie in der Stellungnahme von Gemeinde- und Landkreistag selbst dargestellt wird, ergibt sich bereits aus § 2 Absatz 3 LDSG, dass besondere Rechtsvorschriften anderer Gesetze denjenigen des Landesdatenschutzgesetzes vorgehen. Die Bestimmung des Verantwortlichen in § 2 Absatz 1 Satz 2 LDSG ist eine solche (materielle, also nicht nur den Anwendungsbereich betreffende) Vorschrift des Landesdatenschutzgesetzes. Warum ausgerechnet bei dieser Norm erneut der Vorrang spezifischerer Regelungen aus anderen Gesetzen erwähnt werden soll, erschließt sich uns nicht. Der Einschub könnte im Gegenteil verwirren, indem sich die Frage stellen könnte, ob an Stellen, an denen nicht erneut der Vorrang anderer Gesetze betont wird, dieser Vorrang im Umkehrschluss (abweichend von § 2 Absatz 3 LDSG) nicht gelten solle.*

Stellungnahme des Ministeriums für Umwelt, Klima und Energiewirtschaft (Umweltministerium) vom 19.10.2020:
(Ziff. 1) Die Regelung in § 2 Abs. 3 LDSG biete mit der Verwendung des Begriffs der „Sachverhaltsermittlung“ Auslegungsschwierigkeiten und verursache in Folge Probleme hinsichtlich der Frage, welches Recht das speziellere sei, das LDSG oder das LVwVfG. Dies sei insbesondere für die Frage relevant, wie man mit § 73 Abs. 1 und 2 LVwVfG in Bezug auf das Anhörungsverfahren im Planfeststellungsverfahren umgehe. Das Anhörungsverfahren diene nämlich sowohl der Sachverhaltsermittlung als auch der Gewährleistung rechtlichen Gehörs. Ohne eine Korrektur durch das Datenschutzrecht würden die in § 73 Abs. 1 LVwVfG bezeichneten Daten (unter anderem Namen, Anschriften betroffener Eigentümer) im Rahmen eines Anhörungsverfahrens veröffentlicht. Soweit das LDSG keinen Anwendungsvorrang habe, sei dem Wortlaut des § 73 Abs. 1 und Abs. 2 LVwVfG die DS-GVO entgegenzuhalten. Aus diesem Grund werde um eine Klarstellung gebeten.

LfDI: *Die Kritik erscheint zutreffend. Wir haben sie bereits in unserer Stellungnahme zur Neufassung des LDSG im Januar 2020 – leider ohne Erfolg – geäußert.*

Zur Beseitigung des Problems sollte, zusätzlich zu einer Klarstellung im LDSG, eine Änderung von § 73 Abs. 1 S. 2 LVwVfG angestrengt werden.

Wir bitten, Folgendes bei einer etwaigen Neufassung des LVwVfG zu berücksichtigen: Die Anforderung der Nennung von Namen und Anschrift von Grundstückseigentümern im Plan i.R.d. Anhörungsverfahrens bei Planfeststellungsverfahren wurde im Jahr 1991 (GBl. 1991 Nr. 12 vom 14. Juni 1991 S. 292, Ziff. 6) als Ergänzung in § 73 Abs. 1 S. 2 LVwVfG eingefügt. Sinn und Zweck war wohl, dass Eigentümer dadurch leichter erkennen können sollten, ob ihr Eigentum durch das Vorhaben berührt ist. Laut Gesetzesbegründung war dies als Erleichterung gedacht (LT-Drs. 10/4429, S. 91). Naturgemäß wurde damals nicht berücksichtigt, dass die Auslegung der Unterlagen in Zukunft im Internet erfolgen könnte und Eigentumsverhältnisse dadurch potenziell für jedermann weltweit einsehbar sind. Dies führt in der Praxis mittlerweile zu mehr Problemen als Erleichterungen: Pläne werden nach Auskunft eines Regierungspräsidiums uneinheitlich – mal ohne Namen und Anschriften (online) und mal mit den entsprechenden personenbezogenen Daten (in Gemeinden) – ausgelegt. Andere Regierungspräsidien verzichten (entgegen dem eigentlichen Gesetzeswortlaut) teilweise gänzlich auf Namen und Anschriften. Letztere Praxis, das Weglassen, ergibt jedoch sowohl unter praktischen als auch unter rechtlichen Gesichtspunkten Sinn: Eigentümer vermögen schließlich anhand der Flurstücknummer eindeutig zu ermitteln, ob es sich um ihr Grundstück handelt – und können daraus folgern, ob ihr Eigentum von dem jeweiligen Planfeststellungsverfahren betroffen ist. Bei Unklarheiten ließe sich über das Pseudonym in Gestalt der Flurstücknummer der Eigentumsstatus auch durch eine entsprechende Grundbuchabfrage klären. Aus einer Nennung von Namen und Anschrift in veröffentlichten Plänen ergibt sich hier kein Mehrwert, der die damit verknüpften Gefahren aufwiegt. Eigentümer könnten aufgrund der bekannt gemachten Daten potenziell von Dritten erheblich belästigt werden. Auch in rechtlicher Hinsicht erscheint § 73 Abs. 1 S. 2 LVwVfG bedenklich. Die durch die Nennung der personenbezogenen Daten verfolgten Zwecke sind in § 73 Abs. 1 S. 2 LVwVfG nicht weiter dargelegt, was äußerst fraglich erscheinen lässt, ob eine nach Art. 6 Abs. 3 S. 2 DS-GVO und gem. Art. 5 Abs. 1 lit. b DS-GVO erforderliche Festlegung der mit der Datenverarbeitung verfolgten Zwecke hinreichend erfolgt ist. Alles in allem sollte somit eine Anpassung des § 73 Abs. 1 LVwVfG erfolgen, die (gleichzeitig vereinheitlichend) zurück zur Fassung des § 73 Abs. 1 VwVfG (Bund) führt.

Stellungnahme des Landtags vom 10.11.2020:
(S.1) Die DS-GVO sehe nach einem Urteil des EuGH vom 09.07.2020 (C-272/19) für parlamentarische Tätigkeiten keine Ausnahme vom sachlichen Anwendungsbereich

vor. Eine solche Ausnahme sei jedoch bisher in § 2 Abs. 5 LDSG geregelt. Hierzu sei zu überdenken, welche Auswirkungen das Urteil für den parlamentarischen Bereich haben könnte. Sollten parlamentarische Verarbeitungsvorgänge in den Anwendungsbereich der DS-GVO fallen, wäre eine entsprechende Einschränkung von Betroffenenrechten (in §§ 8 bis 11 LDSG) in Betracht zu ziehen. Dies sei z.B. erforderlich, um im Rahmen eines Untersuchungsausschusses auf ein entsprechendes Auskunftsersuchen hin nicht preisgeben zu müssen, welche Daten bereits zu einer vor den Ausschuss geladenen Person gesammelt worden seien. Auch eine Ergänzung in § 10 LDSG („Beschränkung des Rechts auf Löschung“) wäre notwendig. Denn ohne eine entsprechende gesetzliche Vorsorge könnte eine betroffene Person bei Protokollen, in denen sie namentlich erwähnt werde, u. U. eine Einschränkung der Verarbeitung erzwingen.

LfDI: *Inwieweit die DS-GVO tatsächlich für den parlamentarischen (Kern-)Bereich gilt, war trotz des zitierten EuGH-Urteils 2020 nicht abschließend entschieden, da dies dort nicht streitentscheidend war. Deutlich in Richtung einer Anwendbarkeit auch im besagten Kontext kann man aber das jüngst ergangene Urteil des EuGHs C-33/22 vom 16. Januar 2024 lesen. Die Befunde des Gerichtshofs zu den Tätigkeiten eines Untersuchungsausschusses dürften auf andere Bereiche der parlamentarischen Tätigkeiten übertragbar sein. Wie weit § 2 Abs. 5 LDSG dann vor diesem Hintergrund im Lichte von Art. 6 Abs. 1 UAbs. 1 lit. e), Art. 6 Abs. 3 S. 1 DS-GVO Bestand haben kann, bleibt weiterer Analyse vorbehalten. Soweit nach dem genannten Urteil vom 16. Januar 2024 eine Datenschutzaufsicht auch für den parlamentarischen Bereich erforderlich ist, regen wir – mit Blick darauf, dass aus verfassungsrechtlichen Gründen eine Kontrolle der parlamentarischen Arbeit durch die Exekutive, zu der der LfDI insoweit gehört, wegen des Gewaltenteilungsprinzips untunlich ist – an, die Einrichtung einer unabhängigen Kontrollstelle beim Landtag zu prüfen, die dort die Datenschutzaufsicht übernimmt und bei deren Ausgestaltung die parlamentarischen Besonderheiten berücksichtigt werden.*

Anlässlich der Rechtsprechung des EuGH sollte außerdem überprüft werden, ob die Datenschutzordnung des Landtags, die noch aus der Zeit vor der Geltung der Datenschutz-Grundverordnung stammt, noch hinreichend aktuell ist. Für das konkret angesprochene Problem der Betroffenenrechte bei Untersuchungsausschüssen ist zu prüfen, ob das Untersuchungsausschussgesetz einschließlich seiner Verweisungen auf die Strafprozessordnung insoweit im erforderlichen Umfang angemessene Einschränkungen der Betroffenenrechte vorsieht; soweit dies nicht der Fall sein sollte, wäre dieses Gesetz als sedes materiae sachnäher als das LDSG.

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(3.4) Angeregt wird, in § 2 Abs. 6 LDSG deutlich zu machen, von welchem Unternehmensbegriff ausgegangen wird.

***LfDI:** Es ist nicht bekannt, inwieweit es hinsichtlich des Unternehmensbegriffs in der Praxis zu Einordnungs- und damit Anwendungsproblemen kommt. Etwaige Einzelfallprobleme dürften sich durch Auslegung mit Hilfe eines Rückgriffs auf die Definition des Art. 4 Ziff. 18 DS-GVO sowie die weitere Tatbestandsvoraussetzung der „Teilnahme am Wettbewerb" lösen lassen. Sollte eine Klarstellung dennoch für erforderlich gehalten werden, böte sich eine Bezugnahme auf Art. 4 Ziff. 18 DS-GVO an.*

***Vgl.** hierzu auch die – von uns nicht geteilten – Ausführungen des Sozialministeriums in dessen Stellungnahme vom 27.10.2020 zum Unternehmensbegriff bei gesetzlichen Krankenkassen im Zusammenhang mit der Möglichkeit, gegen sie Geldbußen zu verhängen, hier wiedergegeben bei § 28 LDSG.*

§ 3 LDSG

Zu § 3 Absatz 1 LDSG allgemein

Stellungnahme des LfDI vom 6. November 2020 im Rahmen der Evaluation:
§ 3 Absatz 1 S. 3 Nr. 1 LDSG lese sich derzeit so, als seien technische und organisatorische Maßnahmen ein „Kann", kein „Muss". Das widerspreche dem Wortlaut des Artikel 32 Absatz 1 HS 1 DS-GVO, wonach (unter Berücksichtigung des Stands der Technik usw.) der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen müssten, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Erst im zweiten Halbsatz zähle Artikel 32 Absatz 1 in den Buchstaben a) bis d) auf, welche Maßnahmen „gegebenenfalls" zu den TOMs gehören würden.

Stellungnahme des RP Freiburg vom 28.10.2020:
„Die Vorschrift hebt erfreulicherweise die Bedeutung des technischen und organisatorischen Datenschutzes hervor und ist als Konkretisierung der in Art. 32 Abs. 1 DSGVO als geeignet genannte Maßnahmen zielführend."

***LfDI:** Wir halten die Regelung in Absatz 1 nach wie vor für systematisch verfehlt und in der Praxis verwirrend (s. zur Kritik auch schon unsere Stellungnahme im Gesetzgebungsprozess vom Januar 2018). Die Regelung hat eine schillernde Rechtsnatur,*

die unterschiedliche Aspekte nicht deutlich genug voneinander trennt (s. auch Keber in Debus/Sticko, Landesdatenschutzgesetz Baden-Württemberg, 1. Auflage 2022, § 3 LDSG Rn. 7: ein „inkonsistenter und daher für die Normadressaten und die Rechtsanwendung problematischer Hybride"): Einerseits scheint die Norm eine Konkretisierung der technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO vornehmen zu wollen (vgl. insoweit die zitierte Stellungnahme des RP Freiburg), obwohl insoweit eine Öffnungsklausel nicht erkennbar ist; auch eine Wiederholung der Regelungen der Datenschutz-Grundverordnung erscheint für die in Erwägungsgrund 8 zur Datenschutz-Grundverordnung erwähnten Zwecke nicht erforderlich, sondern sogar kontraproduktiv. Andererseits soll die Regelung in Absatz 1 wohl – zusätzlich zu Art. 32 DS-GVO – spezifische Maßnahmen im Sinne von Art. 6 Absatz 2 und 3 DS-GVO normieren für die Verarbeitung personenbezogener Daten durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung. Dies kommt im Gesetzestext indes nicht deutlich zum Ausdruck, ohnehin bleiben die angeführten Maßstäbe und Maßnahmen und ihr Unterschied zu den ohnehin nach Art. 32 DS-GVO zu ergreifenden technischen und organisatorischen Maßnahmen zum Datenschutz beispielhaft und vage, so dass eine wesentliche Konkretisierung im Sinne einer „spezifischen Bestimmung" darin nicht gesehen werden kann (vgl. zu den Anforderungen an eine spezifische Bestimmung am Beispiel des Art. 88 DS-GVO jüngst EuGH, Urteil vom 30. März 2023 – C-34/21 [Hauptpersonalrat der Lehrerinnen und Lehrer gegen Hessisches Kultusministerium] – u. a. Rn. 61, 65, 71, 74 und dazu noch unten bei §§ 15 und 17 LDSG). Drittens soll nach der Begründung des Gesetzgebers die Norm auch eine Regelung „spezifischer Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" bei der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Absatz 2 Buchstabe g DS-GVO darstellen, ohne dass erkennbar wäre, dass in § 3 spezielle Maßnahmen für die besonderen Kategorien personenbezogener Daten tatsächlich getroffen würden (s. hierzu noch unten zu § 17 LDSG). Überdies bildet die Norm teilweise die Pflichten aus dem Unionsrecht nur unvollständig ab, etwa in Bezug auf die Verarbeitung durch Auftragsverarbeiter (s. hierzu Keber, in Debus/Sticko, LDSG BW, § 3 LDSG, Rn. 9).

Die Norm ist daher grundlegend zu überarbeiten, wobei nach den skizzierten verschiedenen ihr zugedachten Funktionen zu differenzieren ist.

Speziell zu § 3 Absatz 1 Nr. 2 LDSG

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:

(3.3) Es wird eine Vereinheitlichung der Terminologie gewünscht und dazu auf § 3

Abs. 1 Nr. 2 LDSG Bezug genommen, welcher das Erfassen, Verändern und Löschen von Daten umfasst. Hier seien weitere Verarbeitungen nach Art. 4 Nr. 2 DS-GVO nicht umfasst.

LfDI: *Generell trifft es zu, dass Terminologien, wo möglich, vereinheitlicht werden sollten. Inwieweit hier eine Ersetzung der Einzelbeschreibung von Verarbeitungsformen durch den allgemeinen Begriff der Verarbeitung erfolgen soll, bedarf indes sorgfältiger Abwägung. Einerseits können auch weitere (unberechtigte) Formen der Verarbeitung als das Erfassen, Veränderung und Löschen von hinreichender Eingriffsintensität sein, dass es angemessen sein kann, auch insoweit für eine Möglichkeit der Überprüfung und Nachvollziehbarkeit Sorge zu tragen, wie zum Beispiel die unbefugte Einsichtnahme oder die unbefugte Übermittlung. Andererseits kann es nicht das Ziel sein, standardmäßig eine vollständige, lückenlose Protokollierung im Zusammenhang mit personenbezogenen Daten zu etablieren. Eine solche würde im Ergebnis dazu führen, dass sich jeder einzelne Arbeits-/Bearbeitungsschritt vollständig nachvollziehen ließe. Eine solche vollumfängliche Kontrollmöglichkeit liefe wiederum Gefahr, unverhältnismäßig in das Recht auf informationelle Selbstbestimmung von Beschäftigten einzugreifen. Daher sollte nicht ungeprüft standardmäßig eine Vollprotokollierung im vorgenannten Sinne erfolgen. Diese Aspekte sollten im Gesetzestext zum Ausdruck kommen, wobei anzumerken ist, dass es sich bei den derzeit in § 3 Absatz 1 aufgelisteten Maßnahmen ohnehin nur um Beispiele handelt.*

Zu § 3 Absatz 2

Stellungnahme des LfDI vom 6. November 2020 im Rahmen der Evaluation des LDSG: In der Bußgeldpraxis des LfDI würden Behördenbeschäftigte, die ihre gesetzlichen Datenverarbeitungsbefugnisse überschreiten und damit gegen das Datengeheimnis des § 3 Abs. 2 LDSG verstoßen würden, wie Privatpersonen nach DS-GVO und BDSG behandelt (und damit selbst bußgeldrechtlich sanktioniert). Klarer wäre es, wenn dies ausdrücklich im LDSG geregelt würde. Es sei nicht nachvollziehbar, weshalb öffentlich Bedienstete sanktionslos gegen Datenschutzbestimmungen verstoßen können sollten.

LfDI: *An diesen Ausführungen halten wir in dieser Form aktuell nicht mehr fest. Sie waren insoweit unpräzise, als sie dahingehend verstanden werden könnten, dass jeder (z. B. auch nur fahrlässige) Verstoß gegen Datenverarbeitungsbefugnisse durch Beschäftigte öffentlicher Stellen eine bußgeldrechtliche Sanktionierung der jeweils handelnden beschäftigten Person sollte nach sich ziehen können.*

Maßgeblich für eine Sanktionierung Beschäftigter durch ein Bußgeld ist nach der inzwischen ständigen Praxis des LfDI indes nicht die Frage, ob die beschäftige Person gegen das Datengeheimnis verstoßen hat, sondern inwieweit sie personenbezogene Daten zu eigenen, nicht-dienstlichen Zwecken verarbeitet hat. Soweit Beschäftigte öffentlicher Stellen zu eigenen Zwecken Daten verarbeiten, unterfallen sie als Verantwortliche (auch sanktionsrechtlich) den Haftungsregeln der DS-GVO. In diesem Bereich ist eine Sanktionierung also möglich. Eine Sanktionierung ist dort nicht möglich, wo Beschäftigte zwar gegen Datenschutzvorschriften verstoßen, dies aber im Rahmen ihrer Tätigkeit für die öffentliche Stelle machen. In diesem Bereich ist eine Zurechnung zur öffentlichen Stelle als Verantwortliche konsequent. Eine Sanktionierung in diesem Bereich würde zu einer Schlechterstellung von Beschäftigten öffentlicher Stellen gegenüber solchen nicht-öffentlicher Stellen führen. Eine solche generelle Schlechterstellung erachten wir nicht für geboten.

Hierzu verweisen wir auch auf die Evaluationsstellungnahmen anderer Ressorts, die wir unter § 29 LDSG wiedergeben

Ergänzend weisen wir zu § 3 Absatz 2 LDSG darauf hin, dass die Konzeption des § 3 Absatz 2 LDSG mit seiner Anknüpfung an die alte Rechtslage insoweit unionsrechtsverkürzend ist, als Art. 29 und Art. 32 Absatz 4 DS-GVO anders als das landesrechtliche Konzept des gesetzlichen „Datengeheimnisses“ von einer auf Dauer angelegten (und nicht nur initialen) Pflicht des Verantwortlichen ausgehen, die Beschäftigten zur Einhaltung datenschutzrechtlicher Vorschriften anzuhalten (vgl. näher Keber in Debus/Sicko, LDSG BW, § 3 LDSG Rn. 10 ff.). Diese Bedenken sollte im Rahmen der Überarbeitung des LDSG Rechnung getragen werden. Dabei sollte freilich die Strafbarkeit von Beschäftigten unter den Voraussetzungen des § 29 LDSG erhalten bleiben.

§ 4 LDSG

Verarbeitungsbefugnis von Meldedaten zugunsten kommunaler Musik-, Kunst-, und Volkshochschulen

Stellungnahme des Oberbürgermeisters von Offenburg vom 21.10.2020:
Vorgeschlagen wird, mittels einer Konkretisierung des § 4 LDSG die Adressweitergabe von Kommunen an Musik-, Kunst- und Volkshochschulen (als Teil der kommunalen Daseinsvorsorge) zu erlauben. Begründet wird dies damit, dass die Adressierung von Kindern (insbesondere bildungsferner Schichten) nicht mehr hinreichend

möglich sei. In der Rechtsgrundlage solle in Konkretisierung des bisherigen § 4 LDSG bestimmt werden, dass kommunal getragene Musik-, Kuns- und Volkshochschulen ermächtigt werden, Adressdaten noch zu bestimmender Zielgruppen zu genau bestimmten Zwecken von kommunaler Seite erhalten und verarbeiten zu dürfen. Mit einer solchen Rechtsgrundlage könnten die Musik-, Kunst- und Volkshochschulen erheblich unterstützt werden.

LfDI: *Auch wenn die Intention generell nachvollziehbar ist, ist zunächst zu prüfen, ob gleich geeignete Mittel ohne Verarbeitung personenbezogener denkbar erscheinen, die den Zweck gleichermaßen erreichen könnten, wie z. B. eine Werbung in Bildungseinrichtungen (z.B. Grundschulen), in denen sich die Zielgruppe aufhält (sei es durch Präsenzveranstaltungen oder Aushang bzw. Auslegung von Druckerzeugnissen). Dies sollte auch unter der Geltung der Verwaltungsvorschrift des Kultusministeriums zur Werbung an Schulen vom 21.09.2002 (Az. 6499.10/417) möglich sein.*

Soweit diese Form der Werbung tatsächlich nicht ausreichen sollte, ist zwischen der Erhebungsbefugnis der Musik-, Kunst- und Volkshochschulen auf der einen Seite und der Übermittlungsbefugnis der Meldebehörden auf der anderen Seite zu unterscheiden. Hinsichtlich der Übermittlungsbefugnis der Meldebehörden ist das Landesdatenschutzgesetz nicht das richtige Regelungswerk. Insoweit ist vielmehr das Bundesmeldegesetz (BMG) maßgeblich, das insbesondere in § 46 BMG unter den dort genannten Voraussetzungen Gruppenauskünfte gestattet.

Soweit eine Erhebungs- und Verwendungsbefugnis der Kunst-, Musik- und Volkshochschulen zu Zwecken der Förderung der Bildungsanliegen der genannten Schulen geregelt werden sollte, wäre dies nicht ganz ohne Vorbild (in gewisser Weise ähnlich etwa § 2 des Gesetzes über die Zentrale Stelle zur Durchführung des Einladungswesens im Rahmen des Mammographie-Screenings). Allerdings sollte bei der Entscheidung über eine solche Aufgabenzuweisung bedacht werden, dass in den hier einschlägigen Bereichen die genannten Schulen als öffentliche Stellen vielfach mit privaten Stellen mit einem ähnlichen Leistungsangebot konkurrieren.

Als Alternative – datensparsamere –Variante wäre auch ein Adressmittlungsverfahren in Betracht zu ziehen, bei dem die Kommune die Versendung der Werbungspost im Auftrag der Kunst- oder Musikschule vornimmt, ohne der Schule gegenüber die Identität der Werbungsempfängerinnen und -empfänger offenzulegen.

Soweit das Anliegen der Kunst-, Musik- und Volkshochschulen nicht im Wege einer allgemeinen Norm zur Öffentlichkeitsarbeit öffentlicher Stellen geregelt werden soll (s. dazu noch sogleich), würde sich als sedes materiae für eine derartige Regelung eher das Kommunalrecht (und nicht das LDSG) anbieten.

Allgemeine Kritik an dem Generalklausel-Charakter von § 4 LDSG sowie an der Struktur der §§ 4-6 LDSG

Stellungnahme des Verkehrsministeriums vom 30.10.2020
(Ziff. 2) § 4 LDSG werfe in der Anwendungspraxis Schwierigkeiten auf bei der Prüfung, was unter die „erforderliche Aufgabenerfüllung“ fallen soll. Als Beispiele benannt werden Streaming von Veranstaltungen und soziale Netzwerke. Für diese Datenverarbeitungsvorgänge werden konkretisierende Vorschriften gewünscht.

Stellungnahme des Referat 35 des Innenministeriums vom 30.10.2020:
(S. 1, 2 § 4) Hingewiesen wird darauf, dass sich bzgl. § 4 LDSG, je nach Eingriffsintensität, die Frage der Wahrung des Bestimmtheitsgebots stelle. In § 4 werde aus der Zulässigkeitsvoraussetzung der DSGVO im LDSG lediglich positiv eine Ermächtigungsgrundlage formuliert; einschränkende Tatbestandsmerkmale lägen nicht vor. Hierdurch stelle sich, je nach Eingriffsintensität der jeweils vorgenommenen Datenverarbeitung, die Frage der Einhaltung des Bestimmtheitsgebots. Insbesondere habe sich dort die Frage ergeben, welche Maßnahmen/Grundrechtseingriffe zulässigerweise auf die Generalklausel des § 4 LDSG gestützt werden könnten. Konkret werde beispielsweise – trotz der Regelung in § 4 LDSG – bei Bild- und Tonaufnahmen wegen der Betroffenheit des allgemeinen Persönlichkeitsrechts zusätzlich eine Einwilligung der aufgenommenen Person für erforderlich gehalten.

Stellungnahme des Ministeriums für Umwelt, Klima und Energiewirtschaft (Umweltministerium) vom 19.10.2020:
(Ziff. 4) Gewünscht wird, dass das Verhältnis von §§ 4-6 LDSG und Art. 6 DS-GVO „klarer gestellt“, d.h. der gesamte Normenkomplex §§ 4-6 LDSG neu sortiert und in seinem Zusammenspiel klarer gefasst werde. § 6 LDSG dürfe nicht die alleinige Übermittlungsnorm sein, denn neben der zweckändernden Übermittlung in § 6 Abs. 1 LDSG gebe es auch noch andere, die nicht Abs. 2 oder 3 unterfallen, sondern über § 4 LDSG liefen. Auch das Verhältnis zu § 5 LDSG bleibe unklar.

LfDI: *Die Notwendigkeit einer die Anforderungen aus Art. 6 Absatz 1 Buchstabe e DS-GVO kaum konkretisierenden Generalklausel wird auch in der Literatur vielfach*

bezweifelt. Teilweise wird sie sogar mit Blick auf das europarechtliche Wiederholungsverbot als unzulässig angesehen (einen Überblick über die Kritik gibt insoweit z. B. Osterried in Debus/Sicko, LDSG BW, § 4 LDSG, Rn. 4 ff.). Soweit Konkretisierungen in der Generalklausel möglich erscheinen, sollten solche sicherlich vorgenommen werden; die eingegangenen Stellungnahmen enthalten hierzu indes kaum Vorschläge (zur Frage der Regulierung der Öffentlichkeitsarbeit s. noch sogleich).

Dass der Begriff der „Erforderlichkeit zur Aufgabenerfüllung" zuweilen Auslegungsschwierigkeiten birgt, ist zutreffend. Diese sind allerdings regelmäßig eher in der Frage begründet, was genau zum Kreis der Aufgaben der jeweiligen Stelle gehört; dieser ist durch das jeweils die Aufgabe der Stelle zuweisende Gesetz möglichst normenklar zu regeln. Der Begriff der „Erforderlichkeit" mag im Einzelfall auch noch als unbestimmter Rechtsbegriff Interpretationsspielräume eröffnen, erscheint aber durch die datenschutzrechtliche Rechtsprechung und Literatur grundsätzlich als ausreichend geklärt.

Zutreffend ist auch die Auffassung, dass die Generalklausel in § 4 LDSG (u.a. aufgrund der Wesentlichkeitslehre des Bundesverfassungsgerichts) nur eine subsidiäre Bedeutung haben kann, und zwar für Datenverarbeitungen mit geringer Eingriffsintensität (s. z. B. Osterried in Debus/Sicko, LDSG BW, § 4 LDSG Rn. 12 m. w. N.), und die Einschätzung, dass die Abgrenzung, wann die Eingriffsintensität hinreichend gering ist, im Einzelfall in der Praxis durchaus Schwierigkeiten aufwerfen kann. Allerdings handelt es sich hierbei nicht um eine Besonderheit der datenschutzrechtlichen Generalklausel aus § 4 LDSG; derartige Abgrenzungsprobleme des Anwendungsbereichs der Generalklausel im Verhältnis zur Eingriffsintensität und zu einzelnen Spezialklauseln gibt es auch bei anderen Regelungsmaterien (wie beispielsweise im allgemeinen oder besonderen Polizei- und Ordnungsrecht). Dennoch erscheint dort wie hier die von Praxis und Wissenschaft geschaffene Dogmatik grundsätzlich als hinreichend gefestigt, um noch von einer ausreichend normenklaren Regelung auszugehen. Die praktische Bedeutung der generalklauselartigen Regelung in § 4 LDSG für Datenverarbeitungen durch öffentliche Stellen ist indessen – insbesondere bei neuen, bislang nicht spezifisch geregelten Formen (digitaler) Datenverarbeitungen – nicht zu bestreiten.
Was die Systematik der §§ 4-6 LDSG angeht, sollte diese in der Tat noch einmal im Einzelnen einer Überprüfung unterzogen werden. So ist es beispielsweise misslich, wenn die Zulässigkeit der (nicht zweckändernden) Übermittlung eines personenbezogenen Datums rechtssicher nur im Wege eines Erst-recht-Schlusses aus der Regelung für zweckändernde Übermittlung in § 6 LDSG hergeleitet werden kann.

Anregungen zur Schaffung eines Verarbeitungstatbestandes der Öffentlichkeitsarbeit öffentlicher Stellen des Landes

In diesem Zusammenhang ist zunächst auf die unter der vorangehenden Überschrift („Allgemeine Kritik an dem Generalklausel-Charakter von § 4 LDSG...) wiedergegebenen Stellungnahmen des Verkehrsministeriums und des Referats 35 des Innenministeriums hinzuweisen, die ebenfalls die Datenverarbeitung zu Zwecken der Öffentlichkeitsarbeit betreffen.

Stellungnahme des LfDI vom 06.11.2020 im Rahmen der Evaluation des LDSG:
Das LDSG enthalte keine spezielle Norm zur Datenverarbeitung im Rahmen von Öffentlichkeitsarbeit. Es könne immer lediglich auf die Generalklausel des § 4 zurückgegriffen werden. Wie bereits in der Broschüre „Wesentliche Anforderungen an die behördliche Nutzung Sozialer Netzwerke“ des LfDI gefordert, sei die Schaffung einer Norm, die Umfang und Grenzen von Öffentlichkeitsarbeit (insbesondere) in sozialen Medien regele, dringend erforderlich, um die Arbeit der Behörden in diesem Bereich zu legitimieren. Nur so könnten rechtsklare und bestimmte Vorgaben für den immer wichtiger werdenden öffentlichen Auftritt von Behörden und anderen öffentlichen Stellen in sozialen Netzwerken geschaffen und gleichzeitig der Schutz personenbezogener Daten gewährleistet werden.

Konkret schlug der LfDI die Aufnahme der folgenden Regelung in § 4 Absatz 2 LDSG vor:

> „Als Aufgabe der öffentlichen Stelle gilt auch deren Öffentlichkeitsarbeit. Findet die Öffentlichkeitsarbeit durch Nutzung eines sozialen Netzwerks statt, ist die öffentliche Stelle für die Verarbeitung personenbezogener Daten gemäß Artikel 26 der Datenschutz-Grundverordnung gemeinsam mit dem Anbieter des sozialen Netzwerks verantwortlich. Sie hat die Einrichtung und Einhaltung geeigneter technischer und organisatorischer Maßnahmen nach der Datenschutz-Grundverordnung zu gewährleisten.“

Stellungnahme des Wirtschaftsministeriums vom 30.10.2020:
(Abs. 2) Es wird erbeten, eine Rechtsgrundlage im LDSG im Zusammenhang mit der Nutzung von sozialen Netzwerken durch Behörden aufzunehmen, da Datenauswertungen, die über die Öffentlichkeitsarbeit hinausgehen (wie Analysen des Nutzerverhaltens), nach der Orientierungshilfe des LfDI: „Wesentliche Anforderungen an die behördliche Nutzung ‚Sozialer Netzwerke‘“ vom 06.02.2020 als nicht rechtmäßig angesehen werden.

Stellungnahme des Landtags vom 10.11.2020:
(S. 3 Punkt 5) Vorgeschlagen wird die Schaffung eines Erlaubnistatbestandes (vergleichbar mit § 14 Abs. 1 LDSG) für die Öffentlichkeitsarbeit des Landtags. Als Beispiele genannt werden das Veranstaltungsmanagement (Speicherung von Adressen von Interessenten für die Teilnahme an Veranstaltungen) oder die Weihnachtspost der Landtagspräsidentin.

LfDI: *In der Tat besteht in der Praxis zuweilen eine Rechtsunsicherheit, inwieweit personenbezogene Daten im Interesse der Öffentlichkeitsarbeit einer Behörde auf gesetzlicher Grundlage, also ohne Einwilligung verarbeitet werden darf. Allerdings haben sich aus unserer Sicht in der Praxis durchaus sachgerechte Fallkonstellationen etabliert, beispielsweise dafür, dass für die Versendung von Newslettern in der Regel auch Behörden auf die Einholung einer Einwilligung angewiesen sind. Dasselbe gilt unseres Erachtens grundsätzlich für das vom Landtag so bezeichnete „Veranstaltungsmanagement", also das Speichern (und ggf. Verwenden) von Kontaktdaten von Interessierten. Dagegen könnte es grundsätzlich auf § 4 gestützt werden, wenn etwa zur Durchführung einer (in den Aufgabenbereich der öffentlichen Stelle fallenden) Veranstaltung die Speicherung von personenbezogenen Daten angemeldeter Personen erforderlich sein sollte. Ähnliches könnte für die „Weihnachtspost" oder Veranstaltungshinweise an die Dienstadressen von Bediensteten anderer öffentlicher Stellen angenommen werden, soweit es zu den Aufgaben dieser anderen öffentlichen Stelle und der angeschriebenen Person gehört, mit der die Daten verwendenden Stelle zusammenzuarbeiten bzw. sich mit den Themen von deren Veranstaltungen zu beschäftigen. Die Fertigung von Fotografien oder Videoaufnahmen von Besucherinnen und Besuchern einer Veranstaltung sowie deren Veröffentlichung dürfte dagegen zur Aufgabenerfüllung regelmäßig nicht erforderlich sein und deswegen (soweit nicht im Einzelfall Ausnahmen nach dem Kunsturhebergesetz einschlägig sein sollten) einer Einwilligung bedürfen. Diese Fälle könnten schon de lege lata grundsätzlich angemessen gelöst werden.*

Soweit dennoch im Interesse der Normenklarheit eine Regelung zur Datenverarbeitung zum Zweck der Öffentlichkeitsarbeit aufgenommen werden sollte, halten wir an der Formulierungsempfehlung aus unserer Stellungnahme vom 6. November 2020 nur noch teilweise fest. Das gilt namentlich mit Blick auf die Verwendung sozialer Netzwerke zur Öffentlichkeitsarbeit. Insoweit dürfte durch die Rechtsprechung des EuGH inzwischen hinreichend geklärt sein, unter welchen Voraussetzungen die Nutzung eines sozialen Netzwerks eine gemeinsame Verantwortung bewirkt. Die Aussage aus unserem Regelungsvorschlag, es sei bei Nutzung sozialer Netzwerke stets

von einer gemeinsamen Verantwortung auszugehen, ist im Lichte der (weiteren) technischen Entwicklung in dieser pauschalen Form nicht möglich. In Bezug auf das beispielsweise von unserer Dienststelle für andere öffentliche Stellen gehostete Mastodon gehen wir beispielsweise von einer Auftragsverarbeitung aus. Unabhängig davon, dass unser Regelungsvorschlag nur die gemeinsame Verantwortung festschreiben sollte, aber keine Rechtsgrundlage für die Übermittlung von Daten betroffener Personen seitens der öffentlichen Stelle an den Anbieter des sozialen Netzwerks begründen würde, halten wir es für zielführender und datenschutzrechtlich sicherer, wenn öffentliche Stellen für ihre Öffentlichkeitsarbeit durch soziale Netzwerke solche Anbieter auswählen, die die personenbezogenen Daten nicht auch für eigene Zwecke verarbeiten.

Weitere Anregungen im Zusammenhang mit der Öffentlichkeitsarbeit oder Sensibilisierungsmaßnahmen von Behörden:

Stellungnahme des Landtags vom 10.11.2020:
(S. 2, Punkt 1) Für Präsenzveranstaltungen solle geprüft werden, ob auch eine Opt-Out-Lösung für Fotografien der Veranstaltung zulässig wäre. Diese sollte so gestaltet werden, dass – nach entsprechender Ankündigung – diejenigen Personen, die nicht fotografiert werden möchten, dies mitteilen und sich in entsprechend eingerichtete räumliche Bereiche begeben.

***LfDI:** Ein Opt-Out ist in diesem Rahmen keine zulässige Lösung. Von den europarechtlich vorgegebenen Anforderungen an die Einwilligung (Art. 7 DS-GVO i.V.m. ErwG 32 S. 3 DS-GVO) kann insoweit nicht abgewichen werden. Im Übrigen bedarf die Veranstaltungsfotografie auch nicht per se der Einwilligung der betroffenen Personen, in bestimmten Konstellationen kann eine solche auch im Rahmen der Aufgabenerfüllung mit entsprechendem Widerspruchsrecht der betroffenen Personen (Art. 21 Abs. 1, Art. 6 Abs. 1 Buchst. e DS-GVO) erfolgen; vgl. https://www.baden-wuerttemberg.datenschutz.de/faq-kommunen/ (S. 14).*

(S. 2 Punkt 2) Bei Fortbildungs- und Sensibilisierungsveranstaltungen, die im Interesse der Informationssicherheit durchzuführen seien, sei es im Interesse des Informationsmanagements erforderlich, die Namen der Teilnehmenden zu dokumentieren, um sie für ein Audit vorzuhalten. Dies betreffe beim Landtag nicht nur Verwaltungsmitarbeitende, sondern auch Abgeordnete und Mitarbeitende in Fraktionen und Abgeordnetenbüros. Gelegentlich würden zur Durchführung von Sensibilisierungs-

maßnahmen in Form von E-Mail „Spear-Phishing“ Angriffen personenbezogene Daten auch im Internet erhoben und an Dienstleister übertragen. Der Landtag regt an, für solche Maßnahmen eine geeignete Rechtsgrundlage zu schaffen.

LfDI: *Eine Regelung erscheint zumindest nicht hinsichtlich aller genannten potenziell betroffenen Personenkreise notwendig, könnte aber aufgrund der unterschiedlichen Nutzergruppen grundsätzlich sinnvoll sein. Der Landtag ist Teil der kritischen (IT-) Infrastruktur gem. KRITIS-Liste BW (S. 17). Entsprechend ist davon auszugehen, dass insbesondere organisatorische Maßnahmen – wie Schulungen – erforderlich sein sollten, um i.S.d. Art. 5 Abs. 1 lit. f DS-GVO i.V.m. ErwG 39 S. 12 DS-GVO eine angemessene Sicherheit personenbezogener Daten zu gewährleisten. Gestützt wird dies durch die gem. Art. 32 Abs. 1 lit. d, Abs. 4 DS-GVO bestehenden Pflichten. Nachdem die Maßnahmen (Schulungen, Kontrollen) der Rechenschaftspflicht des Verantwortlichen gem. Art. 5 Abs. 2 DS-GVO i.V.m. ErwG 74 S. 2 DS-GVO unterliegen, sind sie grundsätzlich dokumentierbar und erlauben somit auch eine Verarbeitung personenbezogener Daten. Diese Verarbeitung sollte, bezogen auf die personenbezogenen Daten der Nutzerinnen und Nutzer der Landesverwaltung, zur Durchführung des Beschäftigungsverhältnisses i.S.d. § 15 Abs. 1 LDSG erforderlich sein. Denkbar sein könnte wohl die Einfügung einer Regelung hinsichtlich der Sensibilisierungsmaßnahmen, z.B. in Form der „Spear-Phishing“ Angriffe. Dies v.a., um Zugriffe auf und die Übermittlung von zu sensiblen/intimen Daten zu unterbinden.*
Auch hinsichtlich der Gruppe der nicht beim Landtag direkt beschäftigten Nutzer/innen (d.h. Abgeordneten etc.) könnte eine gesetzliche Regelung sinnvoll sein und Rechtssicherheit schaffen.

§ 5 LDSG

Stellungnahme des Ministeriums für Kultus, Jugend und Sport vom 07.10.2020:
(S. 2 „Zu § 5“) Die Darstellung in § 5 Abs. 1 sorge in der Praxis immer wieder für Verwirrung, weil dort zum einen die Nummern 1 bis 4 einzelne Zulässigkeiten zur Verarbeitung von personenbezogenen Daten vorgegeben, zudem aber mit der Formulierung „unbeschadet der Bestimmungen der EU-DSGVO“ weitere Zulässigkeiten genannten würden, dies aber in uneinheitlicher Formatierung.

Vorgeschlagen werde daher die Neufassung:
„Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig
1. gemäß den Bestimmungen der Verordnung EU 2016/679 (EU-DSGVO)

2. bis 5.“ [seitherige Nr. 1 bis 4 als neue Nr. 2 bis 5 einfügen.]

***LfDI:** Der Vorschlag scheint das Rangverhältnis zwischen DS-GVO und dem LDSG zu verkennen. Die Formulierung „unbeschadet der Bestimmungen der DS-GVO“ verweist auf die in Art. 6 Absatz 4 DS-GVO vorgesehenen sonstigen Möglichkeiten der zweckändernden Weiterverarbeitung, also insbesondere Einwilligung und Zweckkompatibilität. Eine Aufnahme dieser Vorschriften würde einerseits gegen das Wiederholungsverbot verstoßen, andererseits auch nicht zur Systematik passen, wonach Art. 6 Abs. 4 DS-GVO eine Öffnungsklausel für nationale Rechtsvorschriften zulässt. § 5 LDSG ist die Umsetzung dieser Öffnungsklausel.*

Stellungnahme des Ministeriums für Wirtschaft, Arbeit und Tourismus (Wirtschaftsministerium) vom 30.10.2020:
(Abs. 1) Aus Gründen der Rechtsklarheit und Rechtssicherheit sollte eine Rechtsgrundlage insbesondere zu Zwecken (bzw. der Zweckänderung zu) der Beantwortung von Landtagsanfragen geschaffen werden.

***LfDI:** Tatsächlich gibt es derzeit – abgesehen von Regelungen im Untersuchungsausschussgesetz und im Gesetz über den Petitionsausschuss des Landtags – keine spezialgesetzliche Regelung zur Übermittlung personenbezogener Daten zur Beantwortung von Landtagsanfragen. Hier ist vielmehr vielfach unmittelbar auf Verfassungsrecht zurückzugreifen, was in der Praxis erhebliche Verunsicherung nach sich zieht. Soweit verfassungsrechtlich zulässig, erschiene eine gesetzliche Regelung daher durchaus wertvoll für die Praxis. Mit Blick auf die wiederholt an den LfDI herangetragenen Fragestellungen besitzt der LfDI inzwischen einige Expertise in diesem Themenbereich, weswegen wir ggf. gerne auch zur Beratung im Einzelnen zur Verfügung stehen. Das Problem dürfte allerdings nicht zentral bei der Zweckänderung liegen, sondern eher bei den Fragen der Zulässigkeit der Übermittlung an sich und der Erforderlichkeit sowie bei der Vereinbarung und Schaffung korrespondierender Schutzmaßnahmen auf Seiten des Landtags. Die Zweckänderung könnte grundsätzlich noch durch den Wortlaut des § 5 Abs. 2 Nr. 1 LDSG (Aufsichts- und Kontrollbefugnisse) gedeckt sein.*

Stellungnahme des Regierungspräsidium Freiburg, Abt. 1, vom 28.10.2020:
(Ziff. 3.2) Konkretisierungsbedürftig seien die Begriffe „Abwehr erheblicher Nachteile für das Gemeinwohl […] oder zur Wahrung erheblicher Belange des Gemeinwohls“.

Dabei sei für den Regionalen Sonderstab „gefährliche Ausländer“ relevant, dass hierunter auch die Ausweisung oder Verlustfeststellung eines Ausländers subsumierbar seien.

LfDI: *Dem ist zuzustimmen. Nach Art. 23 Abs. 2 Buchst. a DS-GVO ist es Sache des Gesetzgebers, Zwecke und Ziele der Weiterverarbeitung näher festzulegen. Wegen der Weite des Begriffs „Gemeinwohl“ kann es Zweifel an der Europarechtskonformität der Regelung geben (so auch diverse Kommentierungen zur wortlautgleichen Norm des § 23 BDSG).*

Stellungnahme des Referat 35 des Innenministeriums vom 30.10.2020:
(S. 2, zu § 5 Abs. 1) Vereinzelt sei die Rückmeldung gekommen, die Tatbestände des § 5 Abs. 1 LDSG zur Zulässigkeit von Zweckänderungen seien zu eng gefasst. Relevant sei dies insbesondere bei der Zweckänderung zum Zweck der Verfolgung von Ordnungswidrigkeiten und solchen Straftaten, die die Schwelle der erheblichen Bedeutung i.S.d. § 5 Abs. 1 Nr. 1 LDSG nicht erfüllen würden.

LfDI: *Der Forderung, die Möglichkeiten zur Zweckänderung insoweit zu erweitern, ist entgegenzutreten. Die Öffnungsklausel aus Art. 23 Abs. 1 Buchst. d DS-GVO spricht eigentlich nur von Straftaten (vgl. aber zum Begriff der Straftat gem. Art. 10 DS-GVO EuGH, Urt. vom 22.6.2021 – C-439/19 –, und den Erwägungsgrund 13 zur JI-Richtlinie). Auch erscheint fraglich, ob Art. 23 Abs. 1 Buchst. e DS-GVO, auf den sich der Gesetzgeber daneben stützt, für die Weiterverarbeitung wegen Ordnungswidrigkeiten herangezogen werden kann, da es sich danach um „wichtige Ziele“ handeln muss und dies konkretisierend allein Fiskalinteressen sowie der Bereich der öffentlichen Gesundheit und der sozialen Sicherheit aufgeführt sind.*

Rückgriff kann zur notwendigen Konkretisierung auf § 44 Abs. 10 Satz 3 PolG genommen werden, wonach die Bedeutung einer Ordnungswidrigkeit erheblich ist, „wenn nach den Umständen des Einzelfalls ein Schaden für ein wichtiges Rechtsgut oder für andere Rechtsgüter in erheblichem Umfang droht oder wenn die betreffende Vorschrift ein sonstiges wichtiges Interesse der Allgemeinheit schützt.“

Anzumerken ist noch, dass sich die Einschränkung auf Taten mit erheblicher Bedeutung sich allein auf Ordnungswidrigkeiten bezieht, da Art. 23 Abs. 1 Buchst. d DS-GVO für Straftaten keine entsprechende Beschränkung vorsieht (vgl. auch § 18 Absatz 3 LDSG). Dies könnte man durch eine der Regelung in § 18 Absatz 3 LDSG entsprechende Fassung des Wortlauts klarer formulieren.

Stellungnahme des Referat 35 des Innenministeriums vom 30.10.2020:
(S. 2, zu § 5 Abs. 2) Es fehle eine Vorschrift zur Weitergabe von Daten zur Einleitung disziplinarrechtlicher Maßnahmen. Im privaten Bereich verstießen Beamte immer wieder gegen Vorschriften des Beamtenstatusgesetzes, ohne dass Straftaten oder Ordnungswidrigkeiten vorlägen. Eine Information des Dienstherrn sei daher in solchen Fällen, wenn keine Straftaten oder Ordnungswidrigkeiten vorlägen, obwohl für das Beamtenverhältnis von Relevanz, nicht möglich.

LfDI: *Die Zielrichtung bzw. die konkret in Betracht gezogene Fallkonstellation erscheint uns nicht ausreichend klar. Innerhalb einer Dienststelle lässt sich bei Pflichtverletzungen eine Verarbeitung personenbezogener Daten über § 15 LDSG legitimieren. In Betracht käme dementsprechend nur die Konstellation, dass eine öffentliche Stelle personenbezogene Daten von Beschäftigten anderer öffentlicher Stellen erhebt, im Rahmen dieser Erhebung einer Pflichtverletzung der Beschäftigten (welche keine Straftat oder Ordnungswidrigkeit darstellt) gewahr wird und nunmehr den Dienstherrn der Beschäftigten informieren möchte. Der Anwendungsbereich erscheint wenig praxisrelevant, so dass es u. E. hierfür keiner Normierung einer gesonderten Rechtsgrundlage bedarf.*

Stellungnahme des Referat 35 des Innenministeriums vom 30.10.2020:
(S. 2 § 5 Abs. 3) In § 5 Abs. 4 LDSG, der die Übermittlung insbesondere von Protokolldaten zu anderen Zwecken ermögliche, werde durch die Anfügung *„Straftaten gegen Leib, Leben oder Freiheit einer Person erforderlich sind“* ein höherer Maßstab angelegt, als dies z.B. bei der JI-RL (Art. 25 Abs. 2: *„Strafverfahren“*), BDSG (§ 76 Abs. 3: *„Strafverfahren“*) der Fall sei. Die DS-GVO enthalte hierzu keine entsprechende Regelung.

LfDI: *Eine Aufweichung der Norm durch eine Entfernung der Anforderungen des § 5 Abs. 4 LDSG könnte zu einer unverhältnismäßigen Zweckentfremdung personenbezogener (Protokoll-)daten führen, die es zu vermeiden gilt. Ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs gespeicherte Daten unterliegen einer engen Zweckbindung i.S.d. Art. 5 Abs. 1 lit. b DS-GVO. Diese spiegelt sich richtigerweise in § 5 Abs. 4 LDSG wider. Zudem ist darauf hinzuweisen, dass neben § 5 Abs. 4 LDSG weitere spezialgesetzliche Ermächtigungen zur Weiterverarbeitung, insbesondere im Straf- oder Steuerrecht, bestehen (LT-Drs. 16/3930 S. 95).*

Anlage 1 (vom 21.10.2020) zur Stellungnahme des Verkehrsministeriums vom 30.10.2020:
(Ziff. 2 a.E., Ziff. 3) Zur Ermöglichung der Weitergabe forschungsrelevanter personenbezogener Daten wird vorgeschlagen, entsprechende Öffnungsklauseln zu nutzen, um Einfügungen in § 5 LDSG bzw. §§ 12 – 19 LDSG vorzunehmen. Begründet wird dieser Vorschlag mit der bisher (nach Einschätzung des Verkehrsministeriums) fehlenden Möglichkeit der Weitergabe von Daten eines Testfelds Autonomes Fahren in Baden-Württemberg an Forschende.
(Auf diesen Vermerk wird auch in der *Stellungnahme der behördlichen DSB des Ministeriums für Inneres, Digitalisierung und Migration vom 30.10.2020* verwiesen.*)*

***LfDI:** In Bezug auf § 5 LDSG – die Zulässigkeit der Zweckänderung – bedarf es der angeregten Regelung nicht. Nach Art. 5 Absatz 1 Buchstabe b (2. Halbsatz) DS-GVO gilt allgemein eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken.*

§ 6 LDSG

Zu § 6 Absatz 1 LDSG
Stellungnahme des Kultusministeriums vom 07.10.2020, S. 2 (Überschrift: „Zu § 5“)
Der Verweis in § 6 Abs. 1 Nr. 1 LDSG auf § 5 LDSG sei wiederholt problematisch gewesen: In diesem Zusammenhang habe sich bspw. in Fällen, in denen Schulen personenbezogene Daten an die Polizei übermitteln sollten, immer wieder die Frage gestellt, ob die Voraussetzungen des § 5 LDSG (für die Zulässigkeit der Übermittlung i.S.d. § 6 Abs. 1 Nr. 1 LDSG) erfüllt seien.

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(3.5) Der 2. Halbsatz in § 6 Abs. 1 Nr. 2 LDSG sei zu streichen, da dieser eine nicht zu erklärende Dopplung zu § 6 Abs. 1 LDSG darstelle (Redaktionsversehen).

***LfDI:** Die Korrekturanregung überzeugt (vgl. auch Osterried in Debus/Sicko, LDSG BW, § 6 Rn. 35: der Halbsatz 2 aus § 6 Absatz 1 Nr. 2 habe keine gesonderte Bedeutung).*

Stellungnahme des Referat 53 des Innenministeriums vom 22.10.2020:
(S. 2 Ziff. 4.) Angeregt wird die Anpassung des § 6 Abs. 1 Nr. 2 LDSG, da diese Norm – anders als Nr. 1 – keinen Katalog von Anforderungen für die Zulässigkeit der Zweckänderung (vergleichbar § 5 LDSG) vorsehe, sondern lediglich eine Interessenabwägung. Hier solle geprüft werden, ob nicht auch die Angabe des mit den Daten verfolgten Zwecks oder Ziels erforderlich ist.

LfDI: *Dem Anliegen der Konkretisierung ist zuzustimmen. Zum einen muss § 6 LDSG, damit diesbezüglich überhaupt eine Rechtsetzungsbefugnis besteht, Art. 6 Abs. 1 Buchst. e DS-GVO genügen (öffentliches Interesse). Zum anderen muss § 6 LDSG auch die Anforderungen aus Art. 23 Abs. 1 DS-GVO erfüllen (wegen Art. 6 Abs. 4 DS-GVO). In Betracht kommen mit Blick auf die Übermittlung an nicht-öffentliche Stellen allein Art. 23 Abs. 1 Buchst. i (Rechte und Freiheiten anderer Personen) und j DS-GVO (Durchsetzung zivilrechtlicher Ansprüche). Eine Konkretisierung mit Blick hierauf wäre wünschenswert.*

Zu § 6 Absatz 2 LDSG
Stellungnahme des Ministeriums für Kultus, Jugend und Sport vom 07.10.2020:
(S. 2 „Zu § 6 Abs. 2“) Gewünscht werde eine Konkretisierung, auf welche Weise die Prüfung i.S.d. § 6 Abs. 2 S. 3 LDSG, ob ein Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden öffentlichen Stelle liege, zu erfolgen habe.
Weiterhin solle konkretisiert werden, wann gemäß § 6 Abs. 2 S. 4 LDSG Anlass bestehe, die Rechtmäßigkeit eines Ersuchens zu prüfen. Abhilfe könne es – neben weiteren Konkretisierungen – hier schaffen, wenn der ersuchten Stelle die „Benennung“ der für die Prüfung „einschlägigen Rechtsvorschrift“ mitgeteilt werden müsse.

LfDI: *Die Regelung in § 6 Absatz 2 Satz 2 und 3 LDSG gehört zwar zum Bestand der althergebrachten datenschutzrechtlichen Vorschriften. Gleichwohl ist sie weder normenklar noch sachgerecht und sollte insgesamt gestrichen werden.*

Die Regelung ist in mehrfacher Hinsicht – auch über die vom Kultusministerium angeführten Fragestellungen hinaus – nicht normenklar: So ist bereits unklar, ob die Norm auch auf die Anforderung durch eine Stelle Anwendung finden soll, die die Daten zu Zwecken der JI-Richtlinie verarbeiten will und daher selbst nicht dem Anwendungsbereich des LDSG unterfällt, so dass dieses ihnen eigentlich auch keine datenschutzrechtliche Verantwortung zuweisen kann.

Ebenso wenig ist nachvollziehbar, dass die Regelung stets für die Anforderung durch „eine öffentliche Stelle im Geltungsbereich des Grundgesetzes“ gelten soll. Dies würde auch öffentliche Stellen anderer Länder oder des Bundes erfassen. Hierfür fehlt dem Landesgesetzgeber aber die Gesetzgebungskompetenz, da die Norm nicht nur eine Privilegierung hinsichtlich der Prüfungsdichte enthält, sondern darüber hinaus die Verantwortlichkeit der ersuchenden Stelle begründet wird.

Nach Absatz 2 Satz 3 erteilt die ersuchende Stelle die Information nach Art. 14 DS-GVO. Dies ist insoweit missverständlich, als auch ohne die in Absatz 2 vorgenommene Zuordnung der Verantwortung für die Übermittlung die ersuchende Stelle die Informationspflicht nach Art. 14 DS-GVO wegen der Dritterhebung bei der übermittelnden Stelle zu erfüllen hat. Absatz 2 gibt insoweit nur die Rechtslage nach DS-GVO wieder, trifft aber keine Regelung hinsichtlich der Informationspflicht der übermittelnden Stelle nach Art. 13 Abs. 3 DS-GVO (auf Grund der Zweckänderung). Hinsichtlich der Zweckänderung erscheint es aber ohnehin sachnäher, die übermittelnden Stellen die Informationspflicht aufzuerlegen – unabhängig davon, ob die Übermittlung auf Anforderung erfolgt oder von Amts wegen.

Unklar ist weiterhin, welchen Charakter und welche Rechtsfolgen die Prüfungspflicht der übermittelnden Stelle aus Absatz 2 Satz 3 und 4 haben soll: Betrifft sie ebenfalls die datenschutzrechtliche Verantwortung mit der Folge, dass auch die übermittelnde Stelle eine solche Verantwortung – ggf. neben oder gemeinsam mit der anfordernden Stelle – trägt? Oder ist hier nur eine haftungsrechtliche Verantwortung vorgesehen? Auf welcher Öffnungsklausel sollte hier dann die Prüfungspflicht der nicht datenschutzrechtlichen Verantwortung tragenden übermittelnden Stelle beruhen?

Vor allem aber ist die Regelung nicht sachgerecht und stellt eine Überforderung der anfordernden Stelle dar: Die anfordernde Stelle wird regelmäßig zwar in der Lage sein, ihre eigene Erhebungsbefugnis zu beurteilen, da diese sich in der Regel aus derjenigen Rechtsmaterie ergibt, für die sie selbst zuständig ist. Mit der rechtlichen Erwartung des § 6 Absatz 2 LDSG, dass sie vor der Anforderung darüber hinaus auch die Übermittlungsbefugnis der übermittelnden Stelle zu prüfen und zutreffend zu bewerten hat, ist die anfordernde Stelle aber vielfach überfordert, und sie wird in der Praxis vielfach auch nicht durch die anfordernde Stelle erfüllt. Als ein Beispiel sei auf die in der Presse bekannt gewordenen Fälle hingewiesen, in denen die Polizei entgegen der engen Zweckbindung aus § 28a Absatz 4 Satz 6 des Infektionsschutzgesetzes der Freigabe von Kontaktdaten aus der Luca-App von Gesundheitsämtern forderte. Dabei hatten die handelnden Polizeibeamten offenbar die Zulässigkeit der

Übermittlung seitens des Gesundheitsamts nicht geprüft; erst die eigene Prüfung der zur Übermittlung aufgeforderten Gesundheitsämter verhinderte in diesen Fällen regelmäßig den Datenschutzverstoß, obwohl sie bei Anwendbarkeit von § 6 Absatz 2 Satz 3 und 4 LDSG wohl nicht zur Prüfung verpflichtet gewesen wäre, weil die Anforderung durchaus im Rahmen der Aufgaben der Polizei erfolgte.

Wir empfehlen daher dringend, die die Rechtslage verunklarende und in der Praxis fehleranfällige Regelung in § 6 Absatz 2 Satz 2-4 LDSG zu streichen.

§ 8 LDSG

Stellungnahme des LfDI vom 06.11.2020 im Rahmen der Evaluation des LDSG:
Die Regelung in § 8 sei in seiner aktuellen Fassung mit den Vorgaben der DS-GVO nicht vereinbar. Sie stelle weitgehend eine bloße Wiederholung der Ziele aus der einschlägigen Öffnungsklausel in Artikel 23 Absatz 1 DS-GVO dar. Es fehle an zusätzlichen konkretisierenden Angaben in Sinne von Artikel 23 Absatz 2 DS-GVO. Artikel 23 Absatz 2 DS-GVO stellt die Einhaltung des Bestimmtheitsgrundsatzes sicher. Da dessen Anforderungen nicht eingehalten sind, sei § 8 LDSG zu unbestimmt und müsse konkretisiert und grundsätzlich überarbeitet werden.

Stellungnahme des Ministeriums für Umwelt, Klima und Energiewirtschaft (Umweltministerium) vom 19.10.2020:
(S. 3, 4 Ziff. 5) Es werde eine Ergänzung in § 8 LDSG gewünscht, die Informationspflichten im Fall des Art. 13 DS-GVO weiter einzuschränken. Dem Umweltministeriums erscheine es insbesondere „nicht überzeugend“, dass die Ausnahmen von der Pflicht zur Erteilung von Datenschutzinformationen in Art. 13 Absatz 4 DS-GVO enger geregelt seien als in Art. 14 Absatz 5 DS-GVO; nach Art. 14 Absatz 5 DS-GVO müsse (gemäß Buchstabe c) beispielsweise – abweichend von Art. 13 DS-GVO – dann keine Information an die betroffenen Personen erfolgen, wenn die Übermittlung im mitgliedsstaatlichen Recht ausdrücklich geregelt sei. Unsicherheiten über die Notwendigkeit von Datenschutzinformationen bestünden daher z.B. im Zusammenhang mit Landtagsanfragen, in denen personenbezogene Daten Gegenstand waren und entsprechend an den Landtag übermittelt worden seien.

***LfDI:** Es erscheint äußerst fraglich, ob eine solche Einfügung in § 8 LDSG erfolgen sollte. Eine entsprechende Ergänzung hätte – je nach Gestaltung – den Voraussetzungen des Art. 14 Abs. 5 lit. c DS-GVO zu genügen. Problematisch erscheint in die-*

sem Zusammenhang, ob eine Einfügung in § 8 LDSG diese Voraussetzungen überhaupt erfüllen kann. Art. 14 Abs. 5 lit. c DS-GVO regelt den Entfall der Informationspflicht in Fällen, in denen die betroffene Person die Hintergründe der Erhebung oder Offenlegung der jeweiligen Rechtsvorschrift entnehmen kann, wenn die Norm also eine entsprechende Information – wie eine sonst durch einen Verantwortlichen zu erteilende – bietet und die jeweils betroffene Person dadurch Reichweite und Risiko der Datenerhebung und Weiterverarbeitung ausreichend abschätzen kann. Ein Beispiel hierfür sind Meldepflichten an Behörden zur Geldwäschebekämpfung (Taeger/Gabel/Mester, 4. Aufl. 2022, DS-GVO Art. 14 Rn. 26). Auf den Fall der Landtagsanfrage bezogen, erscheint eine solche Einfügung, gerade unter dem Gesichtspunkt, dass betroffene Personen von einer solchen Anfrage wohl i.d.R. keine Kenntnis erlangen werden, grundsätzlich unzureichend. Selbst, wenn die Datenverarbeitung der betroffenen Person bekannt sein sollte, erscheint fraglich, wie sie eine entsprechende „normative Information" im Rahmen des LDSG überhaupt auffinden können soll. Ein Blick in das LDSG wäre in diesem Fall wenig intuitiv. Eine „versteckte" Information widerspräche der Anforderung des Art. 5 Abs. 1 lit. a DS-GVO, der die Transparenz/Nachvollziehbarkeit der Verarbeitung für die betroffenen Personen gebietet. Selbst, wenn sich dies, ggf. durch nach Art. 14 Abs. 5 lit. c DS-GVO zusätzlich erforderliche, geeignete Maßnahmen, erreichen ließe, ist darauf hinzuweisen, dass diese „normative Information" dann auf konkrete Fälle (wie die Landtagsanfragen) zu beziehen und dadurch durchaus umfangreich wäre. Von einer Einfügung in § 8 LDSG wird im Ergebnis sowohl aus Transparenzgründen als auch Gründen der Umsetzbarkeit abgeraten.

Stellungnahme des Referat 53 des Innenministeriums vom 22.10.2020:
(S. 2 Ziff. 3.) Die in § 8 LDSG vorgesehene grundsätzliche Überwiegen der in den § 8 Abs. 1 Nr. 1-5 LDSG aufgezählten Fallgruppen könne dem in Art. 23 Abs. 1 DS-GVO angelegten Grundsatz der Verhältnismäßigkeit widersprechen und sollte durch eine Einzelfallabwägung ersetzt werden.

***LfDI:** Die Kritik teilen wir und verweisen ergänzend auf den bereits mit unserer Stellungnahme vom 06.11.2020 dargelegten Konkretisierungsbedarf. An unseren damaligen Ausführungen halten wir fest.*

§ 9 LDSG

Stellungnahme des LfDI vom 06.11.2020 im Rahmen der Evaluation des LDSG
Zur Klarstellung solle die Bezugnahme auf Artikel 15 DS-GVO nicht nur in der Überschrift, sondern – wie in Gesetzen sonst üblich – auch im Normtext selbst erfolgen.

Eine Einschränkung für Behörden sei sinnvoll, aber die praktische Anwendung/Umsetzung erscheine problematisch:

- Die Norm sei zu unkonkret – in der Praxis gebe es viele Rückfragen zum Anwendungsbereich.
- Eine Erläuterung des Begriffs „große Mengen von Informationen“ sei erforderlich, ebenso eine Erläuterung des Begriffs „unzumutbarer Aufwand“.
- Es sei eine Klarstellung erforderlich, ob bei der Betrachtung die jeweilige Einzelbehörde entscheidend ist oder ob es auch auf Kommunikationsvorgänge mit anderen Behörden ankommt.

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(3.6) §§ 8, 9 Abs. 1 LDSG würden die Frage aufwerfen, warum ein Verantwortlicher aufgrund von § 9 Abs. 1 LDSG eine Auskunft nach Art. 15 DS-GVO ablehnen darf, wenn eine Speicherung zu Datensicherung oder Datenschutzkontrolle erfolgt, aber gleichzeitig über diese „Erhebungen“ (sämtliche Protokollierungs- und Backupmaßnahmen) i.S.d. Art. 13, 14 DS-GVO informieren müsse. Insoweit erscheine – bezogen auf Mitarbeiterdaten – eine gesetzliche Einschränkung hinsichtlich der Informationspflicht zielführend.

LfDI: *Eine weitere Einschränkung ist nicht erforderlich oder gar zielführend. Missverständlich ist hier die Verwendung des Begriffes der „Erhebungen“. Bei der von Protokollen und Backups dürfte es sich um Speicherungen bereits anderweitig „erhobener“ Daten handeln.*

Bereits für die in § 9 Abs. 1 S. 2 LDSG vorgesehene Ausnahme ist eine Öffnungsklausel der Datenschutz-Grundverordnung schwerlich zu erkennen (vgl. im Einzelnen Debus in Debus/Sicko, LDSG BW, § 9 LDSG Rn. 4, 14 m. w. N.), so dass sie zu streichen ist.

Selbst wenn aber § 9 Absatz 1 Satz 2 LDSG in seiner bisherigen Form aufrechterhalten werden sollte, würde keine Notwendigkeit für eine entsprechende Ausnahme in § 8 LDSG (für die ebenfalls eine Öffnungsklausel nicht ersichtlich wäre) bestehen.

Verkürzungen der Rechte gem. Art. 13 ff. DS-GVO (und dadurch mittelbar am Recht der informationellen Selbstbestimmung) dürfen nur sparsam erfolgen, um die Rechte nicht vollkommen auszuhöhlen. Während die Auskunft gemäß Art. 15 die gespeicherten Inhalte selbst beträfe (und mithin die Erteilung einer Auskunft hierüber voraussetzen würde, dass die öffentliche Stelle auf diese Inhalte zugreifen würde), kann die Datenschutz-Information nach Art. 13 und 14 DS-GVO allgemein erfolgen. Angesichts des geringen Aufwandes für die Verwaltung, über die Datenverarbeitung in Form von Protokollen und Backups allgemein zu informieren, ist nicht ersichtlich, dass das Interesse der betroffenen Person an einer Information hierüber zurücktreten müsste (wie § 9 Absatz 1 Satz 2 LDSG in seiner derzeitigen Fassung für die Auskunftserteilung voraussetzt). Würde neben dem Auskunftsrecht auch noch die Informationspflicht ausgeschlossen, wären die Bereiche der Datensicherung/Datenschutzkontrolle durch die Verwaltung für den Bürger vollkommen intransparent. Das Ob und Wie, d.h. die Art und Weise der Verarbeitung, wären für Betroffene nicht mehr erkennbar. Eine Transparenz, wie sie Art. 5 Abs. 1 lit. a DS-GVO als Grundprinzip – gerade auch über die Auskunftsrechte hinausgehend – vorschreibt, wäre nicht länger gewährleistet.

Stellungnahme des Regierungspräsidiums Freiburg vom 28.10.2020
Bei den Regelungen in § 9 Abs. 2 LDSG ließen die Begriffe „eine große Menge von Informationen“ oder „unzumutbarer Aufwand“ zu viel Interpretationsspielraum und würden der Verwaltung nicht wirklich helfen. Insoweit wäre eine klarere Definition wünschenswert. Bezeichnenderweise würde diese Bestimmung die Verwaltung deutlich mehr befasst als die in Absatz 1 der Vorschrift geregelten Tatbestände.

***LfDI:** Die Kritik entspricht zwar derjenigen aus unserer Stellungnahme von 06.11.2020. Die Regelung ist indes insgesamt zu streichen, weil die Datenschutz-Grundverordnung für sie keine Öffnungsklausel enthält (s. Debus in Debus/Sicko, LDSG BW, § 9 Rn. 5). Das gewünschte Ziel, nämlich die Möglichkeit der öffentlichen Stelle, eine Präzisierung des Auskunftsverlangen zu fordern, ergibt sich bereits aus Erwägungsgrund 63 Satz 7 zur Datenschutz-Grundverordnung.*

§ 13 LDSG

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
In der Stellungnahme des Wissenschaftsministeriums wird viel Änderungsbedarf bei den forschungsrelevanten Regelungen (§ 13 LDSG) gesehen und werden größtenteils Formulierungsvorschläge unterbreitet:

(1.1) Die Schwelle für die Ermöglichung einer Datenverarbeitung für Forschungszwecke gem. § 13 Abs. 1 LDSG soll herabgesetzt und an die weniger strenge Formulierung in § 27 Abs. 1 BDSG („erforderlich“ statt „nicht oder nur mit unverhältnismäßigem Aufwand“) angepasst werden.

LfDI: *Tatsächlich ist die Vorschrift insoweit unglücklich gefasst (vgl. Keber in Debus/Sticko, Landesdatenschutzgesetz Baden-Württemberg, 1. Auflage 2022, § 13, Rn. 21 ff.), als mit der partiellen Anknüpfung an entsprechende Formulierungen vor Geltung der DSGVO eine doppelte Vorgewichtung impliziert sein könnte. Auch die vom Wissenschaftsministerium aufgegriffene Abweichung gegenüber der Parallelvorschrift im geltenden Bundesrecht ist misslich. Die Datenschutzkonferenz hat in ihrer Entschließung vom 23.11.2023 – „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“ (abrufbar unter „ https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf) – angeregt, die Regelungen zur Verarbeitung personenbezogener Daten zu Forschungszwecken (zum Beispiel nach dem Vorbild der Verwaltungsverfahrensgesetze) in Bund und Ländern im Sinne einer Wortgleichheit zu vereinheitlichen und dabei ein angemessenes und hohes Datenschutzniveau zu sichern. Sollte die Landesregierung diese Anregung aufgreifen, stünde der LfDI gerne zur näheren beratenden Unterstützung zur Verfügung.*

Aus Sicht des LfDI ist es entscheidend, dass die datenschutzrechtlichen Anforderungen auch in der Forschungspraxis umgesetzt werden. Zur Umsetzung in der Praxis wird z. B. in Niedersachen (siehe § 13 Abs. 1 S. 2 f. NDSG) gefordert, dass die Abwägungen im Zusammenhang mit dem Datenschutz aufzuzeichnen sind. Weiterhin sind nach § 13 Abs. 1 S. 3 NDSG die Datenschutzbeauftragten über Verarbeitungsvorgänge zu unterrichten. Diese Anforderungen verbessern auf der einen Seite zwar die Einhaltung des Datenschutzes. Gleichzeitig stellen Sie aber auch (hohe) Anforderungen an die Dokumentation der Forschenden. Aus Sicht des LFDIs ist es gleichwohl hilfreich, wenn die Datenschutzbeauftragten der Forschungseinrichtungen über Verarbeitungen personenbezogener Daten zumindest informiert sind. Daher schlagen wir vor, dass die Datenschutzbeauftragten in einfacher und (digitaler) Weise über Forschungsvorhaben mit personenbezogenen Daten zu unterrichten sind. Diese Unterrichtungspflicht ist zudem eine Konkretisierung der Pflicht der Forschungseinrichtung zum Führen eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 1 DS-GVO. Weiterhin halten wir es für zweckmäßig, dass die Forschungseinrichtungen freiwillige Schulungsmaßnahmen zum Thema Datenschutz, auch zur Sicherung der guten wis-

senschaftlichen Praxis (Siehe hierzu die Anforderungen zur Einhaltung der rechtlichen Rahmenbedingungen in Deutsche Forschungsgemeinschaft, Leitlinien zur Sicherung guter wissenschaftlicher Praxis, 2019, S. 16 ff: https://www.dfg.de/resource/blob/173732/4166759430af8dc2256f0fa54e009f03/kodex-gwp-data.pdf), anbieten müssen. Im Rahmen dieser Schulungsangebote wird die eigenständige Berücksichtigung des Datenschutzes von Forschenden weiter verbessert. Wir halten es daher für sinnvoll, ein solches Schulungsangebot für die Universitäten im Rahmen von § 13 LDSG festzulegen. Bei der Ausgestaltung des Schulungsangebots steht der LfDI durch seine Erfahrungen im Bereich des Bildungszentrums BIDIB (siehe https://www.baden-wuerttemberg.datenschutz.de/bildungszentrum/) gerne beratend zur Seite.

(1.2) Es sollten zusätzlich zu den Interessen der konkreten öffentlichen Stelle auch die Interessen der Allgemeinheit an einem Forschungsvorhaben im Rahmen der Interessenabwägung zu berücksichtigen sein (die der „Allgemeinheit“). Hierdurch solle ein „Gleichklang mit § 27 Abs. 1 BDSG“ erreicht werden.

LfDI: *Die Formulierung in § 13 LDSG, es sei „das Interesse der öffentlichen Stelle an der Durchführung des Forschungs- oder Statistikvorhabens“ in die Abwägung einzustellen, entspricht zwar derjenigen in § 27 BDSG, wonach es auf „die Interessen des Verantwortlichen“ ankommen soll. Die vorgeschlagene Formulierung, insoweit „die Interessen der öffentlichen Stelle oder der Allgemeinheit an der Durchführung des Forschungs- oder Statistikvorhabens“ als maßgeblich zu beschreiben, würde keinen „Gleichklang“ mit § 27 BDSG herbeiführen, sondern eine Differenz.*

Die vorgeschlagene Formulierung wäre auch insoweit missverständlich, als sie suggerieren würde, das „Interesse der öffentlichen Stelle“ sei von dem Interesse der Allgemeinheit zu unterscheiden, das alternativ für die Berechtigung zur Verarbeitung der personenbezogenen Daten genügen soll. Und was dann genau unter „dem Interesse der Allgemeinheit“ verstanden werden soll, bliebe unklar. Tatsächlich kann es aber bereits bei der bestehenden Formulierung nicht auf ein persönliches Interesse oder ein Individualinteresse der Stelle (z. B. dass sie selbst Aufwendungen erspart, wenn sie ein neues Verfahren einführt und dieses deswegen untersuchen möchte) ankommen. Maßgeblich für das auf Seiten der forschenden Einrichtung in die Waagschale zu werfende Interesse ist vielmehr das allgemein-wissenschaftliche Interesse einschließlich des Interesses am konkret angestrebten Erkenntnisgewinn und ggf. dessen Bedeutung für das Gemeinwohl (vgl. etwa zu § 27 BDSG BeckOK DatenschutzR/Koch, 46. Ed. 1.11.2023, BDSG § 27 Rn. 31).

(1.3) Es wird eine Regelung vorgeschlagen, die explizit die Forschung mit Daten erlaubt, die unter das Berufsgeheimnis fallen. Die Träger von Berufsgeheimnissen sollen dafür von diesen entbunden werden. („Ein Berufsgeheimnis steht der Datenverarbeitung zu Zwecken nach § 13 Absatz 1 bis 3 nicht entgegen“). Eine solche Regelung stünde dem Gesetzgeber gemäß Art. 9 Absatz 3 DS-GVO frei.

LfDI: *Für die Beurteilung von Fragen des Berufsgeheimnisses ist der LfDI grundsätzlich nicht die zuständige Aufsichtsbehörde (sondern die jeweilige Berufskammer). Der LfDI kann daher z. B. weder das Berufsgeheimnis durchsetzen noch dessen Verletzung sanktionieren. Der LfDI ist daher nicht in erster Linie dazu berufen, zu einer Regelung Stellung zu nehmen, die das Berufsgeheimnis betrifft.*

Gleichwohl ist die der Anregung zugrunde liegende Annahme des Wissenschaftsministeriums zutreffend, dass de lege lata in denjenigen Fällen, in denen personenbezogene Daten zu Forschungszwecken nicht durch die verarbeitende Stelle genutzt, sondern übermittelt werden sollen, eine doppelte Prüfung zu erfolgen hat, nämlich einerseits dahingehend, ob es für die Übermittlung eine datenschutzrechtliche Rechtsgrundlage gibt, und andererseits dahingehend, ob die Übermittlung mit der auf dem Berufsgeheimnis beruhenden Verschwiegenheitspflicht vereinbar ist. Die auf gesetzlicher Ermächtigung (z. B. § 31 Absatz 4 Nr. 1 des Heilberufekammergesetzes) beruhenden berufsrechtlichen Regelungen zur Schweigepflicht sehen für Ärztinnen und Ärzte in Baden-Württemberg vor, dass diese zur Offenbarung befugt sind, soweit sie von der Schweigepflicht entbunden worden sind oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist, wobei gesetzliche Aussagepflichten unberührt bleiben und die Ärztinnen und Ärzte die Patientinnen und Patienten darüber unterrichten sollen, soweit gesetzliche Vorschriften die Schweigepflicht von Ärztinnen und Ärzten einschränken (vgl. § 9 Absatz 2 der Berufsordnung der Landesärztekammer Baden-Württemberg). Ob und inwieweit es angemessen und sinnvoll wäre, eine Befreiung von der Schweigepflicht auch immer schon dann zu statuieren, wenn eine Übermittlung zu Forschungszwecken durch den Geheimnisträger datenschutzrechtlich zulässig wäre, bedarf sorgfältiger Prüfung. Mit Blick auf die durch § 2 Absatz 3 Satz 1 LDSG angeordnete Subsidiarität wäre als sedes materiae möglicherweise eine Regelung der Frage bei den Bestimmungen zum Berufsgeheimnis sachnäher.

Vorsorglich weisen wir in diesem Zusammenhang darauf hin, dass die Regelung in § 7 des Gesundheitsdatennutzungsgesetzes in der vom Bundestag im Dezember

2023 Fassung (https://dserver.bundestag.de/btd/20/097/2009785.pdf) ein strafbewehrtes Forschungsgeheimnis für die mit Gesundheitsdaten Forschenden geregelt werden soll.

(1.4) Weiter sollen klarstellende Einfügungen zur Forschung mit menschlichen Gewebe-/Körperflüssigkeitsproben erfolgen.

LfDI: *Gewebeproben eines Menschen sind selbst keine personenbezogenen Daten, ihnen lassen sich ggf. personenbezogene Daten genetische Informationen durch entsprechende biotechnische Analysen bzw. Aussagen über den Gesundheitszustand einer betroffenen Person entnehmen (vgl. Schantz/Wolff, Das neue Datenschutzrecht, C. Die unterschiedlichen Kodifikationen des Datenschutzrechts Rn. 275; Kühling/Buchner/Weichert, 3. Aufl. 2020, DS-GVO Art. 4 Abs. 13 Rn. 10).*

Worin genau das Wissenschaftsministerium hier datenschutzrechtlichen Regelungsbedarf sieht, wird nicht näher ausgeführt. Grundsätzlich sollte die Verwendung von Gewebeproben lebender Personen zur Forschung wegen der Vielzahl der aus einer solchen Probe entnehmbaren und in der Regel (z. B. aufgrund einer genetischen Analyse) personenbeziehbaren Daten einer Einwilligung der betroffenen Person vorbehalten bleiben, zumal hier auch Rechtsmaterien außerhalb des Datenschutzes (z. B. die Eigentumsfrage) betroffen sind. Für die Praxis der Forschung an den Universitätskliniken dürfte durch die mit der Datenschutzkonferenz abgestimmte Einwilligungsdokumentation die Medizin-Informatik-Initiative des TMF e. V. (s. hierzu https://www.medizininformatik-initiative.de/de/zusammenarbeit/koordinationsstelle) eine gewisse Vereinfachung eingetreten sein. Die Abstimmung mit der DSK bezieht sich dabei auf die Version 1.6d der Einwilligungsdokumente und 0.9d der zugehörigen Handreichung, s. die Pressemitteilung der DSK vom 24.04.2020, https://www.datenschutzkonferenz-online.de/media/pm/20200427_Einwilligungsdokumente_der_Medizininformatik-Initiative.pdf). Zur Überarbeitung dieser Versionen aufgrund von weiteren Verarbeitungswünsche seitens der TMF befindet sich die DSK mit dieser in einem ständigen Austausch. Eine gesetzliche Regelung erscheint uns insoweit derzeit nicht erforderlich.

(1.5) Es wird gefordert, eine Einfügung zur Forschung mit KI-Anwendungen vorzunehmen. Klare datenschutzrechtliche Anforderungen für Forschungstätigkeiten würden fehlen. Dabei geht es dem Wissenschaftsministerium um KI-Anwendungen die „im Rahmen von gemeinwohlorientierten Forschungszwecken genutzt werden sollen und die vom Land gefördert werden."

LfDI: *Zu der Frage, welche datenschutzrechtlichen Rechtsgrundlagen zum Zweck der Verarbeitung personenbezogener Daten in Anwendungen künstlicher Intelligenz zur Anwendung kommen können, hat der LfDI jüngst ein Diskussionspapier veröffentlicht (s. https://www.baden-wuerttemberg.datenschutz.de/diskussionspapier-rechtsgrundlagen-im-datenschutz-beim-einsatz-von-kuenstlicher-intelligenz/). Hier wird dargelegt, dass nach Maßgabe der dortigen Ausführungen schon unter den aktuellen rechtlichen Rahmenbedingungen der Anwendungen der KI auch zu Forschungszwecken rechtskonform eingesetzt werden können.*

Daher wäre genau zu prüfen, wo aus welchem Grund – auch unter Berücksichtigung der zu erwartenden Regelungen in Bezug auf Anwendungen künstlicher Intelligenz welcher Regelungsbedarf im Einzelnen besteht, insbesondere auch, inwieweit der Gedanke der Schaffung von KI-Reallabore in Baden-Württemberg umgesetzt werden kann und soll (vgl. Art. 53 des Entwurfs der Kommission einer KI-Verordnung) und es hierzu ergänzender Normierungen bedarf. Auch insoweit könnte der LfDI gerne die Landesregierung weiter beratend unterstützen.

(1.6) Erbeten wird ferner, dass zur Verarbeitung von Patientendaten aus der klinischen Versorgung zu Forschungszwecken keine Anonymisierung zu erfolgen hat, da es ansonsten schwierig sei, Kandidaten zu finden, die sich für Studien eignen. Insoweit sei eine Pseudonymisierung zum Datenaustausch angebracht.

LfDI: *Hier ist keine Ergänzung notwendig. So ist nicht ersichtlich, warum in solchen Fällen nicht mit einer Einwilligung gearbeitet werden können soll. Betroffene Patienten müssten schließlich auch dann, wenn sie dafür ausgewählt werden, der Studienteilnahme zustimmen und ggf. hier weiter Mitwirkungsbereit sein. Die grundsätzliche/abstrakte Frage der Bereitschaft zur Verwendung ihrer Daten im Rahmen der Suche nach einer möglichen Teilnahme an einer Studie sollte sich Patienten somit auch vorab stellen lassen. Nach einer entsprechenden Einwilligung ließen sich die Daten auch ohne eine Anonymisierung für die Zwecke der Abfrage der Bereitschaft der jeweiligen Patientin/des jeweiligen Patienten verarbeiten, an dem konkreten Studienvorhaben mitzuwirken.*

Mit Blick auf die Anregung des Wissenschaftsministeriums, für die Kandidatenfindung eine Rechtsgrundlage zur Verarbeitung der Diagnose- und Kontaktdaten kraft Gesetzes zu normieren, ist zu bedenken, dass jede Patientin/jeder Patient ein Recht darauf hat, in Ruhe gelassen zu werden und nicht ungefragt (ggf. noch Jahre nach der Behandlung) mit seiner Erkrankung konfrontiert zu werden. Ferner ist zu bedenken,

dass Kontaktdaten sich ändern können und ein mit Zeitablauf nach dem Abschluss der Behandlung zunehmendes Risiko besteht, dass durch unrichtig gewordene (Namens- und) Kontaktdaten (oder auch sonst durch Fehler bei der Übermittlung von Anfragen zu einer Studienteilnahme) die Erkrankung Dritten gegenüber offenbar werden kann.

Die Pseudonymisierung der Daten stellt ferner eine technische und organisatorische Maßnahme i.S.d. Art. 32 Abs. 1 lit. a DS-GVO dar, die ohnehin bei der Suche nach Übereinstimmungen genutzt werden sollte. Es handelt sich schließlich um Gesundheitsdaten, d.h. personenbezogene Daten der besonderen Kategorien, von deren Verarbeitung ein besonders hohes Risiko aushergeht. Der Schutz persönlicher Informationen ist im Hinblick auf die Sicherstellung des Vertrauens in die wissenschaftliche Forschung sowie die Akquirierung von Teilnehmern für wissenschaftliche Studien essentiell (BeckOK DatenschutzR/Schlösser-Rost/Koch, 38. Ed. 1.11.2021, BDSG § 27 Rn. 1).

(1.7) Gewünscht wird eine Einfügung zur Forschung mit bereits veröffentlichten, allgemein zugänglichen Daten. Es sei nicht durchweg rechtssicher festzustellen, ob i.S.d. § 13 Abs. 1 S. 1 LDSG die Forschungsinteressen gegenüber den Interessen an einem Ausschluss der Verarbeitung überwiegen.

LfDI: *Wir können nicht sicher abschätzen, wie hoch der Bedarf nach einer solchen Regelung ist. Bereits jetzt dürfte eine rechtskonforme Forschung mit bereits veröffentlichten personenbezogenen Daten nicht grundsätzlich ausgeschlossen sein.*

Die Zweckänderung selbst dürfte im Falle der Forschung durch Art. 5 Absatz 1 Buchstabe b (2. Halbsatz) DS-GVO im Allgemeinen zulässig sein. Allerdings bedarf die Forschungstätigkeit selbst darüber hinaus einer Rechtgrundlage.

Hier kann es in der Tat schwierig sein, die in die Abwägung nach § 13 LDSG einzustellenden Interessen der betroffenen Personen ohne Anhörung zu ermitteln. Bei der Beurteilung, ob bereits veröffentlichte personenbezogene Daten zu weiteren Zwecken – hier der Forschung – weiterverwendet werden dürfen, dürfte etwa als eine wesentliche Unterscheidung danach zu differenzieren sein, ob die Veröffentlichung mit dem Willen der betroffenen Person oder sonst zumindest rechtmäßig erfolgte oder ob es sich um rechtswidrige Veröffentlichungen handelt. Dies wird die forschungswillige Stelle möglicherweise – je nach Fallkonstellation – nicht ohne eine Anhörung der betroffenen Personen sicher feststellen können. Allerdings wird es hier auch eindeutige

Konstellationen geben, in denen das Einverständnis der betroffenen Person mit der Veröffentlichung offensichtlich und der Verarbeitung zu Forschungszwecken entgegenstehende Interessen nicht ersichtlich ist.

Je nach dem Gewicht des vom Wissenschaftsministerium vorgeschlagenen Wunsches nach einer Rechtsgrundlage für diese Fallkonstellation wäre grundsätzlich daran zu denken, ob hier andere Garantien für die Rechte und Freiheiten der betroffenen Personen gesetzlich eingeführt werden könnten, um den Eingriff in die Rechte betroffener Personen möglichst gering zu halten, und dies durch Verfahrensvorsorge sicherzustellen. So könnte z. B. daran gedacht werden zu regeln, dass die Angemessenheit des Vorgehens zuvor von einer einzurichtenden unabhängigen Stelle geprüft und genehmigt werden muss. Auch die gesetzliche Sicherstellung von Transparenzanforderungen und die tatsächliche Möglichkeit zur Ausübung von Betroffenenrechten einschließlich des Widerspruchs könnte zur Abmilderung beitragen. Soweit im Übrigen eine Verknüpfung der veröffentlichten personenbezogenen Daten mit weiteren Datensätzen für das Forschungsvorhaben erforderlich sein sollte, wären weitere Risiken zu bedenken und Vorsorge zu treffen (vgl. hierzu die Petersberger Erklärung der DSK vom 24.11.2022, S. 8 (abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf).

Ergänzend erlauben wir uns noch die folgenden ergänzenden Anmerkungen:

- *Eine öffentliche Stelle wird grundsätzlich generell vor einem Eingriff in das informationelle Selbstbestimmungsrecht aufgrund verfassungsrechtlicher Anforderungen (Grundrecht auf rechtliches Gehör) eine Anhörung durchführen müssen. Dies dürfte allerdings keine Vorgabe der DS-GVO sein, sondern sich allein nach dem Recht des Mitgliedsstaats richten, das hier Ausnahmen vorsehen kann (vgl. z. B. für Verwaltungsakte § 28 LVwVfG).*
- *Zu der Pflicht zur Erteilung von Datenschutzinformationen sieht Art. 14 Absatz 5 Buchstabe b DS-GVO Erleichterungen vor, die hier einschlägig sein könnten.*

(1.8) „Um exzellente interdisziplinäre Forschungsergebnisse erzielen zu können“ soll eine Klarstellung zur Möglichkeit erfolgen, Forschungsdaten an Kooperationspartner (Kooperationsverbände wie der Max-Planck-Gesellschaft, Kliniken, öffentliche Ämter) weiterzugeben.

LfDI: *Dass in der Praxis immer häufiger Forschung in Verbänden betrieben wird, ist zwar richtig. Allerdings sind auch hierfür gute Lösungen denkbar, ohne dass es einer gesetzlichen Änderung bedarf. Insbesondere können hier die Kooperationsverbände nicht als gemeinsam Verantwortliche (Art. 26 DS-GVO) gegenüber den betroffenen Personen auftreten. Soweit sie die Forschung auf Einwilligungsbasis ausüben wollen, könnte Sie sich insoweit bereits vorab Einwilligungen für die Übermittlung in die gemeinsame Verantwortung und ggf. an die verschiedenen Projektpartner einholen. In einem solchen Fall wäre der freie Austausch zugunsten der Forschungsprojekte zu gewährleisten. Bei Verarbeitung auf gesetzlicher Grundlage kann insoweit § 13 LDSG eine geeignete Rechtsgrundlage zur Übermittlung in die gemeinsame Verantwortung darstellen, ohne dass es dafür der vorgeschlagenen Ergänzung bedarf.*

(1.9) Des Weiteren wird vorgeschlagen, Abs. 3 so zu erweitern, dass die Veröffentlichung von Forschungsdaten erleichtert wird.

LfDI: *Es sollte bei der derzeitigen Formulierung bleiben, die § 27 Absatz 4 BDSG entspricht (und auch schon § 35 Absatz 3 LDSG a. F.). Auch hierbei gilt, dass der Schutz persönlicher Informationen im Hinblick auf die Sicherstellung des Vertrauens in die wissenschaftliche Forschung sowie die Akquirierung von Teilnehmern für wissenschaftliche Studien essentiell ist (BeckOK DatenschutzR/Schlösser-Rost/Koch, 38. Ed. 1.11.2021, BDSG § 27 Rn. 1). Es könnte der Bereitschaft zur Teilnahme an wissenschaftlichen Studien schwere Schäden zufügen, wenn nicht klar ist, ob Veröffentlichungen erfolgen, die im Nachhinein Rückschlüsse auf bestimmte Personen zulassen.*

Stellungnahme des Verkehrsministeriums vom 30.10.2020
Das Verkehrsministerium ist der Auffassung aufgrund der Praxiserfahrung seines Referats 42 „Elektromobilität und Fahrzeuginnovation“, dass die Nutzung von Daten mit Personenbezug für gemein-wohlorientierte Forschungszwecke wegen fehlender Auslegungshilfen und daraus resultierender Uneinheitlichkeit der Auslegung erschwert sei. Gegebenenfalls seien die datenschutzrechtlichen Anforderungen für Forschungstätigkeiten zu ergänzen, bei denen große Datenmengen mit Personenbezug erforderlich seien und die vom Land gefördert würden.

LfDI: *Die vom Verkehrsministerium gesehene Problematik ergibt sich näher aus dessen Anlage 2 zur Stellungnahme. Soweit dort davon ausgegangen wird, dass der Grundsatz der Erforderlichkeit (bzw. der Datenminimierung) hinderlich sei, dürfte die-*

ser wesentliche Grundsatz der Datenschutz-Grundverordnung für das mitgliedsstaatliche Recht nicht disponibel sein. Allerdings können für das Training einer künstlichen Intelligenz auch große Datenmengen im Sinne der Datenschutz-Grundverordnung erforderlich sein (vgl, näher zu den „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz" das bereits oben erwähnte Diskussionspapier des LfDI, Version 1.0 vom 07.11.2023, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/). Im Übrigen werden hier die Regulierungen durch die künftige KI-Verordnung der EU einschließlich der Möglichkeit zur Einrichtung sogenannter KI-Reallabore (vgl. Art. 53 des VO-Entwurfs der Kommission) zu beachten sein.

Soweit in der Stellungnahme bemängelt wird, dass eine föderale Diversität der Forschungsregelungen besteht, wird sich dies durch das LDSG allein nicht ändern lassen. Allerdings könnte sich der Landesgesetzgeber bemühen, nach dem Vorbild anderer Gesetze wie z. B. den Verwaltungsverfahrensgesetzen für eine inhaltlich übereinstimmende Normierung durch Bund und Länder hinsichtlich der Datenverarbeitung für Forschungszwecke zu sorgen. Dies entspräche auch der – mit Betonung auf die Forschung mit Gesundheitsdaten ausgesprochenen und bereits oben erwähnten – Anregung der Datenschutzkonferenz aus der Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken" vom 23. November 2023 (abrufbar z. B. unter https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf).

§ 14 LDSG

Zu § 14 LDSG wird überwiegend kein Änderungsbedarf gesehen (Landtag, Stellungnahme vom 10.11.2020). Teilweise (Landtag, a. a. O.) wird hervorgehoben, es wäre nicht praxisgerecht, die mit § 14 LDSG vorgenommene Einschränkung der Betroffenenrechte „zurückzuschrauben". Das Regierungspräsidium Freiburg schildert, dass eine Stelle die klare Regelung der Anbietungspflicht in § 14 Abs. 5 LDSG begrüßt habe. Andererseits sehe sie zugleich die Gefahr, dass im Rahmen der zunehmenden Digitalisierung von Verwaltungsprozessen die Funktion der Archive als Langzeitgedächtnis der Verwaltung und Gesellschaft beeinträchtigt werden könnte. Das staatliche Schulamt Karlsruhe schreibt, die vom Landesarchiv geforderten Akten, die seitens der Schulen nach dem Landesarchivgesetz zur Archivierung angeboten werden müssten, seien in der Breite ebenso wenig bekannt wie ein Bewertungsmodell für Unterlagen der Schulen; der Aufwand für die Schulen werde als kritisch bezeichnet.

Stellungnahme des LfDI vom 06.11.2020 im Rahmen der Evaluation des LDSG:
Die Beschränkungen, die § 14 LDSG hinsichtlich der Rechte der betroffenen Personen vornehme, seien zu weitgehend und stünden damit im Widerspruch zur Öffnungsklausel des Artikels 89 Abs. 3 DS-GVO.

In Abs. 2 werde das Recht auf Auskunft in unzulässiger Weise allein aus Gründen des Verwaltungsaufwands eingeschränkt. Der Absatz 3 schließe das Recht auf Berichtigung bei Datenverarbeitungen zu im öffentlichen Interesse liegenden Archivzwecken generell aus und gestehe den Betroffenen nur ein Recht auf Gegendarstellung zu. Damit berücksichtige die Norm nicht hinreichend, dass es auch Fälle geben könne, in denen ein gewichtiges Interesse an einer Richtigstellung besteht (bspw. zu Rehabilitationszwecken), ohne dass hierdurch die Archivzwecke unmöglich gemacht oder ernsthaft beeinträchtigt würden. Absatz 4 erscheine schließlich im Hinblick auf den Bestimmtheitsgrundsatz und die insofern von Artikel 23 Absatz 2 DS-GVO formulierten Anforderungen problematisch, da er den Wortlaut des Art. 89 Abs. 3 DS-GVO lediglich wiederhole.

LfDI: *An unserer damaligen Stellungnahme halten wir inhaltlich fest. Wir empfehlen daher (weiterhin) eine Neufassung des § 14 LDSG unter Beachtung des grundrechtsverkürzenden Charakters der Einschränkungen der Betroffenenrechte und mit nur restriktivem Gebrauch der Öffnungsklausel des Art. 89 Abs. 3 DS-GVO unter Beachtung des Verhältnismäßigkeits- und des Bestimmtheitsgrundsatzes.*
Das Wissenschaftsministerium hat ferner bereits vor einigen Jahren eine Novellierung des Landesarchivgesetzes in Angriff genommen, zu der der LfDI umfangreich beraten hat. Die Bemühungen, das Landesarchivgesetz u. a. an die Datenschutz-Grundverordnung und die zunehmende Digitalisierung anzupassen, haben aber bislang noch nicht zu einer Gesetzesänderung geführt.

§ 15 LDSG

Stellungnahme des Ministeriums für Umwelt, Klima und Energiewirtschaft (Umweltministerium) vom 19.10.2020:
(Ziff. 2) Es wird angeregt zu prüfen, ob genauere Regelungen bezüglich des Schutzes der Daten speziell von Behördenmitarbeitern und Behördenmitarbeiterinnen in das LDSG integriert werden könnten. [Anm. LfDI: Gemeint ist damit wohl insbesondere, dass explizite Regelungen zur Veröffentlichung personenbezogener Daten von Behördenmitarbeitern und Behördenmitarbeiterinnen gewünscht werden.] Als Bei-

spiel für eine explizite Regelung wird § 6 Landesverwaltungsgesetzes (LVG) genannt. Nach dieser Regelung können die an die Verwaltungsnetze angeschlossenen Verwaltungsbehörden und Stellen die Namen, Kontaktdaten, Aufgabenbereiche, Gremienzugehörigkeiten und zeitliche Verfügbarkeit ihrer Bediensteten verarbeiten und untereinander zur allgemeinen verwaltungsinternen Einsicht in elektronischen Verzeichnissen bereitstellen. In der Praxis würden insbesondere in förmlichen Verwaltungsverfahren Unsicherheiten auftreten, da dort der Bedarf, große Mengen an Dokumenten unter Zeitnot zu veröffentlichen (z. B. durch das Einstellen von Plänen und Protokollen in das Internet oder auf Anfragen nach dem Umweltinformationsrecht), besonders groß sei.

LfDI: *Zeitnot kann keine rechtfertigende Grundlage dafür sein, personenbezogene Daten zu veröffentlichen. Mit dem Hinweis auf eine etwaige Zeitnot – tatsächlich bestehend oder nicht – ließe sich der Aufwand einer Durchsicht von Dokumenten, wie bisher erforderlich, zu einfach umgehen.*

Vorsorglich verweisen wir auf die in der Sache weiterhin aktuellen Ausführungen im Beitrag „Grundsätzlich keine Namen von Beschäftigten ins Internet“ im 29. Tätigkeitsbericht 2008/2009 des Landesbeauftragten für den Datenschutz Baden-Württemberg (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/29.-T%C3%A4tigkeitsbericht-2009.pdf), dort S. 77 ff., wonach unter anderem grundsätzlich keine Namen von Beschäftigten ins Internet gehören, denn Dritte können den zuständigen Beschäftigten bei einer öffentlichen Stelle auch erreichen, wenn nur dessen Sachgebiet, die Telefondurchwahl und beispielsweise eine funktionsbezogene E-Mail-Adresse angegeben sind, und die zusätzliche Angabe des Namens trägt nicht dazu bei, dass sie die öffentliche Stelle besser oder schneller erreichen.

Für eine ausnahmsweise zulässige Veröffentlichung von Daten von Ansprechpersonen in Behörden bietet des Weiteren § 15 Abs. 1 S. 1 LDSG (§ 26 Abs. 1 BDSG nachgebildet) bereits eine ausreichende rechtliche Grundlage. So kann die Veröffentlichung von personenbezogenen Daten im Internet als erforderlich angesehen werden bei Personen, deren Tätigkeit nach außen wirkt (z. B. Behördenleitung, Abteilungs- und Referatsleitungen, Pressesprecherinnen/Pressesprecher, Ansprechpersonen für Projekte mit Bürgerbeteiligung). Ohne deren Einwilligung können folgende Daten veröffentlicht werden: Name, Vorname (s. u.), Tätigkeitsbereich (Behördenbezeichnung, Organisationseinheit), Adresse der Dienststelle, dienstliche Telefon-, Te-

lefaxnummer sowie dienstliche E-Mail-Adresse. Ob der Dienstverkehr die Bekanntgabe von Namen etc. sonstiger Mitarbeitenden im Internet erfordert, bedarf der Abwägung im Einzelfall. Derartige Entscheidungen sind aktenkundig zu machen.

Eine weitergehende Klarstellung könnte erfolgen, erscheint aber nicht zwingend notwendig.

Stellungnahme des Referat 35 des Innenministeriums vom 30.10.2020:
(S. 2 § 15) Es wird angeregt, den Anwendungsbereich von § 15 Abs. 2 LDSG bei den besonderen Kategorien personenbezogener Daten beim Verarbeitungszweck um die Begriffe „Gesundheitsvorsorge“ und „Arbeitsmedizin“ zu ergänzen. Für Zwecke des Gesundheitsschutzes von Beschäftigten könne es erforderlich sein, zweckgebunden personenbezogene Daten besonderer Kategorien nach Artikel 9 Absatz 2 DSGVO behördenintern sowie mit über- oder nachgeordneten Stellen zu verarbeiten. Gleiches gelte für Zwecke des Arbeitsschutzes, beispielsweise im Kontext des Dienstfähigkeitsmanagements.

***LfDI:** Eine erweiternde Auslegung erscheint angesichts des klaren Wortlauts problematisch. Zudem werden die benannten Bereiche bundesrechtlich von § 22 Abs. 1 Nr. 1 lit. b BDSG, der u. a. Datenverarbeitungen zum Zweck der Gesundheitsvorsorge und für die Beurteilung der Arbeitsfähigkeit des Beschäftigten regelt, erfasst. Nach der Gesetzesbegründung zum BDSG ist bei Beschäftigten in diesem Bereich § 22 Abs. 1 Nr. 1 lit. b BDSG vorrangig. Eine vergleichbare Norm gibt es im LDSG nicht, weshalb eine Erweiterung des § 15 Abs. 2 LDSG durchaus zu überlegen ist.*

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(2.1) Es solle in § 15 Absatz 5 LDSG eine Regelung aufgenommen werden, die zur Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen unter denselben Bedingungen auch die Herausgabe der Daten von Beschäftigten, die nicht selbst im Verdacht stehen, (wie z. B. von Dienstplänen) erlaubt.

***LfDI:** Das Erfordernis einer gesonderten Rechtsgrundlage wird nicht gesehen. § 15 Abs. 5 LDSG stellt eine Rechtsgrundlage für besonders eingriffsintensive Maßnahmen dar. Dementsprechend zielt die Norm nur auf die jeweiligen Verdächtigen. Datenverarbeitungen sonstiger Beschäftigter in dem Kontext der Aufdeckung von Straftaten oder Pflichtverletzungen, welche keine eingriffsintensiven Maßnahmen darstellen, sind – jedoch nur soweit im Einzelfall auch tatsächlich erforderlich – von der allgemeinen Rechtsgrundlage des § 15 Abs. 1 LDSG gedeckt.*

Zusätzlich sollte eine Klarstellung erfolgen, dass die Verarbeitung biometrischer Daten grundsätzlich untersagt ist, außer zu den genannten Zwecken. Der Wortlaut der Norm könnte nämlich so verstanden werden, dass lediglich die Verarbeitung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken untersagt ist, zu anderen Zwecken aber nach den Grundsätzen des Absatz 2 zulässig bleibe.

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(2.2) Verarbeitungen biometrischer Daten Beschäftigter würden i.d.R. durch eine Dienstvereinbarung generell geregelt. Die Formulierung in § 15 Abs. 6 LDSG a.E. verlange jedoch zusätzlich: *„**und** für die Datenverarbeitung besteht **jeweils** ein dringendes dienstliches Bedürfnis.“* und stelle somit auf den jeweiligen Einzelfall ab. So sei z.B. ein flächendeckendes Zutrittskontrollsystem auf dem Campus einer Universität ausgeschlossen. Es werde angeregt, dass das Wort *„jeweils“* entfalle, da sonst eine generelle Vereinbarung mit der Personalvertretung ausgeschlossen sei. (Folge: Es wäre nicht mehr für jeden Einzelfall ein dringendes dienstliches Bedürfnis erforderlich.)

***LfDI:** Dem ist nicht zu folgen. Biometrische Daten unterliegen nach der DS-GVO einem besonderen Schutz, s. Art. 9 DS-GVO. Sie dienen als individuelle und universale Identifikatoren natürlicher Personen. Gerade aufgrund des hohen Risikos, das von einer umfangreichen Verarbeitung biometrischer Daten, noch dazu von Beschäftigten, ausgeht, wäre eine Streichung von Schutzmechanismen verfehlt.*

*Auch der Wunsch nach einer Pauschallösung für flächendeckende biometrische Zugangskontrollsysteme ändert hieran nichts. So erfordert z.B. ein dringendes dienstliches Bedürfnis, den Zugang zu **einzelnen** Räumlichkeiten/Bereichen über die Abfrage biometrischer Daten zu regeln, nicht die entsprechende Überwachung des Zugangs zum **gesamten** Gebäudekomplex. Wo im Einzelfall mangels dienstlichen Bedürfnisses bzw. wegen verfügbarer milderer Mittel kein biometrisches Zugangskontrollsystem erforderlich ist, darf ein solches nicht eingerichtet werden. So könnten zur allgemeinen Zugangskontrolle bspw. auch persönliche Passwörter, Chipkarten oder Transponder zum Einsatz kommen. Biometrische Zugangskontrollsysteme erscheinen allenfalls dort denkbar, wo besondere Sicherheitsanforderungen bestehen. Um dies festzustellen, bedarf es aber gerade einer Einzelfallbetrachtung, wie sie derzeit gesetzlich – auch als Ausdruck des Art. 88 Abs. 2 DS-GVO, welcher geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen verlangt – vorgesehen ist. Diese kann nicht entfallen.*

Stellungnahme des Landtags vom 10.11.2020:
(S. 3, Punkt 3) Es wird angeregt zu prüfen, ob rechtliche Voraussetzungen für biometrische Methoden zur Absicherung des Zugangs zu informationsverarbeitenden Geräten geschaffen werden können, soweit dadurch ein höheres Sicherheitsniveau erreicht werden kann als mit alternativen Methoden und dies aus Sicht des Verantwortlichen angemessen ist.

LfDI: *Von einer solchen Regelung ist abzusehen, nachdem für eine solche keine Erforderlichkeit erkennbar ist. Eine Verarbeitung biometrischer Daten zur Zugangskontrolle käme nur in Betracht, wenn kein gleich wirksames Mittel vorhanden ist, welches das Persönlichkeitsrecht der Beschäftigten weniger stark beeinträchtigt. Zudem muss eine umfassende Abwägung der schutzwürdigen Interessen und Grundrechte der Beschäftigten mit den Interessen des Verantwortlichen zu dem Ergebnis kommen, dass die Beeinträchtigung durch das biometrische Verfahren in einem angemessenen Verhältnis zu dem angestrebten Zweck der Datenverarbeitung steht. § 15 Abs. 6 LDSG bietet insoweit einen sinnvollen Rahmen. Passwörter bieten bisher – bei ausreichender Länge und Gestaltung – eine adäquate Möglichkeit, um Zugänge technisch hinreichend abzusichern. Gerade in Verbindung mit einem weiteren (z.B. physischen) Faktor im Rahmen einer Zwei-Faktor-Authentifizierung lässt sich das Schutzniveau auch ohne die Nutzung biometrischer Merkmale auf einen äußerst hohen Stand bringen. Zudem bieten nicht alle biometrischen Verfahren und Systeme aus sich heraus eine ausreichende Sicherheit, um z.B. dem Identitätsdiebstahl oder einer sonstigen Verwendung der sensiblen Daten vorbeugen zu können. Anders als von entwendeten Passwörtern geht von entwendeten biometrischen Daten eine viel größere Gefahr aus, nachdem sich diese nicht einfach verändern lassen, sondern dauerhaft mit der jeweiligen Person verknüpfbar bleiben. Eine freiwillige Möglichkeit der Nutzung biometrischer Merkmale i.S.d. § 15 Ab. 6 LDSG zur Absicherung von Zugängen (auf Grundlage einer Einwilligung, an deren Freiwilligkeit jedoch hohe Anforderungen zu stellen sind, vgl. § 26 Abs. 2 BDSG, und bei Vorliegen eines dienstlichen Bedürfnisses) wird dadurch nicht beeinträchtigt.*

Stellungnahme des Landtags vom 10.11.2020:
(S. 3, letzter Punkt) In Bezug auf § 15 LDSG wird angeregt, eine Rechtsgrundlage für eine Kommunikation über Parlaments- und Behördengrenzen hinweg (und das Vorhalten entsprechender Kontaktdaten) zu entwickeln. Wer die Kontaktdaten angebe, willige zwar konkludent in die Kontaktaufnahme ein, aber eine Rechtsgrundlage sei besser als eine Einwilligung.

LfDI: *Die exakte Intention und Stoßrichtung erscheint hier nicht so recht nachvollziehbar. Soweit damit – über die oben bereits erwähnte Vorschrift des § 6 LVG hinaus – die Kommunikation des Parlament- und Verwaltungsaufbau untereinander gemeint ist, fehlt es hierfür der Festlegung eines Zweckes (Art. 5 Abs. 1 Buchst. b DS-GVO) sowie der Erforderlichkeit hierfür. Zudem ist zu bedenken, dass eine vollständige Freigabe sämtlicher Adressbücher untereinander die tatsächliche Problematik beinhalten könnte, dass deutlich über 500.000 Personen im öffentlichen Dienst des Landes beschäftigt sind (Pressemitteilung des statistischen Landesamtes 89/2020 vom 29.04.2020). Bestehende Namensgleichheiten und dadurch fehlgehende E-Mails/dadurch auftretende Datenpannen sind dabei nur einige der zu erwartenden Probleme. Des Weiteren ist kein Grund ersichtlich, warum z.B. ein Beschäftigter eines Bürgeramts Zugang zu sämtlichen Kontaktdaten Parlamentsangehöriger haben sollte. Dies birgt ein gewisses Missbrauchsrisiko. Zudem dürfte der Umfang einer solchen Verarbeitung personenbezogener Daten mit Rücksicht auf die elementaren Grundsätze der Datenminimierung bzw. Datensparsamkeit gem. Art. 5 Abs. 1 lit. c DS-GVO und den Anforderungen gem. Art. 25 Abs. 2 S. 2 DS-GVO unzulässig sein. Soweit dagegen die Kommunikation und das Vorhalten von Kontaktdaten von Bürgerinnen und Bürgern gemeint sein sollte, können sich Behörden im Rahmen ihrer Aufgabenerfüllung grds. auf § 4 LDSG stützen, soweit die Verarbeitung der Kontaktdaten für die jeweilige Aufgabenerfüllung erforderlich ist. Hierbei sind jedoch wiederum die Grundsätze der Datenminimierung und Speicherbegrenzung, Art. 5 Abs. 1 lit. c und e DS-GVO, die ein dauerhaftes Vorhalten personenbezogener (Kontakt-)Daten ohne Erforderlichkeit zu festgelegten Zwecken verbieten.*

Weitere Stellungnahme des LfDI zu § 15 LDSG

Zu der Frage, inwieweit das Urteil des Europäischen Gerichtshofs vom 30. März 2023 – C-34/21(Hauptpersonalrat der Lehrerinnen und Lehrer ./. Hessisches Kultusministerium) – Anpassungsbedarf in Bezug auf § 15 LDSG hervorruft, verweisen wir auf die FAQ „Rechtsgrundlagen bei Beschäftigtendaten“ auf unserer Homepage (https://www.baden-wuerttemberg.datenschutz.de/faq-rechtsgrundlagen-bei-beschaeftigtendaten/).

Im Übrigen halten wir an unserer Stellungnahme vom 06.11.2020 fest, derzufolge § 15 Absatz 6 Halbsatz 2 LDSG nicht normenklar ist und überarbeitet werden muss.

§ 16 LDSG

Stellungnahme des Kultusministeriums vom 7.10.2020

Im Rahmen des § 16 Abs. 1 LDSG stelle sich die Frage, was öffentliche Auszeichnungen seien, ob etwa die Ehrungen von Abiturientinnen und Abiturienten für herausragende Leistungen ohne Einwilligung erfolgen könnten, diese Auszeichnungen also unter „öffentliche Auszeichnung und Ehrungen“ subsumiert werden könnten. Es solle daher näher bestimmt werden, was öffentliche Auszeichnungen seien.

Stellungnahme des Innenministeriums vom 28.06.2021:.
(3.9) Die Norm regelt nur öffentliche Auszeichnungen und Ehrungen. Eine entsprechende Regelung für an Hochschulen vorgenommene Auszeichnungen und Ehrungen würde das Durchführen von z.B. Bachelorfeiern deutlich vereinfachen.

LfDI: *Es ist nicht ersichtlich, dass die Durchführung von Bachelorfeiern oder die Ehrungen von Abiturienten mit der öffentlichen Ehrung oder Auszeichnung durch bspw. eine Gemeinde vergleichbar wäre. Für eine Ausweitung der gesetzlichen Erlaubnis ist die Vereinfachung von Verwaltungsabläufen kein hinreichender Grund.*

Bereits für § 16 LDSG ist keine hinreichende Öffnungsklausel ersichtlich, um zu den genannten Zwecken in erheblicher Weise in die Grundrechte der betroffenen Person einzugreifen und Betroffenenrechte auszuschließen. Dabei ist zu bedenken, dass die Verarbeitung zu diesen Zwecken teilweise auch Daten zu strafrechtlichen Verurteilungen u.a. sensible Daten umfasst.

Erst recht ist für eine entsprechende Regelung für an Hochschulen oder Schulen vorgenommene Auszeichnungen und Ehrungen wie Bachelorfeiern eine Öffnungsklausel nicht ersichtlich.

In anderen Bundesländern mit vergleichbaren Regelungen zu öffentlichen Auszeichnungen und Ehrungen sind Betroffenenrechte explizit aufgenommen (vgl. nur § 30 Abs. 4, 5 BbDSG; § 13 Abs. 3, 4 DSG M-V). Eine entsprechende Ergänzung sollte, soweit § 16 LDSG überhaupt beibehalten werden soll, auch im LDSG erfolgen.

§ 17 Absatz 2 LDSG
Stellungnahme des Sozialministeriums vom 27.10.2020 (S. 5, Abs. 2):
Das LDSG solle Lücken der DS-GVO schließen. So nenne bspw. Art. 9 DS-GVO nicht sämtliche sensiblen Merkmale, aufgrund derer Menschen diskriminiert werden könnten, wie z.B. Daten, die Rückschlüsse auf den sozialen Status zulassen. Ziel sollte sein, ein einheitliches Datenschutzniveau für alle sensiblen Daten herzustellen, die ein Diskriminierungsrisiko bergen (können).

LfDI: *Eine entsprechende Einfügung sollte mit Vorsicht überdacht werden. Die Frage der wirtschaftlichen und sozialen Identität wurde vom europäischen Verordnungsgeber im Rahmen der Definition der personenbezogenen Daten ausweislich Art. 4 Nr. 1 DS-GVO durchaus gesehen, aber gleichzeitig nicht in den Rahmen des Art. 9 DS-GVO eingefügt. Art. 9 Abs. 4 DS-GVO sieht eine Möglichkeit für weitere Beschränkungen lediglich für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten vor (vgl. auch ErwG 53 S. 4 DS-GVO). Für die generelle Gleichsetzung zusätzlicher Arten personenbezogener Daten in die von der DS-GVO definierten besonderen Kategorien personenbezogener gäbe es mangels Öffnungsklausel wohl keinen Raum. Denkbar und durchaus wünschenswert wäre es allerdings, im Rahmen der Öffnungsklauseln aus Art. 6 Absatz 1 Buchstabe c und e, Absatz 2 und 3 spezifischere Anforderungen für weitere sensible Datenarten zu regeln, soweit diese von öffentlichen Stellen des Landes zur Erfüllung ihrer Aufgaben oder zur Erfüllung von (landesrechtlichen) Pflichten verarbeitet werden.*

Weitere Anmerkung des LfDI zu § 17 Absatz 2 LSDG
Der Standort der Regelung sollte geändert und die Regelung selbst inhaltlich konkretisiert werden.

Die Regelung soll nach der Gesetzesbegründung (LT-Drs. 16/3930, 106) allgemeinen auf der Grundlage der Öffnungsklausel aus Art. 9 Absatz 2 Buchstabe g DS-GVO einen Auffangtatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten darstellen, falls eine bereichsspezifische Regelung nicht zur Verfügung stehe. Sie soll nach der Gesetzesbegründung darüber hinaus auch die Zweckänderung besonderer Kategorien personenbezogener Daten unter den genannten Voraussetzungen regeln.

Dass diese Art der Generalklausel vor dem europäischen Recht Bestand hat, erscheint durchaus zweifelhaft. Die Beschreibung des Verarbeitungszwecks, die Verarbeitung sei „aus Gründen eines erheblichen öffentlichen Interesses“ erforderlich, stellt eine bloße Wiederholung des Wortlauts der Öffnungsklausel dar, die keinerlei Konkretisierung enthält. Auch verfassungsrechtlich ist zweifelhaft, ob sie insoweit den Anforderungen an die Bestimmtheit der Norm und aus der Wesentlichkeitstheorie des Bundesverfassungsgerichts genügt. Überdies ist nicht erkennbar, dass die Vorschrift – wie von der Öffnungsklausel vorausgesetzt – angemessene und spezifische(!) Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

Die Gesetzesbegründung (a. a. O.) verwies hierzu darauf, dass in § 3 LDSG generell angeordnet werde, angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person zu treffen. Diese Maßnahmen seien immer zu treffen, hätten aber bei der Verarbeitung besonderer Kategorien personenbezogener Daten besondere Bedeutung, um dem Verhältnismäßigkeitsprinzip Rechnung zu tragen. Sie seien nämlich an die jeweilige Schutzbedürftigkeit anzupassen.
Diese Begründung lässt indes nicht erkennen, dass deswegen spezifische Maßnahmen angeordnet würden. Im Gegenteil soll die in Bezug genommene Regelung in § 3 ja gerade unabhängig davon gelten, ob besondere personenbezogene Daten verarbeitet werden oder nicht. Somit lässt auch die Begründung nicht erkennen, welche spezifischen Maßnahmen gerade bei besonderen Kategorien personenbezogener Daten getroffen werden sollen. Der EuGH hat indes jüngst zu Art. 88 DS-GVO klargestellt, dass bei Öffnungsklauseln, die „spezifische" mitgliedsstaatliche Vorschriften zulassen, die umsetzende Norm des Rechts des Mitgliedsstaates konkretere Regelungen enthalten muss und sich insbesondere nicht in einer bloßen Wiederholung von Vorschriften des Datenschutz-Grundverordnung erschöpfen darf (EuGH, Urteil vom 30. März 2023 – C-34/21 [Hauptpersonalrat der Lehrerinnen und Lehrer gegen Hessisches Kultusministerium] – u. a. Rn. 61, 65, 71, 74).

Die Regelung, auf die in der Praxis durchaus oft zurückgegriffen wird, unterliegt daher einem hohen Risiko, europarechtlich unzureichend zu sein (ähnlich kritisch zu Recht auch Debus in Debus/Sicko, LDSG BW, § 17Rn. 3, 4 6, 32 m. w. N.) und sollte daher dringend überarbeitet, insbesondere hinsichtlich des Anwendungsbereichs und der spezifischen Maßnahmen konkretisiert werden.

Unabhängig davon ist der Standort der Regelung verfehlt. Die Aufnahme in § 17 Absatz 2 LDSG verleitet in der Praxis vielfach zu dem Missverständnis, die Norm gelte nur für die Fälle des § 17 Absatz 1 LDSG (also die Zuverlässigkeitsüberprüfungen). Die Regelung soll aber ausweislich der oben wiedergegebenen Begründung des Gesetzentwurfs weit darüber hinaus Bedeutung erlangen. Soweit sie – ggf. in überarbeiteter Form – aufrecht erhalten bleiben soll, wäre es daher empfehlenswert, ihr einen eigenen Paragraphen zu widmen.

Soweit in der Begründung des Gesetzentwurfs (LT-Drs. 16/3930, S. 106) ferner die Ansicht vertreten wurde, die Vorschrift des § 9 Absatz 2 LDSG regele „auch die Zweckänderung besonderer Kategorien personenbezogener Daten unter den genannten Voraussetzungen", kommt dies im Wortlaut der Vorschrift in keiner Weise

zum Ausdruck. Im Übrigen wäre weder erkennbar, dass ein derartig pauschaler Regelungsgehalt mit den Vorgaben aus Art. 6 Absatz 4 DS-GVO vereinbar wäre (wonach eine mitgliedsstaatliche Rechtsvorschrift in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellen müsse), noch wie sich ein solcher Regelungsgehalt zu der Vorschrift des 5 Absatz 1 LDSG verhalten solle. Es wird daher angeregt, bei der Neufassung von § 17 Absatz 2 LDSG auch zu der Frage der Zulässigkeit einer Zweckänderung Stellung zu nehmen und auf diese Weise klarzustellen, dass die Ausführungen aus der Begründung des Entwurfs 19.04.2018 keine Gültigkeit (mehr) haben.

§ 18 LDSG

1. Kritik am Merkmal „öffentlich zugänglicher Räume“:
In verschiedenen Stellungnahmen wird kritisiert, dass sich der Regelungsbereich der Norm auf öffentlich zugängliche Räume beschränke und damit unklar bleibe, inwiefern öffentliche Stellen des Landes in nicht öffentlich zugängliche Räume eine Videoüberwachung durchführen dürften. Der Bedarf einer Videoüberwachung könne aber auch bei nicht öffentlich zugänglichen Räumen bestehen.

So könne insbesondere an Baustellen ein solcher Bedarf zur Videoüberwachung zur Vermeidung von Diebstählen (durch unbefugte Dritte oder durch Mitarbeitende der dort tätigen Bauunternehmen) und zur Verhinderung von betrügerischen Abrechnungen durch Auftragnehmer etwa in Bezug auf angeblich erfolgter Zusatzarbeit am Wochenende bestehen (so der *Datenschutzbeauftragte des Finanzministeriums in seiner Stellungnahme vom Mail vom 26.10.2020*).

Oder es wird vorgeschlagen, die Schaffung einer Rechtsgrundlage zu prüfen, mit der die Bild- und Audioüberwachung in den Bereichen von Rechnerräumen oder Serverschränken in Rechnerräumen erlaubt wird, um zu verhindern, dass sich eigenes oder fremdes Personal rechtswidrig Zugang zu Informationen verschafft (*so die Stellungnahme des Landtags vom 10.11.2020,* S. 3, Punkt 4).

Oder es wird darauf hingewiesen, dass im Universitätskontext und im Großforschungsbereich bestimmte Räumlichkeiten (z. B. aufgrund eines atomrechtlichen Kontexts) nicht öffentlich zugänglich seien *(Stellungnahme des Wissenschaftsministeriums vom 28.06.2021, Punkt 2.3).* Die Videoüberwachung sei allerdings auch dort zur Ausübung des Hausrechts zuweilen notwendig, namentlich bei Vorliegen von

Sachverhalten i.S.d. § 18 Abs. 1 LDSG. Dafür sei eine Heranziehung von § 15 Abs. 1 LDSG als Rechtsgrundlage nicht zielführend, da sich dort zulässiger Weise auch z. B. Dienstleister oder Studierende aufhalten könnten.

LfDI: *In der Tat ist die Rechtslage umstritten, unter welchen Voraussetzungen öffentliche Stellen (in Baden-Württemberg, vgl. für Bundesbehörden aber auch § 4 BDSG) per Videoüberwachung personenbezogene Daten in nicht öffentlich zugänglichen Räumen verarbeiten dürfen. Als öffentlich zugänglich werden dabei nur solche Räume angesehen, die ihrem Zweck nach dazu bestimmt sind, von einer unbestimmten Zahl oder nach nur allgemeinen Merkmalen bestimmten Personen betreten und genutzt zu werden (vgl. BAG, NZA 2004, 1282; Debus in Debus/Sicko, LDSG Baden-Württemberg, § 18 Rn. 48 ff.). Nach im deutschsprachigen Bereich herrschender Auffassung kommt insoweit ein Rückgriff auf Art. 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO aufgrund des Ausschlusses durch Art. 6 Absatz 1 Unterabsatz 2 DS-GVO nicht in Betracht. Nach anderer Auffassung ist jedoch zu bedenken, dass etwa der Zweck der Sicherung des Eigentums einer öffentlichen Stelle sich nicht zwingend von der Sicherung privaten Eigentums unterscheide; wenn eine öffentliche Stelle eine solche Videoüberwachung vornehme, handele sie also nicht „in Erfüllung ihrer Aufgaben“, sondern eine solche Videoüberwachung sei wie eine fiskalische Tätigkeit anzusehen, so dass auch eine Behörde auf Art. 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO zurückgreifen könne. Innerhalb der herrschenden Ansicht, die die Anwendung von Art. 1 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO ablehnt, wird dagegen zum Teil vertreten, dass eine Videoüberwachung in nicht öffentlich zugänglichen Bereichen keine große Zahl an Personen betreffe, die keinen Anlass für ihre Beobachtung gegeben habe. Deswegen sei von einer geringeren Eingriffsintensität als bei Videobeobachtung öffentlich zugänglicher Räume auszugehen, so dass als Verarbeitungsgrund § 4 LDSG herangezogen werden könne; andere gehen hingegen davon aus, dass der Rückgriff auf § 4 LDSG wegen des abschließenden Charakters der Regelung in § 18 LDSG ausgeschlossen sei (vgl. zum Meinungsstand etwa Debus, LDSG BW, § 18 Rn. 52 und LfDI BW, Videobeobachtung durch öffentliche Stellen in Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/03/Video%C3%BCberwachung-durch-%C3%B6ffentliche-Stellen-in-Baden-W%C3%BCrttemberg.pdf, S. 20 f.).*

Aus unserer Sicht ist daher der Wunsch nach einer Klarstellung, was für die Überwachung nicht-öffentlich zugänglicher Bereiche gelten soll, nachvollziehbar. Insoweit ist nach dem Grund zu fragen, warum der Gesetzgeber überhaupt zwischen öffentlich zugänglichen und nicht öffentlich zugänglichen Räumlichkeiten unterscheidet. In der

Rechtsprechung wird hierzu zum Teil angenommen, eine Überwachung nicht öffentlich zugänglicher Bereiche begründe eine im Vergleich zu dem bereits intensiven Eingriff durch eine Videoüberwachung in öffentlichen Bereichen noch einmal gesteigerte Eingriffsintensität. Dieser äußerst intensive Eingriff ergebe sich u.a. daraus, dass von einer Videoüberwachung in nicht öffentlichen Bereichen vorwiegend Beschäftigte betroffen wären und diese sich der Überwachung regelmäßig nicht entziehen könnten. Der Personenkreis der beobachteten Personen sei zudem überschaubar und dem Arbeitgeber bekannt, was einen erhöhten Überwachungs- und Anpassungsdruck mit sich bringe (vgl. BAG, NZA 2004, 1278 [1282]). Die Gleichsetzung von Videoüberwachung in nicht öffentlich zugänglichen Bereichen mit dem Anwendungsbereich des Beschäftigtendatenschutzes ist freilich nicht vollständig überzeugend: Zum einen können von einer Videobeobachtung in nicht öffentlich zugänglichen Räumen auch Personen betroffen sein, die nicht Beschäftigte des Verantwortlichen sind (z. B. Besucher, Lieferanten, Dienstleister, Einbrechende); zum anderen können auch von einer Videoüberwachung im öffentlich zugänglichen Räumen Beschäftigte des Verantwortlichen betroffen sein. Richtigerweise sind daher die Anforderungen des Beschäftigtendatenschutzes (z. B. § 15 Absatz 7 LDSG, s. LfDI BW, a. a. O., S. 8) bei der Videoüberwachung im öffentlich zugänglichen Raum zusätzlich zu § 18 LDSG zu berücksichtigen.

Eher spricht für einen erhöhten Schutzbedarf nicht öffentlich zugänglicher Bereiche, dass in öffentlich zugänglichen Bereichen typischerweise ohnehin damit zu rechnen ist, dass man beobachtet wird (wenngleich nicht unbedingt per Videoüberwachung), und die betroffenen Personen typischerweise ihr Verhalten ohnehin dem aufgrund der öffentlichen Zugänglichkeit bestehenden Beobachtungsdruck anpassen.

Aus diesem Grund sollte eine etwa zu schaffende Rechtsgrundlage für die Videobeobachtung sich auf enge Anwendungsfälle beschränken und keinesfalls die Anforderungen unterschreiten, die nach der geltenden Rechtslage an die Videoüberwachung öffentlich zugänglicher Räume gestellt werden. Insbesondere sollten dabei keinesfalls die zulässigen Zwecke der Videoüberwachung erweitert oder die Anforderungen an die Gefahr im Sinne von § 18 Absatz 1 Nr. 1 oder 2 LDSG herabgesetzt werden. Die Videoüberwachung könnte insbesondere für den Fall explizit gestattet werden, dass eine öffentliche Einrichtung ihre Innenräume zu Zeiten überwachen will, zu denen mit der Anwesenheit berechtigter Personen in den überwachten Räumlichkeiten nicht zu rechnen ist, aber Anhaltspunkte für eine Gefahr im Sinne von § 18 Absatz 1 Nr. 1 oder 2 LDSG bestehen. Selbstverständlich wären auch hier Anforderungen des

Beschäftigtendatenschutzes zusätzlich zu beachten und müssten auch hier überwiegend schutzwürdige Interessen betroffener Personen der Videoüberwachung entgegenstehen.

Soweit die oben wiedergegebenen Stellungnahmen Beispielsfälle nennen, für die eine Rechtsgrundlage zur Videoüberwachung in nicht öffentlich zugänglichen Räumen geschaffen werden solle, halten wir diese jedenfalls teilweise nicht für geeignet, eine Videoüberwachung zu rechtfertigen. So erschließt sich im Fall des Serverraumes die Erforderlichkeit einer Videoüberwachung nicht: Externen sollte der Zutritt zu so sensiblen Bereichen wie Serverräumen ohnehin durch hinreichende technische Maßnahmen verwehrt werden, soweit er nicht zwingend (etwa zur Wartung) erforderlich ist; soweit ein solcher Zutritt erforderlich ist, sind andere organisatorische Maßnahmen (z. B. die Weisung, den Zutritt nur unter Aufsicht von bestimmten beschäftigten des Verantwortlichen zu gestatten) näherliegend als eine Videoüberwachung, die hier deswegen nicht erforderlich erscheint. Zudem ist der Nutzen der zusätzlich gewünschten Audioaufnahmen bereits aus praktischer Sicht heraus nicht zu erkennen. Wie diese z.B. zur Überwachung von unberechtigten Zugriffen auf informationsverarbeitende Systeme geeignet sein sollen, erschließt sich nicht. Zudem handelt es sich beim Mithören von Gesprächen, insbesondere am Arbeitsplatz, regelmäßig um einen gravierenden und regelmäßig unverhältnismäßigen Eingriff in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung (vgl. deswegen auch die Strafvorschrift des § 201 des Strafgesetzbuchs bzw. die strafprozessualen Vorschriften zum sogenannten kleinen und großen Lauschangriff, §§ 100c, 100f der Strafprozessordnung). Dies gilt sowohl für eigenes als auch fremdes Personal.

Hinsichtlich der Baustellenüberwachung scheidet eine Anwendung von Videoüberwachung zum Zweck der Abrechnungsüberprüfung im beschriebenen Sinne aus: Für eine Zusatzarbeit am Wochenende wäre derjenige beweispflichtig, der diese erbracht haben will und eine Vergütung für diese verlangt. Die Videoüberwachung wäre zur Abwehr solcher Vergütungsansprüche daher nicht erforderlich. Der Zweck der Abwehr unberechtigter Ansprüche würde auch bisher gemäß § 18 LDSG eine Videoüberwachung öffentlich zugänglicher Räume nicht rechtfertigen. Dagegen wäre die Gestattung einer Videoüberwachung zu Zeiten, in denen die Baustelle nicht besetzt ist und eine Diebstahlsgefahr besteht, durchaus vertretbar. Umgekehrt erscheint es fragwürdig, ob und ggf. unter welchen Umständen eine Videoüberwachung während der Anwesenheit von Handwerkern gestattet werden sollte: Denn auch gegenüber Mitarbeitern von Bauunternehmen würde durch die Videoüberwachung nämlich – ähnlich wie bei Beschäftigten des Verantwortlichen – ein erheblicher Überwachungs-

und Anpassungsdruck erzeugt, dem sich diese nicht entziehen könnten. Es scheint daher auch für solche Anwendungsfälle höchstens gerechtfertigt, die Überwachung in äußerst engen Grenzen – als ultima ratio, vergleichbar der Anforderungen an die Aufklärung von Straftaten durch Beschäftigte – zuzulassen. Ob diese Regelungsmöglichkeit ausgeschöpft werden sollte, erscheint jedoch – gerade aufgrund des engen Bereichs und der hohen zu etablierenden Anforderungen – äußerst zweifelhaft.

2. Kritik am Merkmal der Erforderlichkeit; Forderung der Schaffung eines Ausnahmetatbestandes für Eingangsbereiche von Dienstgebäuden

Das Referat 35 des Innenministeriums regt in seiner Stellungnahme vom 30.10.2020 (S. 3 zu § 18) an, den Maßstab der Erforderlichkeit in § 18 Abs. 1 LDSG abzusenken, da die Verhältnismäßigkeitsprüfung ansonsten oft an weniger einschneidenden Maßnahmen (wie z.B. mechanischen Sicherungen, Alarmanlagen…) scheitere. Zumindest solle ein Ausnahmetatbestand für die Videoüberwachung von Eingangsbereichen von Dienstgebäuden geschaffen werden.

LfDI: *Die Voraussetzung der Erforderlichkeit kann nicht zur Disposition stehen. Sie ist ein elementarer Bestandteil der Anforderungen an jegliche Datenverarbeitung (mit Ausnahme der Einwilligung) und wird von der Datenschutz-Grundverordnung u. a. in den Grundsätzen der Datenminimierung und der Speicherbegrenzung vorgegeben (Art. 5 Absatz 1 Buchstaben c und e DS-GVO). Auch der Verarbeitungstatbestand des Art. 6 Abs. 1 Buchstabe e DS-GVO setzt die Erforderlichkeit explizit voraus. Diese Norm bietet in Verbindung mit § 18 LDSG überhaupt erst die Grundlage für die Datenverarbeitung. Des Weiteren verlangt Art. 6 Abs. 3 S. 4 DS-GVO, als Teil der Öffnungsklausel, auf der § 18 LDSG beruht, die Beachtung des Verhältnismäßigkeitsgrundsatzes – und somit auch die Beachtung des Grundsatzes der Erforderlichkeit. Der Verhältnismäßigkeitsgrundsatz in Bezug auf Grundrechtseingriffe ist ferner auch Kernbestand des deutschen Verfassungsrechts.*

Auch für die Einfügung eines weiteren Verarbeitungstatbestandes, der quasi pauschal die Überwachung von Eingangsbereichen von Dienstgebäuden erlauben soll, besteht keine Grundlage. Erfasst werden durch die Videoüberwachung überwiegend anlasslos Personen, denen kein Fehlverhalten vorgeworfen werden kann. Die Videoüberwachung stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung betroffener Personen dar. Für deren Rechtfertigung bedürfte es einer hinreichenden gesetzlichen Grundlage. Anforderung an die Rechtsgrundlage sind

insbesondere ein überwiegendes Allgemeininteresse und die Wahrung des Verhältnismäßigkeitsgrundsatzes. Die gesetzliche Schranke darf dabei nicht weiter sein, als dies zum Schutz des jeweiligen öffentlichen Interesses erforderlich ist (BVerfG, NJW 2001, 2320 (2321)). Diese Anforderungen sind durch eine pauschale Erlaubnis zu einem Filmen von Eingangsbereichen von Dienstgebäuden nicht erfüllbar: Weder ist hierzu überhaupt ein (überwiegendes) Allgemeininteresse erkennbar, noch die sich aus dem Grundsatz der Verhältnismäßigkeit folgenden Anforderungen gewahrt. Eine entsprechende Überwachungsmöglichkeit würde daher zu weit gehen. Eingangsbereiche sind auch insoweit sensibel, dass dazu regelmäßig auch die Rechte Beschäftigter (§ 15 LDSG) zu beachten sind. Für diese könnte eine solche Art der Überwachung aufgrund der damit potenziell einhergehenden Kontrollmöglichkeit seitens des Arbeitgebers eine erhebliche Eingriffsintensität mit sich bringen. Eine generalisierende Betrachtung genügt daher nicht.

3. Kritik an der Wendung „im Einzelfall“ in § 18 Absatz 1 LDSG

In der *Gemeinsamen Stellungnahme des Gemeinde- und Landkreistags Baden-Württemberg vom 29.10.2021* wird angeregt (S. 2 Abs. 3), in § 18 Abs. 1 S. 1 LDSG den Einschub „im Einzelfall“ zu streichen, da dieser missverständlich sei. Es bestehe Klarheit darüber, dass keine anlasslose, rein präventive Videoüberwachung der gesamten Gemeinde möglich sei. Die restlichen Vorgaben des Abs. 1 beschränkten die Videoüberwachung ohnehin zeitlich und örtlich. Insgesamt würden die Kommunen durch die Vorgaben des LDSG zu stark bürokratisch belastet.

LfDI: *Wieso der Begriff „missverständlich“ sein soll, wenn er gleichzeitig – wie Gemeindetag und Landkreistag in ihrer Stellungnahme wohl ebenfalls anerkennen – der Klarstellung dazu dient, dass keine pauschale Betrachtung zur Zulässigkeit der Videoüberwachung möglich ist, sondern eine konkrete Prüfung bezogen auf das jeweilige Überwachungsobjekt vorzunehmen ist, ist nicht nachzuvollziehen. Die Begrifflichkeit bietet vielmehr Anwendern, die sich mit der Norm befassen, eine Hilfestellung und vermag gerade nicht zu Missverständnissen zu führen. Eine rein generalisierende Betrachtung genügt schließlich auch aus Sicht der Kommunalvertretungen nicht.*

4. Schaffung eines eigenen Tatbestandsmerkmals der Verhinderung der Begehung von Ordnungswidrigkeiten oder Straftaten

In der *Gemeinsamen Stellungnahme des Gemeinde- und Landkreistags Baden-Württemberg vom 29.10.2021* wird weiter angeregt (S. 2 Abs. 3), eine Klarstellung ver-

gleichbar mit § 20a LDSG a.F. aufzunehmen, in welchem die Formulierung „insbesondere die Begehung von Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten zu verhindern“ sogleich im ersten Absatz verwendet worden sei, statt diese (wie derzeit) auf § 18 Abs. 1, 3 LDSG zu erstrecken. Hintergrund dieser Anregung sei, dass die Verhinderung von Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung überwiegend Ursache für den Wunsch nach Videoüberwachung im öffentlichen Raum sei. Die derzeitige Regelung in § 18 LDSG erschwere die Begründung und beschränke die Videoüberwachung auf den Schutz vor Straftaten und Ordnungswidrigkeiten gegen die in Abs. 1 genannten Rechtsgüter, baulichen Anlagen und Sachen. In einer vom Gemeinde- und Landkreistag vorgeschlagenen Formulierung wird sodann die Schaffung eines zusätzlichen Aufzählungspunktes in Absatz 1 (also als § 18 Abs. 1 Nr. 3 LDSG) empfohlen, in dem die Verhinderung der Begehung von Straftaten […] als eigenes alternatives Tatbestandsmerkmal neben Nr. 1 und 2 aufgeführt wird.

LfDI: *Die Regelung des § 18 Abs. 1 LDSG zielt auf den Schutz in und um öffentliches Eigentum, sowie des öffentlichen Eigentums selbst ab. Für die allgemeine Überwachung öffentlich zugänglicher Orte existiert bereits § 44 Abs. 3 PolG BW. Dadurch besteht derzeit keine zu weitgehende Beschränkung, sondern eine sinnvolle normative Abgrenzung der Videoüberwachung öffentlichen Eigentums einerseits (LDSG) und öffentlicher Räume andererseits (PolG). Gerade die Gemeinden sind als Ortspolizeibehörden auch gem. § 44 Abs. 3 PolG BW in begründeten Fällen zur Videoüberwachung ermächtigt. Weil den Gemeinden somit bereits weitreichende Rechtsgrundlagen zur Verfügung stehen, bedarf es einer Anfügung in Form der vorgeschlagenen Ziff. 3 in § 18 Abs. 1 LDSG nicht.*

Der Vorschlag aus der Gemeinsamen Stellungnahme des Gemeindetags und des Landkreistags geht zudem zu weit. Er stellt keine Rückkehr zur Klarstellung in § 20a LDSG a.F. dar, sondern ein „Mehr“ an Rechtsgrundlage, für das keine Begründung ersichtlich ist. Denn soweit der Gemeinde- und Landkreistag davon ausgeht, die alte Regelung (§ 20a LDSG a. F.) habe die Videoüberwachung zur Verhinderung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung ohne Rücksicht auf die Schutzgüter in Nr. 1 und 2 legitimiert, ist dies unzutreffend. Wie sich aus dem Wortlaut der früheren Norm klar ergibt, musste die Videoüberwachung stets den Schutz eines in Nr. 1 aufgelisteten Rechtsguts oder in Nr. 2 aufgelisteten Objekts bezwecken, so dass es bei dem mit „insbesondere“ angeschlossenen Beispiel, dass die

Videoüberwachung der Verhinderung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten von besonderer Bedeutung um solche Tatbestände handeln musste, die den Schutz der in Nr. 1 oder 2 genannten Rechtsgüter bzw. Objekte bezweckten.

Im Übrigen ist auf Folgendes hinzuweisen: Mit § 18 LDSG wurden bereits die vormaligen Anforderungen des § 20a LDSG a.F. abgesenkt. Die Vorgängernorm setzte schließlich gem. § 20a Abs. 1 S. 2 LDSG a.F. voraus, dass tatsächliche Anhaltspunkte für eine Gefährdung bestehen. Diese – aus Sicht des LfDI grundsätzlich sinnvolle und begrüßenswerte – Schwelle wurde durch § 18 LDSG beseitigt. Eine weitere Absenkung in den Voraussetzungen ist daher nicht angebracht. Nachdem § 18 LDSG mit Anfügung der vorgeschlagenen Ziff. 3 die Videoüberwachung zu Zwecken der Strafverfolgung erlauben würde, würde ferner die Ermächtigung für Ortspolizeibehörden in § 44 Abs. 3 PolG ausgehöhlt. Örtlich hätten die Gemeinden im Gemeindegebiet dadurch sowieso nahezu freie Hand, Kameras zu errichten. Die gemeindliche Videoüberwachung könnte sich von einer Ausnahme zur – grundrechtlich unzulässigen – Regel verkehren. Gerade aufgrund bereits bestehender Probleme mit ausufernder gemeindlicher Videoüberwachung sollte die derzeitige Regelung beibehalten und nicht ausgeweitet werden.

5. Streichung von § 18 Absatz 4 LDSG

In der *Gemeinsamen Stellungnahme des Gemeinde- und Landkreistags Baden-Württemberg vom 29.10.2021* wird weiter angeregt (S. 3 Abs. 1), § 18 Absatz 4 LDSG komplett zu streichen bzw. zumindest zu überarbeiten. So sei z.B. nicht auszuschließen, dass in einer kleineren Gemeinde die überwachende Stelle Personen, die sich zulässigerweise auf öffentlichem Gebiet aufhalten, erkennen/zuordnen könne. Die Informationspflicht löse einen unverhältnismäßigen Verwaltungsaufwand aus. Die Informationspflicht für die Erhebung personenbezogener Daten für Fälle, die tatsächlich gespeichert blieben, ergebe sich bereits aus Art. 14 DS-GVO.

LfDI: *Im Rahmen der Videoüberwachung erfolgt die Erhebung der personenbezogenen Daten bei der betroffenen Person, weshalb regelmäßig die Informationspflicht gem. Art. 13 DS-GVO einschlägig ist. Die Unterrichtung erfolgt in der Regel in Form eines Hinweisschildes, auf dem die nach Art. 13 DS-GVO erforderlichen Angaben hinterlegt sind. Die Regelung des § 18 Abs. 4 LDSG hat lediglich klarstellende Funktion. Eine vergleichbare Regelung war bereits in § 20a Abs. 4 LDSG a.F. gegeben.*

Allerdings ist die Praxis der ausschließlichen Verwendung von Hinweisschildern insoweit zu überdenken als möglicherweise betroffene Personen zu ändern/ergänzen,

die den (optisch wahrnehmbaren) Inhalt eines Hinweisschildes nicht zur Kenntnis nehmen können, etwa wegen ihrer eingeschränkten Sehfähigkeit.

6. Kritik an der Regelung der Speicherdauer in § 18 Absatz 5 LDSG:

Die Regelung der Speicherdauer in § 18 Absatz 5 LDSG wird verschiedentlich kritisiert. In der *Stellungnahme des Referat 35 des Innenministeriums vom 30.10.2020* (S. 3 unten) wird geschildert, dass in der Praxis die Regelung des § 18 Abs. 5 LDSG immer wieder zu Auseinandersetzungen mit der datenschutzrechtlichen Aufsichtsbehörde führe, weil die dort genannte Vier-Wochenfrist von der Praxis als Höchstspeicherfrist (miss-)verstanden werde. Das Referat 35 des Innenministeriums regt daher an, Rechtsklarheit zu schaffen, indem im Gesetz ausdrücklich betont werde, dass sich die Speicherdauer ausschließlich am Grundsatz der Erforderlichkeit und dem Grundsatz der Speicherbegrenzung i.S.d. Art. 5 Abs. 1 Buchstabe e DS-GVO orientiere.

Umgekehrt wird in der *Gemeinsamen Stellungnahme des Gemeinde- und Landkreistags Baden-Württemberg vom 29.10.2021* (S. 3 Abs. 2) die Streichung der in § 18 Absatz 5 LDSG vorgesehenen Vierwochenfrist angelehnt und das Verständnis als zulässige Maximalspeicherdauer unterstrichen. In der Praxis komme es vor, dass Videos nicht immer unverzüglich ausgewertet werden können. Eine Fristverkürzung diene dem Schutz von Straftätern.
LfDI: *Sind Videoaufnahmen für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig, ist der Verantwortliche verpflichtet, die Aufnahmen unverzüglich zu löschen, vgl. Art. 17 Absatz 1 Buchstabe a DS-GVO (i.V.m. Art. 5 Abs. 1 Buchstabe e DS-GVO). Die zulässige Speicherdauer bei der Videoüberwachung durch nicht-öffentliche Stellen beträgt so i.d.R. maximal 72 Stunden (vgl. DSK Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, S. 22 f.). Davon abweichende Speicherdauern sind nur in Ausnahmefällen zulässig. Die gemeindliche/öffentliche Videoüberwachung ist durchaus mit der Videoüberwachung durch nicht-öffentliche Stellen zu vergleichen; häufig überschneiden sich auch die mit der Videoüberwachung verfolgten Zwecke (Schutz vor Sachbeschädigung, Einbruch). Dabei stellt die Videoüberwachung durch öffentliche Stellen keine anderen Anforderungen an die Speicherdauer als diejenige durch nicht-öffentliche Stellen. Eine abweichende Regelung hinsichtlich der Speicherfrist für öffentliche Stellen ist deswegen nicht gerechtfertigt. Innergemeindliche Abläufe, die eine Sichtung der Bilder verzögern könnten, sind keine Rechtfertigung für eine längerfristige Speicherung von Bildern. Mit der Speicherdauer nimmt auch die Intensität des Eingriffes in die Rechte Gefilmter zu. §*

18 Abs. 5 LDSG sollte aus diesen Gründen gestrichen oder die Speicherdauer erheblich, zumindest auf die maximal zulässigen 72 Stunden, herabgesetzt werden. Die derzeitige Regelung führt leider in der Tat oft zu Missverständnissen hinsichtlich der zulässigen Dauer der Speicherung und bedarf daher der Überarbeitung. Wir teilen insoweit die Kritik des Referats 35 des Innenministeriums ausdrücklich.

7. Vorsorglich: Schaffung eines weiteren Tatbestandes für Webcams zur Dokumentation von Baufortschritten

Der *Datenschutzbeauftragte des Finanzministeriums* spricht in seiner *Stellungnahme vom 26.10.2020* die Fallgestaltung an, dass Webcams zur Dokumentation von Baufortschritten für die interessierte Öffentlichkeit verwendet würden. Er hält aber für diese Konstellation selbst eine Rechtsgrundlage weder für gegeben noch die Schaffung einer solchen für geboten.

LfDI: *Wir teilen die Auffassung des Datenschutzbeauftragten des Finanzministeriums. Für den genannten Zweck ist eine Verarbeitung personenbezogener Daten grundsätzlich nicht zulässig und kommt auch die Schaffung einer Rechtsgrundlage nicht in Betracht. Die Darstellung von Baufortschritten ist auch durch Einzelbilder, die regelmäßig tages- oder wochenweise gefertigt werden, möglich. Diese Einzelbilder können außerhalb der Arbeitszeiten und somit so aufgenommen werden, dass keine personenbezogenen Daten betroffen sind. Gründe für die Erforderlichkeit der Verarbeitung personenbezogener Daten sind insoweit nicht ersichtlich. Wir weisen zudem auf die mit der Veröffentlichung von Aufnahmen ebenfalls verbundenen zivilrechtlichen Fragestellungen hin.*

§ 19 LDSG

LfDI: *Wir halten an unseren Ausführungen in der Stellungnahme vom 06.11.2020 fest: § 19 LDSG enthält eine Einschränkung dahingehend, dass nur bestimmte Normen/Kapitel der DS-GVO (sowie § 19 LDSG) anwendbar sind. Diese Einschränkung muss darauf überprüft werden, ob sie mit der Tatsache vereinbar ist, dass das KUG, insbesondere §§ 21-23 KUG, nach wie vor nicht aufgehoben wurden und laut bisher ergangenen Urteilen weiter Anwendung finden.*

§ 25 LDSG

Stellungnahme des Staatsministeriums vom 28.10.2020:
(S. 2) Gewünscht wird eine Ergänzung in § 25 Abs. 1 LDSG, die durch den Südwestrundfunk angeregt wurde:
„Der Landesbeauftragte für den Datenschutz arbeitet mit anderen Aufsichtsbehörden, auch durch Informationsaustausch, zusammen und leistet ihnen Amtshilfe, um die einheitliche Anwendung der Vorschriften für den Datenschutz zu gewährleisten."

LfDI: *Eine Ergänzung in der vorgeschlagenen Art und Ausmaß ist abzulehnen. Die Formulierung würde eine Pflicht zur Amtshilfe etablieren, wie sie bereits aus Gründen der Zuständigkeitsabgrenzung problematisch ist: So sieht § 4 Abs. 2 Nr. 2 LVwVfG vor, dass eine Amtshilfe nicht vorliegt, wenn die Hilfeleistung in Handlungen besteht, die der ersuchten Behörde als eigene Aufgabe obliegen. Eben eine solche Überschneidung wäre im Verhältnis zwischen dem LfDI und Rundfunkbeauftragten für den Datenschutz zumindest in Einzelfällen möglich, weshalb eine Amtshilfeverpflichtung in solchen Fällen gegen bestehendes Verfahrensrecht verstoßen würde. Gravierender ist jedoch, dass eine solche Amtspflicht die Unabhängigkeit des Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu beeinträchtigen geeignet ist und deshalb strikt abgelehnt wird.*

Stellungnahme des Rundfunkbeauftragten für den Datenschutz beim SWR vom 30.10.2020:
(S. 4 Ziff. 5) Der Rundfunkdatenschutzbeauftragte regt an, dass der Landesgesetzgeber für eine stärkere Einbindung der Rundfunkbeauftragten für den Datenschutz in die nationale Datenschutzkonferenz (DSK) sorgen könnte. Hierfür könne er die Regelungen über den Landesbeauftragten für den Datenschutz in § 25 Abs. 1 LDSG BW um folgenden Satz ergänzen: „Der Landesdatenschutzbeauftragten arbeitet mit allen anderen Aufsichtsbehörden zusammen und unterstützt sie".

Vergleichend verwiesen wird dabei auf § 14 Abs. 1 Nr. 7 BDSG.

LfDI: *Eine landesrechtliche Regelung erscheint hier verfehlt. Die Datenschutzkonferenz (DSK) ist eine Plattform zum gemeinsamen Informationsaustausch und zur Abstimmung nationaler datenschutzrechtlicher Empfehlungen des Bundes und der Länder. Sie ist ein Gremium der unabhängigen Aufsichtsbehörden und gerade keine Institution des Landes Baden-Württemberg. Zudem erscheint der vorgeschlagene Text, insbesondere hinsichtlich der Formulierung „mit allen anderen Aufsichtsbehörden",*

zu unbestimmt. Im Übrigen ist eine gesetzliche Regelung auch deshalb obsolet, weil der LfDI bereits in der Vergangenheit die Zusammenarbeit mit den so. spezifischen Aufsichtsbehörden, wie dem Rundfunkbeauftragten für den Datenschutz nicht gescheut hat und zukünftig noch intensivieren.

Stellungnahme des LfDI vom 06.11.2020 im Rahmen der Evaluation des LDSG:
„1. Die Maßnahmenbefugnisse der Aufsichtsbehörde sind abschließend in Artikel 58 DS-GVO geregelt. Artikel 6 Abs. 2 und 3 DS-GVO eröffnen keinen Spielraum des Landesgesetzgebers, die Durchführung dieser Maßnahmen von weiteren Voraussetzungen abhängig zu machen. Fraglich ist ohnehin, ob hier der Vorrang europarechtlicher Regelungen die Unanwendbarkeit dieser Maßgabe zur Folge hat – wovon der LfDI ausgeht. Abgesehen hiervon hindert die Verpflichtung, vor Durchführung von Maßnahmen eine Stellungnahme einzuholen, den effektiven Schutz der Betroffenen vor fortdauernden Grundrechtsbeeinträchtigungen, da regelmäßig geraume Zeit vergeht, bis es bspw. zu einer Löschungsanordnung oder einem sonstigen Verarbeitungsverbot kommt. Insbesondere auch bei kommunalen Verantwortlichen ist die Unterrichtung des Bürgermeisters regelmäßig überflüssig, da dieser die Korrespondenz mit der Aufsichtsbehörde regelmäßig bereits kennen wird.

Handlungsempfehlung:
Streichung des § 25 Absatz 4 LDSG

2. Die Beschränkung der Aufsichtsbefugnisse gegenüber Notaren ist europarechtswidrig. Sie ist wegen des Vorrangs der DS-GVO nicht anwendbar und sollte der Klarheit wegen gestrichen werden.

Handlungsempfehlung:
Streichung des § 25 Absatz 5 Satz 1“.

LfDI: *An diesen Ausführungen halten wir fest.* Ergänzend führen wir aus:
Wiederum unabhängig von der europarechtlichen Bewertung sollte in § 25 Absatz 4 auch der Verstoß gegen die Unterstützungspflicht gemäß § 26 aufgenommen werden; „Maßnahmen nach Artikel 58 Absatz 2 b bis g und j“ dürfte nicht einschlägig sein.

Aus der Vorschrift geht außerdem nicht eindeutig hervor, dass Einbeziehung nicht bei jedem Verstoß, sondern ausschließlich bei geplanten Maßnahmen nach „…Artikel 58…“ nötig ist.

Falls § 25 Absatz 4 LDSG gestrichen werden sollte, wäre eine Regelung vorteilhaft, die klarstellt, dass sich der LfDI bei Bedarf an die Dienst- oder Fachaufsichtsbehörde wenden kann.

Außerdem wird die Verweisung auf § 29 Absatz 3 BDSG und die dort genannte Einschränkung nur einzelner Befugnisse in der Praxis oft nicht verstanden. Darüber hinaus ging es in den uns vorliegenden Fällen noch nie um Untersuchungsbefugnisse nach Artikel 58 Absatz 1 Buchstaben e und f DS-GVO. Wir regen die Streichung oder eine Klarstellung durch eine eigenständige, von der missverständlichen Regelung in § 29 Absatz 3 BDSG unabhängige Normierung an.

§ 26 LDSG

Gemeinsame Stellungnahme des Gemeinde- und Landkreistags Baden-Württemberg vom 29.10.2021:
(S. 3 Abs. 3 Spiegelstrich 2) Durch die pandemische Lage sei ein Trend zum Homeoffice zu beobachten. Dies habe Auswirkungen auf die Unterstützungspflicht öffentlicher Stellen gegenüber dem LfDI i.S.d. § 26 Abs. 1 Nr. 2 LDSG, jederzeit Zutritt zu den Diensträumen zu gewähren. Wenn eine Ausweitung der Unterstützungspflicht auf den grundgesetzlich geschützten Wohnbereich angedacht wird, hätte man hierfür ggf. eine gesetzliche Grundlage zu schaffen.

***LfDI:** Die Befugnisse und Zutrittsrechte der Datenschutzaufsichtsbehörden ergeben sich aus den gesetzlichen Bestimmungen, insbesondere aus Art. 58 Abs. 1 DS-GVO. Zwar können sich die Zugangsrechte, die gegenüber den datenschutzrechtlich Verantwortlichen bestehen, gem. Art. 58 Abs. 1 lit. f DS-GVO grundsätzlich auch auf geschäftlich genutzte Räume in Privatwohnungen erstrecken (vgl Gola/Nguyen DS-GVO Art. 58 Rn. 11). Allerdings dürfte es in tatsächlicher Hinsicht kaum eine Fallkonstellation geben, in der diese Kontrollrechte gegenüber Beschäftigten an ihrem Heimarbeitsplatz praktische Anwendung finden.*

§ 27 LDSG
Stellungnahme des Rundfunkbeauftragten für den Datenschutz beim SWR vom 30.10.2020:
1. Der Rundfunkbeauftragte betont (S. 1 Ziff. II), dass aus seiner Sicht die Regelung des § 27 LDSG beibehalten werden solle. Das datenschutzrechtliche Kontrollmo-

dell beim SWR, nur einen Rundfunkdatenschutzbeauftragten als Aufsichtsbehörde vorzusehen und nicht noch zusätzlich einen internen behördlichen Datenschutzbeauftragten habe sich bewährt. Eine Doppelstruktur mit Aufsicht nach Art. 51 DSGVO einerseits und behördlichem Datenschutzbeauftragten nach Art. 37 DSGVO andererseits sei für ein einzelnes Unternehmen wie den SWR wenig sinnvoll.

LfDI BW: *Die Ausführungen des Rundfunkdatenschutzbeauftragten scheinen uns nicht zutreffend zu sein. Der SWR ist als Anstalt öffentlichen Rechts gemäß Art. 37 DS-GVO zur Bestellung eines (behördlichen) Datenschutzbeauftragten verpflichtet; dementsprechend hat der SWR auch einen solchen bestellt (s. die Datenschutzinformationen des SWR unter https://www.swr.de/datenschutz/index.html und dort unter „datenschutzrechtliche Formalien“). Gesetzgeberischen Handlungsbedarf sehen wir insoweit nicht.*

2. In formaler Hinsicht weist der Rundfunkdatenschutzbeauftragte darauf hin, dass in § 27 Abs.1 LDSG der Verweis auf § 16c Rundfunkstaatsvertrag (bisher) durch einen Verweis auf § 42 Medienstaatsvertrag (neu) ersetzt werden müsse.

   LfDI: *Dieser Hinweis ist inzwischen obsolet, nachdem der Landesgesetzgeber durch Gesetz vom 6. Dezember 2022 (GBl. S. 622) eine entsprechende Anpassung in § 27 LDSG vorgenommen hat.*

3. Der Rundfunkbeauftragte empfiehlt (S. 2 Ziff. 2), nach § 27 Abs. 4 S. 3 LDSG einzufügen:

   > „Er [der Rundfunkdatenschutzbeauftragte] darf auch nach dem Ende seiner Amtszeit nicht wegen seiner Aufgabenerfüllung benachteiligt werden.“

   Eine solche Regelung sei geboten, da die/der Rundfunkdatenschutzbeauftragte mit dem Ende der Amtszeit in ein normales Arbeitsverhältnis zurückfalle und deswegen eine Diskriminierungsgefahr bestehe. Dies zeige die Erfahrung aus anderen Bundesländern.

   LfDI BW: *Die Forderung des Rundfunkdatenschutzbeauftragten erscheint nachvollziehbar und ihre Umsetzung empfehlenswert. Obwohl der Rundfunkbeauftragte nicht der behördliche Datenschutzbeauftragte der Rundfunkanstalt, sondern dessen Aufsichtsbehörde ist, ist der Schutzbedarf (jedenfalls nach dem*

Ende der Amtsausübung) zumindest vergleichbar. Für behördliche und betriebliche Datenschutzbeauftragte ergibt sich das Benachteiligungsverbot aus Art. 38 Absatz 3 Satz 2 DS-GVO. Hinter diesem Standard sollte der Schutz des Rundfunkdatenschutzbeauftragten nicht zurückbleiben.

4. Nach § 27 Abs. 3 Satz 2 und LDSG ist der Rundfunkdatenschutzbeauftragten angemessen zu vergüten; die näheren Bestimmungen, insbesondere die Regelung der Grundsätze der Vergütung, überlässt der Gesetzgeber der Satzungsgewalt des Rundfunkrats, der für den Erlass der Satzung der Zustimmung des Verwaltungsrats bedarf. Der Rundfunkdatenschutzbeauftragte hält es in seiner Stellungnahme hierzu (S. 2, 3 Ziff. 3 lit. a-e) für fraglich, ob es sich bei der Vergütungshöhe nicht um eine wesentliche Frage handele, für deren Regelung/Festlegung gem. Art. 52 Abs. 4 DS-GVO der Gesetzgeber zuständig wäre und die er nicht (wie bisher geregelt) an die Rundfunkgremien delegieren könne.

   Der Rundfunkdatenschutzbeauftragte verweist hierzu auf die Parallelregelung in § 23 Abs. 4 LDSG, in der die Vergütung des Landesbeauftragten für den Datenschutz anhand der Besoldungsstruktur des Landes explizit gesetzlich geregelt wird. Das Bedürfnis einer gesetzlichen Normierung bestehe auch beim Rundfunkdatenschutzbeauftragten. Beim SWR gebe es nämlich unter der Intendanz und den Direktoren 30-40 Hauptabteilungsleitungen und ca. 120-130 Abteilungsleitungen; im Rahmen der Umsetzung von § 27 Abs. 3 Satz 3 LDSG BW habe die Geschäftsleitung den Rundfunkdatenschutzbeauftragten dabei nur als Abteilungsleiter und nicht als Hauptabteilungsleiter eingestuft. Auf diese Weise würden ihm die den Hauptabteilungsleitungen vorgesehenen Besonderheiten (z.B. hinsichtlich der Raumausstattung) versagt und der Rundfunkdatenschutzbeauftragte der Tarifbindung unterworfen. Das werde seiner unabhängigen Stellung nicht gerecht und offenbare auch nach innen und außen, dass man dem Datenschutzbeauftragten ihm nur einen Status einräume, der mit dem Sinn und Zweck der Aufgabenerfüllung einer unabhängigen Aufsichtsbehörde nach Art. 51 ff. DSGVO nicht zu vereinbaren sei.

   LfDI BW: *Der LfDI vermag nicht aus eigener Anschauung zu beurteilen, inwieweit Gehalt und Ausstattung des Rundfunkdatenschutzbeauftragten derzeit seinem Amt angemessen sind. Die Kritik des Rundfunkdatenschutzbeauftragten, dass sein Amt nicht ausreichend gewürdigt werde, wenn es nur wie eine von ca. 120 Abteilungsleitungen eingestuft werde, erscheint grundsätzlich plausibel. Aus Sicht*

des Datenschutzes wäre es sinnvoll, weitere wesentliche Fragen insoweit gesetzlich zu regeln, um so Reibungen zu vermeiden und die Unabhängigkeit des Rundfunkdatenschutzbeauftragten zu stärken, soweit einer solchen weitergehenden gesetzlichen Festlegung nicht die Unabhängigkeit der Organisation des Rundfunks selbst entgegensteht.

5. Nach § 27 Abs. 10 LDSG BW hat der Rundfunkdatenschutzbeauftragte jährlich einen Tätigkeitsbericht sowohl an die Landtage als auch die Landesregierungen der den SWR Staatsvertrag unterzeichnenden Länder zu übermitteln. Der Rundfunkdatenschutzbeauftragte (S. 3 Ziff. 4) führt aus, dass die Tätigkeitsberichte bei den Landesregierungen und den Landtagen kaum oder sogar gar keine Resonanz fänden; Landesregierungen und –Parlamente würden nicht reagieren oder die Berichte allenfalls ohne Aussprache zur Kenntnis nehmen. Daher wirft der Rundfunkdatenschutzbeauftragte die Frage auf, ob die Verpflichtungen aus § 27 Absatz 10 LDSG so aufrechterhalten werden sollten.

   LfDI BW: *Insoweit sind Vorgaben aus Art. 59 DS-GVO zu beachten. Danach müssen die Jahresberichte einer Aufsichtsbehörde dem nationalen Parlament und der Regierung (ggf. neben anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden) übermittelt und veröffentlicht werden. Die Vorschrift ist daher aufrechtzuerhalten.*

§ 28 LDSG

Stellungnahme des Innenministeriums vom 28.06.2021:
(3.11) Der zweite Halbsatz des § 28 LDSG, dem zu folge Geldbußen verhängt werden dürfen, soweit öffentliche Stellen am Wettbewerb teilnehmen, erscheine überflüssig. Denn nach § 6 Abs. 6 LDSG seien ohnehin die für nichtöffentliche Stellen geltenden „datenschutzrechtlichen Vorschriften“ entsprechend anzuwenden, soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnähmen. Wenn man „datenschutzrechtliche Vorschriften“ in § 2 Abs. 6 LDSG jedoch so verstehe, dass es nur um das materielle Datenschutzrecht gehe, die Geldbuße (als Sanktion) auf Sekundär- oder Tertiärebene jedoch gesondert zu würdigen sei, habe diese Regelung (in § 28, 2. Halbsatz, LDSG) klarstellenden Charakter.

Stellungnahme des Ministeriums für Soziales und Integration (Sozialministerium) vom 27.10.2020:
(S. 2 f.) Aus einem Urteil des EuGHs vom 11.06.2020 folgert das Sozialministerium,

dass es sich bei Krankenkassen um keine Unternehmen handele, sondern um öffentliche Stellen, die nach § 28 LDSG nicht Ziel von Geldbußen sein könnten und sachgerechterweise vom Anwendungsbereich „des LDSG“ ausgenommen werden sollten. Die dahingehenden längeren Ausführungen enden damit, dass das Sozialministerium als Rechtsaufsicht in Zukunft alle notwendigen Maßnahmen zur Verhinderung von Sozialdatenmissbrauch verpflichtend festlegen und die Umsetzung überwachen möchte.

Stellungnahme des Regierungspräsidium Freiburg, Abt. 1, vom 28.10.2020:
(Ziff. 2.3) Gewünscht wird eine Klarstellung zur Frage, ob und ggfs. unter welchen Voraussetzungen Bedienstete, die gegen datenschutzrechtliche Bestimmungen verstoßen, zur Verantwortung gezogen werden können.

Gemeinsame Stellungnahme des Gemeinde- und Landkreistags vom 29.10.2020
Zur Sanktionierung von Bediensteten der Behörden heißt es hier, dass die Komplexität des Datenschutzrechts auch bei einer Umsetzung des nachvollziehbaren Wunsches nach Sanktionierung von Datenschutzverstößen eine angemessene Berücksichtigung finden sollte.

LfDI: *Die Vorschrift ist in ihrer aktuellen Fassung verständlich, sodass es nach hiesiger Auffassung keiner Streichung bedarf. Mit der Regelung berücksichtigt der Landesgesetzgeber den europarechtlichen Behördenbegriff, wonach Unternehmen, die am Wettbewerb teilnehmen ungeachtet ihrer Rechtsform nach nationalem Recht weder Behörde noch (sonstige) öffentliche Stelle im Sinne des Art. 83 Abs. 7 DS-GVO sein können und damit einer nationalstaatlichen Ahndungsbefreiung nicht zugänglich sind. Diesen Regelungsgehalt bildet der zweite Halbsatz des § 28 LDSG ab, sodass auf ihn nicht verzichtet werden sollte.*

Die Auffassung des Sozialministeriums wird nicht geteilt. Sog. gesetzliche Krankenkassen sind öffentliche Stellen im Sinne des § 2 Abs. 2 LDSG und können damit – sofern sie mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen – grundsätzlich dem möglichen Anwendungsbereich des § 28 LDSG unterfallen.

Einer Klarstellung hinsichtlich einer möglichen Sanktionierung bedarf es nach hiesiger Auffassung nicht, denn die Vorschrift benennt als mögliche Adressaten von Bußgeldern nach dieser Norm nur öffentliche Stellen. Diese sind in § 2 Abs. 1, 2 LDSG definiert und meinen gerade keine Mitarbeitenden, sondern spiegeln den Verantwort-

lichenbegriff des Art. 4 DS-GVO wider. Im Übrigen bestimmt sich die Frage der Verantwortlichkeit und damit der Möglichkeit Adressat einer Geldbuße zu sein, unionsrechtsautonom nach Art. 4 Ziff. 7 DS-GVO.

Allerdings wäre es – unabhängig von der bislang in der Evaluation vorgebrachten Kritik – angemessen, die Notare, obwohl es sich bei diesen um öffentliche Stellen handelt, vom Anwendungsbereich des § 28 auszunehmen. Anders als andere öffentliche Stellen handeln diese „auf eigene Rechnung". Sie sind insofern eher mit den Rechtsanwälten zu vergleichen als mit öffentlichen Stellen. Das Argument, es mache keinen Sinn, Gelder einer öffentlichen Stelle einer anderen Stelle zukommen zu lassen, passt hier nicht.

§ 29 LDSG

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(3.12) In § 29 Abs. 1 Nr. 1 lit. a LDSG finden sich noch die aus dem alten Recht stammenden Begriffe „speichert, nutzt, verändert, übermittelt oder löscht". Diese Begriffe müssten nach der neuen Systematik durch den Begriff „verarbeitet" ersetzt werden.

***LfDI:** Dem ist zuzustimmen. Auch die restlichen lit. (b-c) sollten damit obsolet sein.*

II. Sonstige Anregungen zur Aufnahme von Regelungen in das LDSG oder zu dessen allgemeiner Gestaltung

Neue dringende Änderungsanregung des LfDI: Zuständigkeit für Untersuchungs- und Abhilfebefugnisse bzgl. TTDSG

Zum 01.12.2021 ist das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) in Kraft getreten, welches auch eine Vorschrift für Einwilligung beim Einsatz von Cookies und anderen ähnlichen Technologien schafft. Der Bundesgesetzgeber wollte damit durch entsprechende Anpassungen der Datenschutzbestimmungen aus dem Telekommunikationsgesetz (TKG) und Telemediengesetz (TMG) den Anforderungen der Datenschutz-Grundverordnung (DS-GVO) gerecht werden und ebenfalls die Gelegenheit nutzen, eine Regelung zum Schutz der Privatsphäre in Endeinrichtungen gemäß der ePrivacy-Richtlinie in nationales Recht umsetzen. So sieht § 25 TTDSG nunmehr

vor, dass das Speichern und Auslesen von Informationen auf Endeinrichtungen grundsätzlich einer Einwilligung der Nutzerinnen und Nutzer bedürfen. Zur Ahndung und Verfolgung von Verstößen gegen diese Vorschrift im Bereich Telemedien sieht § 1 Absatz 1 Nr. 8 TTDSG die Zuständigkeit bei den nach Landesrecht zuständigen Behörden. So wird dem Landesgesetzgeber überlassen, entsprechende Regelungen zur Zuständigkeit in den Landesgesetzen zu schaffen.

Diese Möglichkeit hat der Landesgesetzgeber in Baden-Württemberg teilweise Gebrauch gemacht. Mit dem neuen § 3a der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten (OWiZuVO) wird dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) ausdrücklich die Zuständigkeit zur Verhängung von Bußgeldern für Verstöße im Bereich Telemedien zugewiesen.

Im Zuge dieser Umsetzung wurde jedoch nicht aufgegriffen, ob der LfDI auch zuständig ist, die Einhaltung der Vorgaben des TTDSG zu überwachen und abseits von Bußgeldern durchzusetzen. Zwar überlässt die ePrivacy-RL es den nationalen Gesetzgebern die Bestimmung, welche nationale Behörde diese Kompetenz übertragen werden soll. Eine Übertragung der Befugnis, die Umsetzung der ePrivacy-RL durch § 25 TTDSG zu überwachen, an den LfDI ist hinsichtlich der bereits erfolgten Übertragung der Bußgeldzuständigkeit folgerichtig. Bei Verstößen gegen § 25 TTDSG sind oftmals auch personenbezogene Daten betroffen. Die Dienststelle des LfDI mit ihrer aufsichtsrechtlichen Kompetenz in der Überwachung der Umsetzung der DS-GVO, verfügt über das technische Know-How sowie langjährige Erfahrung in der Durchsetzung der betroffenen Vorgaben. Bisher ist eine die Zuständigkeit im Landesrecht nicht geregelt, was auch zur Folge hat, dass mildere Mittel als die Verhängung von Geldbußen (z.B. eine Verwarnung oder Untersagung) nach TTDSG nicht möglich sind.

Es zeichnet sich ebenfalls in den anderen Bundesländern eine ähnlich gesetzgeberische Entwicklung aus. So steht aktuell in Hamburg eine Änderung des HmbDSG bevor, wonach der HmbBfDI Aufsichtsbehörde im Sinne des § 113 Satz 1 Medienstaatsvertrag und zuständige Aufsichtsbehörde für Telemedien im Sinne des § 1 Nummer 8, 2. Halbsatz TTDSG wird. Eine Umsetzung haben bereits Rheinland-Pfalz in § 3a Absatz 2 des Landesgesetzes zu dem Staatsvertrag zur Modernisierung der Medienordnung in Deutschland (Medien StVtrG RP) und Nordrhein-Westfalen in § 1 Absatz 2 des Telemedienzuständigkeitsgesetzes NRW vorgenommen und entsprechende Aufsichtsbefugnisse für die Einhaltung des TTDSG im Bereich Telemedien –

analog zu den Befugnissen nach Art. 58 der DS-GVO – den jeweiligen Landesbeauftragten für Datenschutz zugeschrieben.

Vor diesem Hintergrund schlagen wir vor, § 25 des Landesdatenschutzgesetzes BW wie folgt zu ändern und einen neuen Absatz 2a einzufügen:

> *(2a) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist Aufsichtsbehörde im Sinne des § 113 Satz 1 des Medienstaatsvertrages vom 15. April, geändert vom 20. Dezember 2021 (GBl. 2022, S. 244), und zuständige Aufsichtsbehörde für Telemedien im Sinne des § 1 Nummer 8 zweiter Halbsatz des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) vom 23. Juni 2021 (BGBl. 2021 I S. 1982, 2022 I S. 1045), zuletzt geändert am 12. August 2021 (BGBl. I S. 3544, 3545), in der jeweils geltenden Fassung. Im Hinblick auf die Befugnisse der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen ihrer oder seiner Aufsichtstätigkeit über die Einhaltung der Bestimmungen nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz findet Artikel 58 der Verordnung (EU) 2016/679 entsprechende Anwendung. Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten in der Fassung vom 19. Februar 1987 (BGBl. I S. 603), zuletzt geändert am 5. Oktober 2021 (BGBl. I S. 4607, 4617), in der jeweils geltenden Fassung in den Fällen des § 28 Absatz 1 Nummern 10 bis 13 TTDSG, soweit nicht die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit gemäß § 28 Absatz 3 Nummer 2 TTDSG Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist.*

Weitere Punkte aus Stellungnahme des LfDI vom 06.11.2020
„XI. Spezielle Norm für die Übermittlung von Daten an (ausländische) Behörden
Die alte Fassung des LDSG regelte in § 16 bzw. § 20 spezifisch die Übermittlung von Daten an andere deutsche sowie ausländische Behörden. Um den Austausch zwischen Behörden zu vereinfachen, wäre die Wiederaufnahme dieser Vorschriften wünschenswert. ...“

„XII. Aufnahme einer Bestimmung zur Beauftragung der Auftragsverarbeitung durch die Fachaufsichtsbehörde
„Die Regelung in § 7 Absatz 1 Satz 5 LDSG alt sah vor, dass ein Auftrag zur Datenverarbeitung im Auftrag auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegende Stellen des Landes erteilt werden konnte. Eine Aufnahme einer solchen Regelung auch unter Geltung der DS-GVO wäre sinnvoll. ....“

„XIII. Teilnahme des Personals des LfDI an der Personalrotation der Innenverwaltung
Früher war der LfDI als Behörde im Verwaltungsaustausch ausdrücklich mit aufgenommen. In § 26 Absatz 4 Satz 4 der alten Fassung des LDSG war festgelegt, dass bezüglich der Beschäftigten des Landesbeauftragten die „Einbeziehung in den allgemeinen Personalaustausch der Landesverwaltung […] von der Landesregierung gewährleistet [wird]“. Heute fehlt eine entsprechende Regelung. Die Möglichkeit eines solchen Austauschs wäre wegen der Eigenschaft des LfDI als oberste Landesbehörde jedoch wünschenswert und könnte in den bestehenden § 20 Absatz 2 LDSG integriert werden. Der Personalaustausch schafft das notwendige Verwaltungsverständnis innerhalb des Personalkörpers des LfDI und sorgt dafür, dass die Behörden der Innenverwaltung mit datenschutzrechtlich versiertem Personal versorgt werden.“

„XIV. Effektivität und Durchsetzbarkeit von Anordnungen gegenüber Behörden
Nach Artikel 58 Absatz 2 DS-GVO ist die Aufsichtsbehörde befugt, auch Behörden durch förmliche Entscheidung (Verwaltungsakt) zu einem datenschutzkonformen Verhalten anzuhalten. Wirksame Befugnisse, diese Entscheidungen durchzusetzen, gibt es nicht nur wegen der bisher nicht erfolgten Umsetzung des Artikels 58 Absatz 5 DS-GVO nicht, sondern auch, weil das LDSG die Vollstreckung gegen Behörden und juristische Personen des öffentlichen Rechts nicht regelt (§ 22 des Landesvollstreckungsgesetzes). Eine Ermöglichung der Vollstreckung fehlt im LDSG und sollte beispielsweise in § 25 integriert werden, um die datenschutzrechtlichen Abhilfemaßnahmen des LfDI auch Behörden und anderen öffentlichen Stellen gegenüber effektiv durchsetzbar zu machen und seine in § 21 LDSG normierte Unabhängigkeit zu gewährleisten. Gerade die Möglichkeit, Zwangsgelder zu verhängen, könnte insbesondere im kommunalen Bereich die Bereitschaft erhöhen, den Anweisungen der Aufsichtsbehörde Folge zu leisten...“.

LfDI: *An diesen Ausführungen halten wir fest. Soweit wir außerdem in der Stellungnahme unter XV. Sonderzuständigkeit bei Ordnungswidrigkeiten im Telemedien-Bereich angeregt haben, dem LfDI in diesem Bereich die Zuständigkeit zuzuschreiben,*

ist dies zwischenzeitlich geschehen (s. o.). Soweit wir eine Bestimmung zur Beauftragung des Auftragsverarbeitungsverhältnisses durch die fachvorgesetzte Stelle angeregt haben, ist ergänzend darauf hinzuweisen, dass der Gesetzgeber inzwischen für den Schulbereich eine entsprechende Regelung getroffen hat (s. neuerdings § 115 Abs. 3e SchulG, wobei es allerdings statt „Vereinbarungen über die Datenverarbeitung im Auftrag“ nach der Terminologie der Datenschutz-Grundverordnung richtigerweise „Vereinbarungen über eine Auftragsverarbeitung“ heißen müsste).

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(3.2) Es wird generell angeregt, auf Wiederholungen des Textes der DS-GVO zu verzichten und stattdessen auf entsprechende Artikel der DS-GVO zu verweisen.

***LfDI:** Die Anregung halten wir für zutreffend und möchten sie durch Hinweis auf das europarechtliche Wiederholungsverbot unterstreichen, das nach Erwägungsgrund 8 zur Datenschutz-Grundverordnung nur dann nicht greifen soll, wenn die Aufnahme von Teilen der Verordnung in das mitgliedsstaatliche Recht erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.*

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(3.7) Hinsichtlich der Schutzmaßnahme Pseudonymisierung wurde angeregt, eine Bezugnahme auf den Aufwand zu ergänzen, wobei ergänzend auf § 9 Absatz 2 LDSG Bezug genommen wird.

***LfDI:** Die Anregung ist für uns nicht so inhaltlich nachvollziehbar.*

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(3.10) Vorgeschlagen werden Zusätze zu den Regelungen zur Ernennung eines Datenschutzbeauftragten und von dessen Aufgabenumfang. Insbesondere relevant sind dabei: Regelungen zur Freistellung – gestaffelt nach der Größe der Körperschaft – und zu den (Mindest-)Ressourcen des Datenschutzbeauftragten; Regelungen zur Möglichkeit der Ministerien, für nachgeordnete Bereiche Verfahren zu prüfen und Vorlagen an den LfDI zu übermitteln; Regelungen, die ein Beschwerderecht von bDSB eröffnen sollen, wenn Verstößen behördenintern nicht abgeholfen wurde und der Vorschlag einer Vorlagepflicht der Berichte von Datenschutzbeauftragten an den LfDI; Regelungen zu Ausschreibungsverfahen und Mindestqualifikation von externen Datenschutzbeauftragten.

LFDI: *Eine Regelung von Mindestkapazitäten und Mindestressourcen von Datenschutzbeauftragten erscheint – angesichts des Missstandes, dass teilweise Datenschutzbeauftragte z. B. für Schulen für über 100 Schulen zuständig sein sollen oder Datenschutzbeauftragte an Hochschulen nur so wenig Zeitkapazitäten erhalten, dass sie ihren Aufgaben (z. B. auch im Forschungsbereich) nicht nachkommen können, durchaus sinnvoll, soweit über die Vorgaben von Art. 37 f. DS-GVO eine Öffnungsklausel solche konkretisierenden Vorgaben zulässt (z. B. Art. 6 Absatz 2 und 3 DS-GVO). Ob ein explizites Recht zur Vorlage von Vorgängen an den LfDI bzw. gar eine Vorlagepflicht für behördliche Datenschutzbeauftragte eingeführt werden sollte, erscheint zweifelhaft. Vielmehr ist von den jeweiligen verantwortlichen Stellen, vertreten durch ihre Hausleitungen, sicherzustellen, dass die Stellung der behördlichen Datenschutzbeauftragten innerhalb der jeweiligen Organisationseinheiten eine unabhängige und effektive Arbeitsweise ermöglicht. Aus hiesiger Sicht erscheint durch die bereits bestehende Pflicht zur Datenpannenmeldung verbunden mit dem guten Austausch im Rahmen von Beratungs- und Gremienarbeit eine Vorlagepflicht derzeit nicht zwingend erforderlich.*

Stellungnahme des Verkehrsministeriums vom 30.10.2020:
(Ziff. 1) In der Verwaltungspraxis gebe es behördliche Konstellationen, bei denen die Betrauung eines Dienstleisters mit bestimmten Dienstleistungen verpflichtend sei (z. B. bei § 3 Errichtungsgesetz BITBW). Die Auftragsverarbeitungsverträge seien dabei (wohl in Folge mangelnden Wettbewerbsdrucks) häufig ein Problem. Sie würden in der Praxis „hinken“ oder seien zumindest mit mehr Aufwand verbunden als bei einer Beauftragung privater Auftragsverarbeiter. Es werde daher vorgeschlagen, die in Art. 28 Abs. 3 S. 1 Alt. 3 DS-GVO angelegte Möglichkeit einer gesetzlichen Regelung dieser Auftragsverarbeitungsverhältnisse zu nutzen, und zwar entweder per Spezialgesetz oder im LDSG, sodass dazu keine individuelle Vereinbarung i.S.d. Art. 28 Abs. 3 S. 1 Alt. 1 DS-GVO mehr nötig sei. Dasselbe sei in Bezug auf solche Dienstleister sinnvoll, die von Dienststellen fakultativ in Anspruch genommen werden könnten (z.B. fakultative Inanspruchnahme des Logistikzentrums Baden-Württemberg bei Vergabeverfahren), soweit sie eine öffentliche Stelle darstellen bzw. besitzanteilig überwiegend einer öffentlichen Stelle angehören würden.

LfDI: *Eine derartige Normierung eines Auftragsverarbeitungsverhältnisses kann durchaus sinnvoll sein und die Praxis entlasten. Ein Beispiel stellt die (inzwischen außer Kraft getretene) Corona-Verordnung Auftragsdatenverarbeitung dar. Fraglich ist allerdings, inwieweit eine einheitliche Regelung für die mutmaßlich sehr unterschied-*

lichen Leistungen der BitBW (und ggf. des Logistikzentrums) gegenüber den verschiedenen öffentlichen Stellen des Landes getroffen werden kann. Insbesondere die Ausgestaltung des Auftragsverarbeitungsverhältnisses zu den technischen und organisatorischen Maßnahmen oder zu Unterauftragnehmern erfordern möglicherweise eine auf die unterschiedlichen Auftragssituationen angepasste Regelung. Die Frage einer möglichen Vereinheitlichung sollte mit der BitBW (und ggf. mit dem Logistikzentrum) abgeklärt werden.

Wenn eine solche Regelung getroffen werden sollte, schiene das jeweilige Fachgesetzt (also z. B. das BitBW-Gesetz) als sedes materiae sachnäher als das LDSG. Auch dürfte – da ein wiederholter Aktualisierungsbedarf vorhersehbar erscheint – eine Ausgestaltung der Regelungen des Auftragsverarbeitungsverhältnisses im Einzelnen durch eine oder mehrere Rechtsverordnungen praktikabler sein als eine Normierung unmittelbar im Parlamentsgesetz.

Stellungnahme des Ministeriums für Soziales und Integration (Sozialministerium) vom 27.10.2020:
(S. 5, Abs. 1) Diskriminierungsrisiken bei einer Datenverarbeitung auf Grundlage von Algorithmen und Datenbanken – bspw. bei der Verwendung von Algorithmen – sollten Beachtung finden und ein entsprechender Schutz betroffener Personen etabliert werden. So beschreibe eine Studie der Antidiskriminierungsstelle des Bundes (aus dem Jahr 2019) Beispielfälle, in denen algorithmen- und datenbasierte Differenzierungen als Diskriminierung rechtlich festgestellt wurden. Dies würde nach der Studie einen Bedarf nach Reformen des Antidiskriminierungs- und Datenschutzrechts hervorrufen, aber ebenso gesellschaftliche Abwägungen und Festlegungen verlangen, welche algorithmen- und datenbasierten Differenzierungen in einer Gesellschaft überhaupt für akzeptabel gehalten werden.

***LfDI:** Soweit ein Diskriminierungsschutz durch algorithmenbasierte Datenverarbeitung angeregt wird, werden diese zutreffenden Bedenken durch europäische Rahmenwerke, wie die KI-VO aufgenommen.*

Stellungnahme des Ministeriums für den Ländlichen Raum und Verbraucherschutz vom 29.10.2020:
Es fehle eine mit § 5 Abs. 1 Nr. 4 LDSG a.F. vergleichbare Regelung, die es Betroffenen ermögliche, gegenüber einer Verarbeitung von Daten, auch wenn diese rechtmäßig sei, ein schutzwürdiges, in der jeweiligen persönlichen Situation begründetes Interesse einzuwenden (vgl. § 4 Abs. 6 LDSG a.F.). Eine solche Möglichkeit werde

durch das Widerspruchsrecht aus Art. 21 Abs. 1 S. 1 DS-GVO nur für Verarbeitungen aufgrund Art. 6 Abs. 1 lit. e, f DS-GVO eingeräumt. Ein solches Recht müsste ansonsten aus allgemeinen Rechtsgrundsätzen (Verhältnismäßigkeitsgrundsatz) hergeleitet werden.

Anmerkung § 5 Abs. 1 Nr. 4 LDSG a. F. lautete:

(1) „Der Betroffene hat nach Maßgabe dieses Gesetzes ein Recht auf

1. ...
2. ...
3. ...
4. Einwendung eines schutzwürdigen, in seiner persönlichen Situation begründeten Interesses gegenüber der Verarbeitung seiner Daten (§ 4 Abs. 6), ...“

Und hierzu wurde in § 4 Abs. 6 LDSG a. F. geregelt:

(6) „Der Betroffene hat das Recht, gegenüber der Verarbeitung seiner Daten, auch wenn diese rechtmäßig ist, ein schutzwürdiges, in seiner persönlichen Situation begründetes Interesse einzuwenden (Einwendungsrecht). Die Verarbeitung ist in diesem Fall nur zulässig, wenn eine Abwägung ergeben hat, dass sein Interesse hinter dem öffentlichen Interesse an der Verarbeitung zurückzustehen hat. 3Das Ergebnis der Abwägung ist ihm unter Angabe der Gründe mitzuteilen. 4Sätze 1 bis 3 finden keine Anwendung in den in § 33 Abs. 3 genannten Fällen.“

LfDI: *Für uns ist nicht ersichtlich, dass insoweit eine Öffnungsklausel der DS-GVO zur Verfügung stünde. Das Widerspruchsrecht aus Art. 21 DS-GVO gilt unmittelbar.*

Stellungnahme des Staatlichen Schulamts Karlsruhe vom 24.09.2020:
(S. 2) Gewünscht wird eine Befreiung von Schulwebsites von Anforderungen hinsichtlich TLS-Verschlüsselung für HTTPS-Verbindungen, „Cookie-Richtlinien“, soweit es sich lediglich um „Visitenkartenseiten“ handelt. Darüber hinaus fehlten objektive Kriterien zum Beispiel bei der Auswahl einer Schulleitung für kollaborative, digitale Werkzeuge im pädagogischen Kontext oder auch bei der Suche nach datenschutzkonformen Lösungen zum Zwecke des Fernlernunterrichts. Auch sei die Lage zur Nutzung von Software unbefriedigend, die cloudbasiert arbeite und auf Grund von Monopolstellungen der anbietenden US-Firmen nicht mit der DS-GVO konformgehe.

LfDI: *Die vom Staatlichen Schulamt angeführten Anforderungen an Websites sind grundlegende Standards der IT-Sicherheit und zum Schutz von Endgeräten vor einer ungewünschten Speicherung von Informationen. Diese Standards bei der Gestaltung von Websites und informationstechnischen Diensten sind nicht verhandelbar und auch nicht unverhältnismäßig.*

Nachvollziehbar ist, dass die Prüfung der Datenschutzkonformität von digitalen Werkzeugen den Schulen einen erheblichen Aufwand abverlangt. Hier schafft allerdings die digitale Bildungsplattform, die das Kultusministerium den Schulen anbietet, eine beachtliche Abhilfe; im Übrigen werden künftig auch die jüngsten Änderungen im Schulgesetz, die namentlich den Einsatz digitaler Medien und digitaler „Lehr- und Lernformen" betreffen, zu beachten sein (s. z. B. § 115b des Schulgesetzes). Auch wenn die Regelungen im Schulgesetz aus Sicht des LfDI teilweise nicht hinreichend normenklar sind (oder gegen sie andere Bedenken bestehen), erscheint insoweit jedenfalls eine Änderung des Landesdatenschutzgesetzes nicht geboten. Die Schulen werden insoweit durch ihre Datenschutzbeauftragten und das Kultusministerium unterstützt; auch der LfDI bietet Beratung und insbesondere – in Bezug auf das Lehrpersonal gemeinsam mi dem ZSL – Fortbildungen für den Schulbereich an.

Stellungnahme des Ministeriums für Kultus, Jugend und Sport vom 07.10.2020:
(S.1 f.) Eine Datenschutz-Folgeabschätzung (DSFA) sei eine sehr komplexe Angelegenheit. Zudem gebe es bislang keine Negativliste von Verarbeitungen, für die keine DSFA erforderlich sei. Vorgeschlagen wird die Schaffung einer spezialgesetzlichen Norm vergleichbar § 9 LDSG RLP (in der Fassung vom 08.05.2018).
Diese Norm aus Rheinland-Pfalz laute wie folgt:

> „§ 9 Datenschutz-Folgenabschätzung
> (1) Eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der Datenschutz-Grundverordnung durch den Verantwortlichen kann unterbleiben, soweit
> 1. eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Ministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird oder
> 2. der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine Datenschutz-Folgenabschätzung erfolgt ist, es sei denn, dass in der Rechtsvorschrift etwas anderes bestimmt ist.
> Die Ministerien stellen den öffentlichen Stellen die Ergebnisse der von ihnen und der von ihnen ermächtigten öffentlichen Stellen durchgeführten Datenschutz-Folgenabschätzungen zur Verfügung.

(2) Entwickelt eine öffentliche Stelle ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, so kann sie, sofern die Voraussetzungen des Artikels 35 Abs. 1 der Datenschutz-Grundverordnung bei diesem Verfahren vorliegen, die Datenschutz-Folgenabschätzung nach den Artikeln 35 und 36 der Datenschutz-Grundverordnung durchführen. Soweit das Verfahren von öffentlichen Stellen im Wesentlichen unverändert übernommen wird, kann eine weitere Datenschutz-Folgenabschätzung durch die übernehmenden öffentlichen Stellen unterbleiben."

In eine vergleichbare Richtung geht die Stellungnahme des Staatlichen Schulamts Karlsruhe vom 24.09.2020:
Aus Sicht der Schulen bleibe unklar, ob und wie DSFA durchzuführen (bzw. verpflichtend) sei.

LfDI: *Vorzugswürdig erschiene hier wohl, einen (evtl. auch konkretisierenden) Verweis auf Art. 35 Abs. 1 S. 2 DS-GVO und Art. 35 Abs. 10 DS-GVO zu schaffen, der mögliche Probleme des § 9 LDSG RLP auslässt.*
§ 9 LDSG RLP ist keine Norm, die als Vorbild für eine entsprechende Regelung im LDSG BW dienen sollte: So ist für die Regelung des § 9 Abs. 1 S. 1 Nr. 1 LDSG RLP bereits keine taugliche Öffnungsklausel ersichtlich. Abgestellt wurde hierfür wohl auf Art. 35 Abs. 1 S. 2 DS-GVO (vgl. Landtag RLP, Drs. 5703/17, S. 64 „Zu § 9, Zu Absatz 1"). Ob Art. 35 Abs. 1 S. 2 DS-GVO überhaupt einen solchen Rechtssetzungsrahmen bietet, ist jedoch äußerst fraglich. Der Inhalt des Art. 35 Abs. 1 S. 2 DS-GVO wurde zudem durch § 9 Abs. 1 S. 1 Nr. 1 LDSG RLP wohl zu sehr verfremdet. Dies ist jedoch nicht nötig: Art. 35 Abs. 1 S. 2 DS-GVO erlaubt bereits aus sich selbst heraus eine Datenschutz-Folgenabschätzung für die Untersuchung ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken, unter anderem dann, wenn ***mehrere Verantwortliche*** *gemeinsame Anwendungen/Verarbeitungsumgebungen nutzen wollen, vgl. ErwG 92 DS-GVO. In diesen Fällen ist es ratsam, eine Referenz-DSFA gemeinsam zu nutzen bzw. öffentlich zugänglich zu machen;* ***zudem*** *müssen die in der DSFA beschriebenen* ***Maßnahmen umgesetzt*** *und eine* ***Begründung vorgelegt*** *werden können, warum eine einzige DSFA ausreichend ist (WP 248 Rev. 01, S. 8). Insbesondere die letztgenannten Anforderungen spiegeln sich nicht in § 9 Abs. 1 S. 1 Nr. 1 LDSG RLP wider. Dadurch ergibt sich eine nicht unerhebliche Wahrscheinlichkeit, dass Referenz-DSFA „blind" als reine Formalie übernommen werden könnten, obwohl sie auf die konkreten Anwendungsfälle überhaupt nicht zutreffen. Da DSFA überhaupt erst ab einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen erforderlich sind, wären die aus einer solchen Regelung erwachsenden Ge-*

fahren als zu hoch zu betrachten. Dasselbe gilt für § 9 Abs. 2 LDSG RLP, der ebenfalls auf Art. 35 Abs. 1 S. 2 DS-GVO beruht (vgl. Landtag RLP, Drs. 5703/17, S. 64 „Zu § 9, Zu Absatz 2“).

Auch § 9 Abs. 1 S. 2 LDSG RLP vermag in diesem Gefüge nicht zu überzeugen. Was i.d.S. von den „Ergebnisse(n)“ der von den Ministerien durchgeführten Datenschutz-Folgeabschätzungen inhaltlich umfasst sein soll, erschließt sich nicht. Wo keine komplette DSFA bereitgestellt wird, wäre es sonstigen Verantwortlichen, die auf diese zugreifen, quasi unmöglich, zu beurteilen, ob konkrete Faktoren, die zum Ergebnis geführt haben, auch bei ihnen vorliegen. Hinsichtlich § 9 Abs. 1 S. 1 Nr. 2 LDSG RLP ist zudem umstritten, ob der europäische Verordnungsgeber mit Art. 35 Abs. 10 DS-GVO überhaupt eine Öffnungsklausel etablieren wollte, wie sie der rheinland-pfälzische Gesetzgeber wohl erkannt hat (vgl. Landtag RLP, Drs. 5703/17, S. 64 „Zu § 9, Zu Absatz 1“ a.E.). Gegen eine solche Öffnungsklausel spricht u.a. der Wortlaut des Art. 35 Abs. 10 DS-GVO (u.a. von Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 35 Rn. 57; a.A. Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 35 Rn. 64a). Art. 35 Abs. 10 DS-GVO ist insoweit richtigerweise nicht als Öffnungsklausel für eine Datenschutzgesetzgebung, sondern als Berechtigung der Mitgliedstaaten, eine Verlagerung der Verantwortung für eine DSFA in das Gesetzgebungsverfahren vorzunehmen, aufzufassen (Roßnagel/Geminn/Johannes, ZD 2019, 435 (436)).

Im Ergebnis vorzugswürdig erschiene hier wohl, einen (evtl. auch konkretisierenden) Verweis auf Art. 35 Abs. 1 S. 2 DS-GVO und Art. 35 Abs. 10 DS-GVO zu schaffen. Berücksichtigt werden sollten dabei die o.g. Anforderungen des WP 248 Rev 01, S. 8.

III. Anregung zur Anpassung von Vorschriften außerhalb des LDSG

Stellungnahme des Wissenschaftsministeriums vom 28.06.2021:
(3.8) Hinsichtlich der Regelung des § 85a Abs. 2 LBG, der zufolge eine Zustimmung der obersten Dienstbehörde für eine Auftragsverarbeitung in Bezug auf Personalaktendaten erforderlich sei, könne eine „Nachsteuerung in Betracht“ kommen.

***LfDI:** Hier wird weder der Bedarf nach einer Nachsteuerung näher erläutert noch ein konkreter Vorschlag für eine solche Nachsteuerung unterbreitet. Wir sehen daher derzeit keinen Abänderungsbedarf. Die zusätzliche Kontrolle durch die oberste*

Dienstbehörde erscheint mit Blick auf die Sensibilität der Personalaktendaten als eine sinnvolle Schutzmaßnahme.

Stellungnahme des Ministeriums für Umwelt, Klima und Energiewirtschaft (Umweltministerium) vom 19.10.2020:
(Ziff. 3) Angemerkt wird, dass erhebliche datenschutzrechtliche Unsicherheiten bzgl. Verfahrensformen wie Videokonferenzen, Onlinechats oder ähnlichen Kommunikationsformen, die nach dem PlanSiG nun möglich seien, bestünden.

LfDI: *Hier würde sich wohl eine (sachnähere) Regelung im PlanSiG statt dem LDSG anbieten.*

Stellungnahme des Ministeriums für Justiz und für Europa vom 09.10.2020:
(S. 2) Es wird darauf hingewiesen, dass teilweise angeregt wurde, eine besondere Stelle zur Aufsicht im Justizsystem zu schaffen, vgl. auch ErwG 20 S. 3 DS-GVO.

LFDI: *Dieser Anregung schließen wir uns ausdrücklich an. Sie entspricht einer Forderung, die durch die Datenschutzkonferenz bereits mit Schreiben vom 25. April 2022 an die Justizministerkonferenz herangetragen wurde. Hierauf hat der bayerische Staatsminister der Justiz als damaliger Vorsitzender der Justizministerkonferenz mit Schreiben vom 02.08.2022 geantwortet, dass eine Erörterung der Thematik auf einer Tagung Ende September 2022 geprüft werde. Ggf. wäre beim Ministerium für Justiz und für Europa nachzufragen, ob hierzu zwischenzeitlich eine Position gefunden wurde.*

<u>Gesetz zur Anpassung des besonderen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 für Justiz- und Bußgeldbehörden sowie zur Änderung vollzugsrechtlicher Gesetze (LDSG-JB)</u>
Stellungnahme der Richterin Starke beim VG Stuttgart vom 26.08.2020
Der Anwendungsbereich sei in § 1 Absatz 2 LDSG-JB nicht gleichlaufend zu demjenigen der JI-Richtlinie geregelt. Die JI-Richtlinie gelte für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden für die 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. Dieses Anwendungsfeld werde auch von § 1 Absatz 1 LDSG und § 2 Absatz 1 LDSG-JB eröffnet. Nach § 1 Absatz 2 LDSG-JB und § 2 Absatz 1 Satz 3 LDSG-JB gelte das Gesetz indes für Behörden außerhalb des Geschäftsbereichs des Justizministeriums nur für die Verarbeitung personenbezogener Daten zur „Verfolgung und

Ahndung von Straftaten oder Ordnungswidrigkeiten oder zur Vollstreckung von Geldbußen“. Die Zwecke der Verhütung, Ermittlung und Aufdeckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit seien demgegenüber vom Wortlaut von § 1 Absatz 2 und § 2 Absatz 1 Satz 3 LDSG-JB nicht erfasst, so dass fraglich erscheine, ob insoweit etwa das Landesdatenschutzgesetz anstelle des LDSG-JB gelten solle.

LfDI: *Der Kritik schließen wir uns an. Wir können nicht ohne weiteres erkennen, warum die Anwendbarkeit auf Behörden außerhalb des Justizbereichs auf die Verarbeitung personenbezogener Daten zur Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten oder zur Vollstreckung von Geldbußen erfasst wird. Dies bedarf einer Überprüfung und ggf. Klarstellung im Gesetzestext.*

Darüber hinaus weise wir auf einen weiteren potentiellen Umsetzungsmangel im LDSG-JB hin: In dessen Anwendungsbereich scheint die Vorschrift des Art. 28 Absatz 2 JI-Richtlinie nicht hinreichend umgesetzt. Diese lautet:

> *„Die Mitgliedstaaten sehen vor, dass bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen, die Aufsichtsbehörde konsultiert wird.“*

Diese wird in § 89 Absatz 2 PolG für den Bereich der Polizei ordnungsgemäß umgesetzt. Für die Regelungen betreffend die Verarbeitung personenbezogener Daten Bereich außerhalb der JI-Richtlinie findet sich eine entsprechende Regelung in § 26 Absatz 2 LDSG. Wir empfehlen daher, eine solche Regelung auch in das LDSG-JB aufzunehmen oder dort – z. B. in § 8 Absatz 1 Satz 3 LDSG-JB – die Regelung aus § 26 Absatz 2 LDSG für anwendbar zu erklären.

Stellungnahme des Rundfunkbeauftragten für den Datenschutz beim SWR zur **Evaluierung des Landesdatenschutzgesetzes** - 2-0557.8/7

Mit nationalen Regelungen zum Datenschutz können die Öffnungsklauseln der DSGVO ausgeschöpft werden. Das deshalb erlassene baden-württembergische Landesdatenschutzgesetz (LDSG BW) sieht vor, dass nach 2 Jahren eine Evaluierung vorgenommen wird, zu der aus meiner Sicht folgendes festzustellen ist:

I. Die Erfahrung der vergangenen Jahre zeigt, dass die Herausforderung in der **Umsetzung der DSGVO** lag (und liegt) und glücklicherweise weniger bei den Regelungen des LDSG BW. Berücksichtigt werden muss auch, dass die datenschutzrechtlichen Regelungen für den **journalistischen Bereich** bislang im Rundfunkstaatsvertrag geregelt waren und jetzt dann im neuen Medienstaatsvertrag.

II. Zunächst muss darauf hingewiesen werden, dass sich das datenschutzrechtliche **Kontrollmodell beim SWR** bewährt hat, nur einen Rundfunkdatenschutzbeauftragten als Aufsichtsbehörde vorzusehen und nicht noch zusätzlich einen internen behördlichen Datenschutzbeauftragten (gleiches gilt für den in etwa gleich großen NDR). Denn eine Doppelstruktur mit Aufsicht nach Art. 51 DSGVO einerseits und behördlichem Datenschutzbeauftragten nach Art. 37 DSGVO andererseits ist für ein einzelnes Unternehmen wie den SWR wenig sinnvoll, weshalb insoweit die bisherige Regelung in § 27 LDSG BW beibehalten werden sollte.

III. Unabhängig davon sollten beim § 27 (Rundfunkbeauftragter für den Datenschutz) folgende Ergänzungen und Klarstellungen vorgenommen werden:

1. Zunächst muss ganz formal darauf hingewiesen werden, dass in § 27 Abs. 1 LDSG BW der **Verweis** auf § 16 c Rundfunkstaatsvertrag durch einen Verweis auf § 42 Medienstaatsvertrag **geändert** werden muss.

2. Der Rundfunkdatenschutzbeauftragte hat mit dem SWR ein (privatrechtliches) **Arbeitsverhältnis**, welches durch die öffentlich-rechtlichen Bestimmungen in § 27 überlagert und modifiziert wird. **Endet die Amtszeit**, so fällt er regelmäßig in ein normales Arbeitsverhältnis zurück. Es besteht dann die Gefahr, dass er als unbequem gewordener Datenschützer Nachteile zu befürchten hat. Deshalb könnte man nach § 27 Abs. 4 Satz 3 folgende Formulierung einfügen: *Er darf auch nach dem Ende seiner Amtszeit nicht wegen seiner Aufgabenerfüllung benachteiligt werden.* Meine Erfahrungen im Hinblick auf andere Kolleginnen und Kollegen öffentlich-rechtlichen Rundfunkanstalten lässt mich diesen Vorschlag machen, wobei mich selbst dies **nicht** betrifft, da bei mir das Ende meiner Amtszeit mit meinem Eintritt in den Ruhestand praktisch zusammenfällt.

3. In § 27 Abs. 3 Satz 2 wird der Grundsatz festgehalten, dass eine angemessene Vergütung zu erfolgen hat. Die näheren Bestimmungen werden dann durch Satz 3 dem Rundfunk- sowie Verwaltungsrat überantwortet.

   a) Fraglich ist, ob der Gesetzgeber diese Ausgestaltung den Gremien überlassen durfte. Denn nach dem Wortlaut und Systematik der DSGVO ist für diese **wesentliche** Frage der **Gesetzgeber zuständig**. Denn in Art. 52 Abs. 4 DSGVO ist festgehalten, dass der Mitgliedstaat die Ressourcen und Ausstattung und damit die grundsätzlichen Bestimmungen selbst vorzunehmen hat. In Art. 53 Abs. 1 DSGVO ist **nur** vorgesehen, dass die Mitgliedstaaten die **Ernennung** auf eine unabhängige Stelle verlagern können (hier also auf Rundfunk- und Verwaltungsrat), aber eine entsprechende Regelung für Frage, wer die Grundsätze der Vergütung oder den Status festzulegen hat, kann daraus nicht abgeleitet werden.
   b) Im Hinblick auf die Regelung in Art. 52 Abs. 4 hat deshalb **der Gesetzgeber** in § 23 Abs. 4 LDSG BW konsequenterweise **selbst die Einordnung** des Landesdatenschutzbeauftragten in die Besoldungsstruktur des Landes vorgenommen und ihm die Ebene

zugewiesen, welche durch die Besoldungsgruppe B 6 (§ 23 Abs. 4 S. 1) repräsentiert wird. Es wurde also eine Statusbestimmung und Festlegung der Position innerhalb der baden-württembergischen Verwaltung vorgenommen. Eine derartige Einordnung und Statusfeststellung (die unabhängig von der konkreten finanziellen Entlohnung ist) fehlt beim Rundfunkbeauftragten für den Datenschutz.

c) Es hat sich gezeigt, dass eine derartige Statusfeststellung durch den Gesetzgeber selbst erforderlich ist. Beim SWR stehen an der Spitze der Intendant und die Direktoren. Nächste Ebene bildet die (wachsende) Zahl von Hauptabteilungsleitern (30-40 Personen) sowie dann die der Abteilungsleiter (120-130 Personen). Während die Abteilungsleiter noch tarifvertraglichen Bindungen unterliegen, ist dies bei den Hauptabteilungsleitern nicht mehr der Fall.

d) Im Rahmen der Umsetzung von § 27 Abs. 3 Satz 3 LDSG BW hat die damalige Geschäftsleitung den Rundfunkdatenschutzbeauftragten nur als Abteilungsleiter eingestuft. Damit werden ihm nicht nur die für Hauptabteilungsleiter vorgesehenen Besonderheiten versagt (z.B. was die Raumausstattung anbelangt) und der Tarifbindung unterworfen, was seiner unabhängigen Stellung nicht gerecht wird, sondern damit wird auch innerhalb (und außerhalb) des SWR offenbart, dass man ihm nur einen Status einräumt, der mit dem Sinn und Zweck der Aufgabenerfüllung einer unabhängige Aufsichtsbehörde nach Art. 51 ff. DSGVO nicht zu vereinbaren ist.

e) Zusammenfassend ergibt sich damit, dass es aufgrund Art. 54 Abs. 4 DSGVO notwendig ist, dass der Status des Rundfunkbeauftragte für den Datenschutz jetzt **vom Gesetzgeber** bestimmt wird, er also festlegt, auf welcher Ebene und Hierarchiestufe im SWR der Rundfunkbeauftragte für den Datenschutz eingruppiert werden muss.

4. Nach § 27 Abs. 10 LDSG BW hat in Ergänzung und Ausführung zu Art. 59 DSGVO der Rundfunkdatenschutzbeauftragte jährlich einen **Tätigkeitsbericht** sowohl an die Landtage als auch die Landesregierungen der den SWR-Staatsvertrag unterzeichnenden Länder zu übermitteln. Die Erfahrungen haben folgendes gezeigt: Die Landesregierungen haben auf die Berichte von

2018 und 2019 nicht reagiert. Der Landtag von Baden-Württemberg hat den Bericht zwar auf die Tagesordnung des Ständigen Ausschusses genommen, aber dann ohne Aussprache zur Kenntnis genommen. In Rheinland-Pfalz fand eine kurze Erörterung im zuständigen Ausschuss statt.
Es stellt sich die Frage, ob damit diese Pflichten nach § 27 Abs. 10 LDSG BW so beibehalten werden sollen.

5. Abschließend sei noch auf die **Zusammenarbeit der Aufsichtsbehörden untereinander** eingegangen: Auch wenn die praktische Zusammenarbeit mit den Landesdatenschutzbeauftragten von Baden-Württemberg und Rheinland-Pfalz seit Jahren funktioniert, wäre es doch hilfreich, wenn der Landesgesetzgeber für eine stärkere Einbindung der Rundfunkbeauftragten für den Datenschutz in die **nationale Datenschutzkonferenz** (DSK) sorgen könnte. So könnte man § 25 Abs. 1 LDSG BW um folgenden Satz ergänzt: *„Der Landesdatenschutzbeauftragten arbeitet mit allen anderen Aufsichtsbehörden zusammen und unterstützt sie“* (vergleiche auch die entsprechende Vorschrift für den Bundesdatenschutzbeauftragten in § 14 Abs. 1 Nr. 7 BDSG).

Ich möchte mich nochmals für die Gelegenheit zur Stellungnahme und Darstellung der Erfahrungen bedanken und verbleibe

mit freundlichen Grüßen

Prof. Dr. Armin Herb
Rundfunkbeauftragter für den
Datenschutz beim SWR

30.10.2020

Anlage 6

Gemeindetag Baden-Württemberg

Landkreistag BADEN-WÜRTTEMBERG

Ministerium des Inneren, für Digitalisierung
und Kommunen Baden-Württemberg

Willy-Brandt-Straße 41
70173 Stuttgart

29.10.2021

Stellungnahme der Kommunalen Landesverbände Baden-Württemberg zur Evaluierung des Landesdatenschutzgesetzes
Ihr Schreiben vom 21.06.2021 | Az.: IM2-0557-11/1/7

Sehr geehrter Herr

für die Möglichkeit zur Beteiligung an der Evaluierung des Landesdatenschutzgesetzes (LDSG) bedanken wir uns ganz herzlich. Nachfolgend erlauben wir uns einige generelle Hinweise zur Praxistauglichkeit des Gesetzes sowie spezielle Anmerkungen zu § 18 LDSG (Videoüberwachung öffentlich zugänglicher Räume) und weiteren Einzelpunkten.

Bereits seit vielen Jahren wird die Erfüllung kommunaler Aufgaben durch einen kontinuierlichen Aufwuchs an bürokratischen Anforderungen ebenso wie eine regelmäßige Erhöhung von Standards belastet. In Anerkennung der hohen Bedeutung des Grundrechts auf informationelle Selbstbestimmung, spielen datenschutzrechtliche Vorgaben in diesem Gesamtkontext jedoch eine besondere Rolle. Das Inkrafttreten der europäischen Datenschutzgrundverordnung (DSGVO) im Jahr 2018 einschließlich der in ihrem Gefolge geänderten nationalstaatlichen Rechtsakte hat die organisatorische, technische und finanzielle Belastung der Kommunen noch einmal erheblich verschärft. Insbesondere kleinere Gemeinden mit weniger mitarbeiterstarken Verwaltungen wurden dabei über Gebühr belastet. Dementsprechend sind die Problemanzeigen aus der kommunalen Praxis auch drei Jahre nach Inkrafttreten der DSGVO nicht wesentlich abgeebbt. Im Kern wird vielfach ein Mangel an Praxistauglichkeit bei der Auslegung und Anwendung von datenschutzrechtlichen Vorschriften problematisiert. In der kommunalen Praxis führt dies nicht nur zu einer erheblichen (Mehr)Belastung der Verwaltung, sondern oftmals auch zum Abbruch von Projekten oder der Einstellung von (freiwilligen) Angeboten. In der Folge haftet dem Datenschutz heute in der öffentlichen Wahrnehmung eher das Image eines Verhinderungsinstruments, denn eines wirksamen Mittels zur Durchsetzung des Grundrechts auf informationelle Selbstbestimmung an.

Gemeindetag Baden-Württemberg
Panoramastr. 31, 70174 Stuttgart

Landkreistag Baden-Württemberg
Panoramastr. 37, 70174 Stuttgart

Vor diesem Hintergrund plädieren wir eindringlich dafür, etwaige Änderungen des LDSG vor deren Umsetzung stets im Lichte von Umsetzbarkeit und Praxistauglichkeit zu überprüfen und vorhandene Öffnungsklauseln der DSGVO in diesem Sinne zu nutzen. Dies schließt insbesondere auch die Verschärfung von Sanktionsmöglichkeiten gegenüber Behördenmitarbeitern und Behörden ein. Wir bitten darum, dass die Komplexität des Datenschutzrechts auch bei einer etwaigen Umsetzung des nachvollziehbaren Wunsches nach Sanktionierung von Datenschutzverstößen eine angemessene Berücksichtigung findet.

Darüber hinaus möchten wir nachfolgend einige ergänzende Anmerkungen speziell zu § 18 LDSG (Videoüberwachung öffentlich zugänglicher Räume) einbringen. Die datenschutzrechtlichen Vorschriften zur Videoüberwachung öffentlich zugänglicher Räume sind für die Städte, Gemeinden und Landkreise in Baden-Württemberg von besonderer praktischer Relevanz und verdienen deshalb hier eine gesonderte Erwähnung.

In § 18 Abs. 1 Satz 1 LDSG ist der Einschub „im Einzelfall“ zu streichen. Diese Begrifflichkeit ist missverständlich. Es besteht Klarheit darüber, dass keine anlasslose, rein präventive Videoüberwachung der gesamten Gemeinde möglich ist. Die Überwachung beschränkt sich von sich aus und auf der Basis der weiteren in Abs. 1 genannten Vorgaben automatisch auf bestimmte definierte Zeiträume, Bereiche sowie Sachverhalte und damit auf „Einzelfälle“.

Darüber hinaus sollte § 18 Abs. 1 LDSG hinsichtlich der Zulässigkeit der Videoüberwachung zur Verhinderung von Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung präzisiert werden. In dieser Hinsicht war § 20a LDSG a. F. der aktuellen Regelung in § 18 Abs. 1 i. V. m. Abs. 3 LDSG überlegen. In § 20a LDSG a. F. wurde klar herausgehoben, dass die Videoüberwachung „insbesondere zur Verhinderung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung“ zulässig ist. Diese Klarstellung wurde nicht in § 18 LDSG übernommen. Überwiegend ist die Verhinderung von Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung jedoch die Ursache für den Wunsch einer Videoüberwachung im kommunalen Raum. Die Regelung in § 18 LDSG erschwert zum einen die Begründung, zum anderen beschränkt sie die Videoüberwachung auf den Schutz vor Straftaten und Ordnungswidrigkeiten gegen die in Abs. 1 Nr. 1 genannten Rechtsgüter und die in Abs. 1 Nr. 2 genannten baulichen Anlagen und Sachen.

Für § 18 Abs. 1 LDSG wird dementsprechend folgende Formulierung vorgeschlagen:

> „Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist,
>
> 1. um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich in öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder
>
> 2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen zu schützen, oder
> 3. um die Begehung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung zu verhindern oder deren Verfolgung zu ermöglichen

und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen."

Ferner regen wir an, § 18 Abs. 4 LDSG komplett zu streichen oder zumindest zu überarbeiten. In der Praxis ist es nicht auszuschließen, dass beispielsweise bei der Überwachung eines Schulgeländes ein Anwohner erfasst wird, der dort zulässigerweise seinen Hund ausführt. In einer kleineren Gemeinde wird die überwachende Stelle (Ordnungsamt) diese Person anhand der Aufnahmen (und ggf. des Hundes) erkennen können. Es lägen somit personenbezogene Daten vor, so dass die Person über die Aufzeichnung und die Löschung informiert werden müsste. Dies stellt einen unverhältnismäßigen Verwaltungsaufwand ohne jeglichen Nutzen dar. Die Informationspflicht für die Erhebung personenbezogener Daten für diejenigen Fälle, die tatsächlich gespeichert bleiben, ergibt sich bereits aus Art. 14 DSGVO.

Weiterhin sprechen wir uns gegen die seitens des Landesbeauftragten für den Datenschutz und die Informationsfreiheit geforderte Streichung der in § 18 Abs. 5 LDSG geregelten Vierwochenfrist aus. In der Praxis kommt es häufig vor, dass Meldungen über Sachbeschädigungen nicht immer sofort erfolgen oder die Videoaufzeichnungen nicht immer unverzüglich durch die zuständigen Personen ausgewertet werden können. Eine Verkürzung der Vierwochenfrist würde in der Praxis in zahlreichen Fällen daher zum Schutz von Straftätern führen.

Abschließend erlauben wir uns die folgenden Anmerkungen und Vorschläge zu weiteren Einzelregelungen des LDSG.

- Zur weiteren Verständlichkeit des LDSG regen wir an, § 2 Abs. 1 Satz 2 LDSG um folgenden, kursiv gestellten Einschub zu ergänzen:

  „Die öffentliche Stelle ist zugleich Verantwortlicher nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit dieses *oder ein anderes* Gesetz nichts ~~anderes~~ *abweichendes* bestimmt."

  Auch in Kenntnis der bestehenden Regelung des § 2 Abs. 3 LDSG, halten wir eine Konkretisierung der Definition des Verantwortlichen an dieser Stelle für zweckmäßig. Dies würde bereits in der Definition den Hinweis auf Spezialregelung wie die des § 67 Abs. 4 SGB X lenken.

- Insbesondere durch die pandemische Lage in den letzten Monaten wurde die zeitweise Verlagerung der Arbeitstätigkeit in den privaten Bereich – üblicherweise unter den Stichworten Homeoffice bzw. mobiles Arbeiten – stark forciert. Wenngleich dies oftmals über Dienstvereinbarungen o. Ä. berücksichtigt wurde, hat dies bspw. Auswirkungen auf den Zugang zu den Diensträumen i. S. d. § 26 Abs. 1 Nr. 2 LDSG. Sofern hierbei eine Ausweitung auf den grundgesetzlich geschützten Bereich der Wohnung angedacht wird, sollte dies gegebenenfalls auf eine gesetzliche Grundlage gestützt werden.

Für die Berücksichtigung unserer Stellungnahme in dem Abschlussbericht für den Landtag bedanken wir uns.

Mit freundlichen Grüßen

Steffen Jäger
Präsident

Prof. Dr. Alexis von Komorowski
Hauptgeschäftsführer

Gemeindetag Baden-Württemberg
Panoramastr. 31, 70174 Stuttgart

Landkreistag Baden-Württemberg
Panoramastr. 37, 70174 Stuttgart