Schleswig-Holsteinischer Landtag
Umdruck 19/6864

Landesbeauftragte für Datenschutz · Postfach 71 16 · 24171 Kiel

Innen- und Rechtsausschuss
des Schleswig-Holsteinischen Landtages
Landeshaus
Düsternbrooker Weg 7024105 Kiel

Per E-Mail an:
innenausschuss@landtag.ltsh.de

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

Ansprechpartner/in:
Frau Hansen
Durchwahl: 988-1200

Aktenzeichen:
LD-03.13/21.001

Kiel, 30.11.2021

Stellungnahme zum Entwurf eines Digitalisierungsgesetzes, Drucksache 19/3267
Ihre E-Mail vom 05.10.2021

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren,

vielen Dank für die Gelegenheit zur Stellungnahme zum Entwurf eines Gesetzes zur Förderung der Digitalisierung und Bereitstellung von offenen Daten und zur Ermöglichung des Einsatzes von datengetrieben Informationstechnologien in der Verwaltung (Digitalisierungsgesetz).

Ich beschränke mich in meinen folgenden Anmerkungen auf die Punkte, die meinen Aufgabenbereich des Datenschutzes und der Informationsfreiheit betreffen:

I. Zu Artikel 4 – E-Government-Gesetz

a) Begriff „Stand der Technik“

In § 2 Nr. 9 wird der Begriff *„Stand der Technik“* eingeführt (siehe Drs. 19/3267, S. 32) und auf S. 90 des Entwurfs ergänzend erläutert. Der enthaltene Verweis auf die Rechtsprechung des BVerfG ist zwar korrekt, erweist sich im Hinblick auf das zu beachtende EU-Recht im Bereich des Datenschutzes aber als unvollständig: Bezüglich der auch hier maßgeblichen Anforderungen an die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO sollte zur **Vermeidung von Missverständnissen** zumindest in der Gesetzesbegründung darauf eingegangen werden, dass der Begriff „Stand der Technik“ auch europarechtlich ausgelegt werden muss. Hinweise zur Interpretation auf EU-Ebene finden sich u. a. in einem Arbeitspapier des Europäischen Datenschutzausschusses („Leitlinien 4/2019 zu Artikel 25, Datenschutz durch Technikgestaltung

und durch datenschutzfreundliche Voreinstellungen“, Version 2.0, angenommen am 20. Oktober 2020, Rn. 18-22[1]).

b) Begriff „Informationssicherheit“

In § 2 Nr. 11 wird Informationssicherheit als Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen definiert, siehe auch die Erläuterung, Drs. 19/3267, S. 91 f. Auch hier sollte zur **Vermeidung von Missverständnissen** geprüft werden, ob der Begriff *„Informationssicherheit“* im gesamten Digitalisierungsgesetz gleich verwendet wird oder weitere Angleichungen an den Stellen vorgenommen werden sollten, an denen dasselbe gemeint ist. In Artikel 12 (IT-Einsatz-Gesetz-E) wird zwar auf die Verwendung anerkannter Standards der Informationssicherheit verwiesen (§ 10 Abs. 2 des IT-Einsatz-Gesetz-E, Drs. 19/3267, S. 61), jedoch ist der Paragraf betitelt mit *„Sicherheit, Robustheit und Resilienz“* und nur Absatz 2 geht auf *„Integrität, Vertraulichkeit und Verfügbarkeit“* (hier könnte sich ein Angleichen der Reihenfolge dieser drei Gewährleistungsziele anbieten) ein. Dies könnte so verstanden werden, dass Robustheit und Resilienz nicht auch der Informationssicherheit zuzuordnen wären. Dies widerspräche aber zumindest für den Bereich der personenbezogenen Daten der Anforderung des Art. 32 Abs. 1 Buchst. b DSGVO, der auch Belastbarkeit / Resilienz umfasst (deutsch: *„die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste“* / englisch: *„confidentiality, integrity, availability and resilience of processing systems and services“*).

c) Grenzen zentraler Ver- und Entschlüsselung als Basisdienst

In § 12 Abs. 2 (ehemals § 8) Nr. 4 E-Government-Gesetz-E (Drs. 19/3267, S. 38) wird als ein möglicher Basisdienst *„die sichere Kommunikation sowie der sichere Nachrichtentransport zwischen den Verfahrensbeteiligten sowie anderen Nutzerinnen und Nutzern von Verwaltungsleistungen und der Verwaltung, die die Funktionalitäten Signaturprüfung, Ver- und Entschlüsselung, ... umfasst“* genannt.

In diesem Zusammenhang sei darauf hingewiesen, dass in einzelnen Verfahren die Anforderungen an eine hohe Vertraulichkeit und Integrität **nicht ausschließlich durch *zentrale* Ver- und Entschlüsselungskomponenten erfüllt** werden können, da sich der Schutz der Verschlüsselung nur von bzw. bis zur zentralen Stelle, nicht aber bis zum Absender bzw. Empfänger erstrecken würde. Es wird daher angeregt, nicht die Formulierung *„die **sichere** Kommunikation sowie der **sichere** Nachrichtentransport“* zu verwenden, die gerade in Zusammenhang mit § 2 Nr. 11 (Definition von Informationssicherheit, Drs. 19/3267, S. 32) den Eindruck erweckt, dass allen Anforderungen an die Informationssicherheit allein durch Verwendung eines solchen Basisdienstes Genüge getan ist. Daher wäre die folgende alternative Formulierung zu bevorzugen:

> ***„4. um bestimmte Sicherheitsmaßnahmen erweiterte Dienste zur Kommunikation sowie zum Nachrichtentransport zwischen den Verfahrensbeteiligten sowie anderen Nutzerinnen und Nutzern von Verwaltungsleistungen und der Verwaltung, die die Funktionalitäten Signaturprüfung, Ver- und Entschlüsselung, zentrale Authentifizierung, Zeitstempeldienst, Postein- und -ausgangsbücher sowie Virenprüfung umfasst“.***

[1] https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf

II. Zu Artikel 5 – Informationszugangsgesetz

Die vorgeschlagenen Anpassungen des Informationszugangsgesetzes enthalten die mit der Novellierung des Landesdatenschutzgesetzes notwendig gewordenen Regelungen in Bezug auf die Aufgaben und Befugnisse einer oder eines Landesbeauftragten für Informationszugang und stellen bereits eine gute Grundlage dar. Einige meiner Anregungen wurden bereits während der Erarbeitung des vorgelegten Entwurfs aufgegriffen. Darüber hinaus rege ich die folgenden Überarbeitungen an, die der **Praxistauglichkeit und Rechtsklarheit** dienen und in mehreren Punkten dem **guten Beispiel des HmbTG** folgen:

a) Kommunikation mit informationspflichtiger Stelle und Aufsichtsbehörde

Gemäß § 14 Abs. 5 Satz 2 und 3 *„soll die oder der Landesbeauftragte für Informationszugang zuvor die informationspflichtige Stelle zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auffordern. Vor der Beanstandung ist auch der zuständigen Rechts-, Dienst- oder Fachaufsichtsbehörde Gelegenheit zur Stellungnahme zu geben“* (Drs. 19/3267, S.42). Bei der Bestimmung ist zunächst auffällig, dass bezüglich der jeweiligen Aufsichtsbehörde eine Verpflichtung besteht, eine Gelegenheit zur Stellungnahme einzuräumen, wogegen gegenüber der informationspflichtigen Stelle lediglich eine Soll-Vorgabe besteht. Bereits diese Unterscheidung erscheint **nicht praxisgerecht**, da informationspflichtigen Stelle in den Prüfverfahren **stets angehört** werden. Die **Anhörung der Aufsichtsbehörde vor einer Beanstandung ist in keinem anderen Informationsfreiheits- bzw. Transparenzgesetz der Länder** enthalten und würde auch einen **hohen Bürokratieaufwand** erzeugen. Zusätzlich führte dies zur **zeitlichen Verlängerung** der Prüfverfahren, sodass Antragstellerinnen und Antragsteller länger auf ein Ergebnis der oder des Landesbeauftragten für Informationszugang warten müssten. Schließlich handelt es sich bei den Beanstandungen nicht um Verwaltungsakte, wodurch der Eingriffscharakter der Maßnahme gering ist und eine Vorabbeteiligung der Rechts-, Dienst- oder Fachaufsichtsbehörde nicht gerechtfertigt wäre. Daher wird anstelle von § 14 Abs. 5 Satz 2 und 3 in Anlehnung an § 14 Abs. 5 Satz 3 HmbTG folgende Formulierung vorgeschlagen:

> ***„Sie oder er soll zuvor die informationspflichtige Stelle zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auffordern und die zuständige Rechts-, Dienst- oder Fachaufsichtsbehörde über die Beanstandung unterrichten.“***

b) Weiterleitung einer Kopie der Beanstandung

Nach § 14 Abs. 5 Satz 8 *„finden Satz 5 bis 7 nur Anwendung, soweit Ablehnungsgründe nach den §§ 9 und 10 nicht entgegenstehen“* (Drs. 19/3267, S.43). Eine entsprechende Bestimmung findet sich wiederum **in keinem anderen Informationsfreiheits- bzw. Transparenzgesetz** der Länder. Es wird dabei auch nicht aus der Gesetzesbegründung deutlich, in welcher Konstellation eine einschränkende Informationsweitergabe erfolgen soll. Es besteht vielmehr die **Gefahr, dass hierdurch eine Rechtsunsicherheit erzeugt** wird, da ggf. maßgebliche Teile einer Beanstandung nicht an die genannten Beteiligten gegeben werden, obwohl gerade die Aufgabe besteht, betroffene Antragstellerinnen und Antragsteller in ihren Informationsbegehren zu unterstützen und die jeweilige Aufsichtsbehörde angemessen zu informieren.

> **Satz 8 sollte daher gestrichen werden.**

c) Klagerecht

Nach § 14 Abs. 6 HmbTG wird für den **Fall des nicht fristgerechten Behebens festgestellter Mängel ein Klagerecht** des bzw. der Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit geregelt. Es wird angeregt, für die oder den Landesbeauftragte(n) für Informationszugang eine **vergleichbare Bestimmung** aufzunehmen. Im Rahmen bedeutsamer Prüfverfahren besteht dann die Möglichkeit, ein Prüfergebnis gerichtlich beurteilen zulassen. Dies kann etwa von Bedeutung sein bei Rechtsfragen, die eine Vielzahl von Fällen betreffen. Die vorgeschlagene Formulierung erscheint **sachgerecht und folgt dem Vorbild** des HmbTG:

> ***„Werden die Mängel nicht fristgerecht behoben, kann die oder der Landesbeauftragte für Informationszugang das Vorliegen der beanstandeten Verstöße gegen dieses Gesetz gerichtlich feststellen lassen."***

III. Zu Artikel 10 – Offene-Daten-Gesetz

Qualitätssicherung in Bezug auf etwaige Datenschutzrisiken

Die Aufgabe der *„Qualitätssicherung"* des Open-Data-Portals obliegt nach § 4 Abs. 4 der Open-Data-Leitstelle (Drs. 19/3267, S. 50); für die bereitgestellten Daten sind die jeweiligen Träger der öffentlichen Verwaltung verantwortlich. In der Begründung zu § 5 Abs. 5 wird zur Beschränkung der Qualitätssicherung durch die Träger der öffentlichen Verwaltung ausgeführt, dass diese *„die bereitgestellten Daten nicht über das zur Erfüllung ihres gesetzlichen Auftrags erforderliche Maß hinaus auf Richtigkeit, Vollständigkeit, Plausibilität oder in sonstiger Weise prüfen"* müssen (Drs. 19/3267, S.134). Das ist auch nachvollziehbar. Für den Fall, dass *„Fehler in Daten oder Datensammlungen identifiziert werden"* (Drs. 19/3267, S. 134), ist die Möglichkeit einer Korrektur vor der erstmaligen Bereitstellung der Daten vorgesehen.

Aus Sicht der Landesbeauftragten für Datenschutz stellt sich die Frage, wie im Falle eines durch einen Fehler entstehenden Risikos für die Rechte und Freiheiten natürlicher Personen – weil versehentlich personenbezogene Daten einer Behörde bereitgestellt wurden oder weil etwa ein Personenbezug durch Verknüpfung mehrerer bereitgestellter Datensammlungen verschiedener Behörden offenbar wird – dieses Risiko möglichst schnell eingedämmt werden kann. Laut Aussage aus dem Ministerium wurde inzwischen auf meine Anregung hin eine zentrale E-Mail-Adresse hierfür eingerichtet; es soll der Verordnungstext entsprechend angepasst werden. Dies ist zu begrüßen. Aber auch hier ist eine **Klarstellung geboten**, **dass die Qualitätssicherung für das Open-Data-Portal auch eine Reaktion auf mitgeteilte Verletzungen des Schutzes personenbezogener Daten** (z. B. umgehende Sperrung der betroffenen Daten) oder zusätzlich eine Prüfpflicht in Bezug auf Risiken, die erst in der Gesamtschau feststellbar sind, **umfasst**. Ich schlage daher folgende Ergänzung der Aufzählung in § 4 Abs. 4 S. 1 (Drs. 19/3267, S. 50) vor (siehe Unterstreichung):

> ***„Die Aufgaben der Open-Data-Leitstelle umfassen die Sicherstellung des Betriebs, <u>umgehende Bearbeitung von Beschwerden, regelmäßige Überprüfung auf Datenschutzrisiken,</u> die Weiterentwicklung und die Qualitätssicherung des Open-Data-Portals, Festlegung von technischen Standards sowie die allgemeine Förderung des Gesetzeszweckes."***

Die jetzige Formulierung des Entwurfs könnten alle Beteiligten für sich so interpretieren, dass sie nicht verantwortlich seien; eine angemessene zeitnahe Behandlung und Eindämmung eines etwaigen Risikos wäre damit nicht gewährleistet.

IV. Zu Artikel 12 – IT-Einsatz-Gesetz

a) Grundsatz der Überprüfbarkeit und Nachvollziehbarkeit

Wegen der besonderen Bedeutung sollte der aus den in § 9 Abs. 1 Buchst. b genannten „Methoden zur Überprüfung und Nachvollziehbarkeit der Entscheidungsprozesse“ (Drs. 19/3267, S. 60) ableitbare **Grundsatz der *„Überprüfbarkeit und Nachvollziehbarkeit“*** schon in den **Grundsätzen der Zulässigkeit des Einsatzes von datengetriebenen Informationstechnologien,** also bereits in § 2 Abs. 1 (Drs. 19/3267, S. *54), genannt werden. Dies könnte entweder direkt in § 2 Abs. 1 formuliert oder schon in dem referenzierten § 1 Abs. 2 (Drs. 19/3267, S. *53) erfolgen.

Im Falle von Verfahren, die personenbezogene Daten verarbeiten, kommen weitere Grundsätze hinzu, insbesondere die Datenschutzgrundsätze aus Art. 5 DSGVO. Es wird angeregt, in der Begründung des Gesetzes **auf die in der DSGVO normierten Datenschutzgrundsätze hinzuweisen,** um den **Rechtsanwendern Hilfestellung zu geben**. Zumindest in der Begründung sollte darauf verwiesen werden.

b) Unzulässigkeit von Verhaltens- und Leistungskontrolle bei Maßnahmen der Datensicherheit

In § 2 Abs. 2 wird in abschließender Form aufgezeigt, für welche Bereiche von sich selbstständig weiterentwickelnden, datenbasierten Informationstechnologien ein Einsatz nicht zulässig sein soll. In § 2 Abs. 2 Nr. 2 wird etwa die Arbeitsleistung erwähnt. Dabei fehlt eine Verzahnung mit § 15 Abs. 2 LDSG, wonach generell für Zwecke der Verhaltens- oder Leistungskontrolle keine Auswertungen erfolgen dürfen. Da die Aufzählung in § 2 Abs. 2 Nr. 2 nur eine Teilmenge der Maßnahmen zur Verhaltens- oder Leistungskontrolle bildet, wird gebeten, zur **Vermeidung von Wertungswidersprüchen eine Ergänzung aufzunehmen**, sodass sich folgende Formulierung ergibt:

> ***„bei der Verarbeitung personenbezogener Daten zu Zwecken der Verhaltens- oder Leistungskontrolle, wie etwa zum Zweck der Beurteilungen der Persönlichkeit, der Arbeitsleistung, der physischen und psychischen Belastbarkeit, der kognitiven oder emotionalen Fähigkeiten von Menschen, der Erstellung von Prognosen über die Straffälligkeit einzelner Personen oder Personengruppen“***

c) Unzulässigkeit einer massenweisen Identifikation von Personen

In § 2 Abs. 2 Nr. 3 wird ein Einsatz *„zur massenweisen Identifikation von Personen bei Versammlungen oder Veranstaltungen anhand von biometrischen Merkmalen“* (Drs. 19/3267, S. 54) untersagt. Diese Formulierung erscheint zu eng. Nach meiner Auffassung sollte **nicht nur bei Versammlungen oder Veranstaltungen und nicht nur auf Basis von biometrischen Merkmalen der Anwendungsbereich einer – sehr eingriffsintensiven – massenhaften Identifikation von Personen beim Einsatz von datengetriebenen Informationstechnologien unzulässig** sein. Wenn dies vom Gesetzgeber in einer solchen weiteren Bedeutung gemeint ist, wäre eine mögliche Formulierung:

„3. zur massenweisen Identifikation von Personen, z. B. anhand von biometrischen Merkmalen, und“

Die Beispiele, die in der Begründung (Drs. 19/3267, S.142) gegeben werden, z. B. betreffend des öffentlichen Raumes und der Mustererkennung anhand der Bewegungen einer Menschenmenge, stützen dies. Diese Beispiele wären nämlich mit der Formulierung des Entwurfs nicht unbedingt unzulässig, da diese gerade nicht auf eine massenweise Identifikation von Personen abzielen. Nach der hier vorgeschlagenen Formulierung wären allerdings massenweise Identifikationen von Fußgängerinnen und Fußgängern – beispielsweise mit Verknüpfung zu den Geokoordination ihrer Wohnungen oder mit Analyse ihrer Begleiterinnen oder Begleiter – auf Basis von MAC-Adressen oder anderen Kennungen mitgeführter Endgeräte – also nicht anhand biometrischer Merkmale – unzulässig (wie es wohl auch gemeint ist).

In diesem Zusammenhang sei auf das Rechtsetzungsverfahren COM(2021) 206 final („*Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz)und zur Änderung bestimmter Rechtsakte der Union“*[2]) der EU hingewiesen, das Überschneidungen mit dem hiesigen Regelungsgegenstand hat: In Artikel 5 Absatz 1 Buchstabe d dieses Vorschlags wird „*die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken“* **grundsätzlich untersagt;** es werden nur enge Ausnahmeregelungen geschaffen (Artikel 5 Absatz 1 Buchstabe d Nrn. (i)-(iii) und Artikel 2 ff.).

d) Wahrung der Betroffenenrechte der DSGVO bzw. des LDSG

Bei der Verwendung von personenbezogenen Daten als Trainingsdaten sind weiterhin die Rechte der betroffenen Personen, insbesondere gemäß den Abschnitten 2, 3 und 4 der DSGVO, zu beachten. Da dieser Aspekt in der Praxis leicht übersehen werden kann, ist es sinnvoll, zentrale Vorgaben für die Umsetzung der Dokumentations- und Informationspflichten machen zu können. Insbesondere bei zentral bereitgestellten Verfahren sollte diese Möglichkeit eröffnen werden, beispielsweise in der Verordnungsermächtigung in § 11 (Drs. 19/3267, S. 61 f.) durch eine **Regelungskompetenz zum Datenschutz**. Als neu einzufügender Punkt 2 wird vorgeschlagen:

„2. Umsetzung der Betroffenenrechte nach Kapitel III (Artikel 12 bis 22) der Datenschutz-Grundverordnung “

Die bisherigen Punkte 2. bis 6. würden zu 3. bis 7. Dieser Vorschlag steht auch im Einklang mit dem Ziel, verbindliche Mindeststandards fürden Einsatz von datengetriebenen Informationstechnologien durch Verordnung festzulegen.

e) Bezug zu Artikel 22 DSGVO

Der Einsatz von sich selbstständig weiterentwickelnden, datenbasierten Informationstechnologien steht im Kontext mit automatisierten Entscheidungen im Einzelfall einschließlich Profiling nach Art. 22 DSGVO. Der Entwurf zum IT-Einsatz-Gesetz berücksichtigt nach vorliegendem Verständnis die Vorgaben nach Art. 22 Abs. 2 Buchst. b DSGVO, indem angemessene Maßnahmen insbesondere durch die Transparenz hinsichtlich des Algorithmus, der Möglichkeit einer IT-Rüge und der Gewährleistung einer menschlichen Aufsicht umgesetzt werden sollen.

[2] Dokument 52021PC0206, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:52021PC0206

Die Beachtung von Art. 22 Abs. 2 Buchst. b DSGVO wird allerdings an keiner Stelle des Entwurfs erwähnt. Da auch hier die Gefahr besteht, diesen Zusammenhang zu übersehen, sollte zumindest **in der Gesetzesbegründung hierauf Bezug genommen werden.**

Für Nachfragen stehen mein Team und ich gerne zur Verfügung.

Mit freundlichen Grüßen

gez. Marit Hansen
Landesbeauftragte für Datenschutz