Der Landesbeauftragte für Datenschutz und Informationsfreiheit M-V
Lennéstraße 1, Schloss · 19053 Schwerin

AKTENZEICHEN
1.4.1.008/012/2019-02794

Ministerium für Inneres und Europa
Mecklenburg-Vorpommern
19048 Schwerin

Telefon: 0385 59494-49
E-Mail: [redacted]

Per E-Mail:
[redacted]

6. März 2019

Entwurf für ein Gesetz zur Änderung des Sicherheits- und Ordnungsgesetzes und weiterer Gesetze

Sehr geehrte Frau [redacted],

wir danken Ihnen für die erneute Gelegenheit zur Stellungnahme zu dem Gesetz zur Änderung des Sicherheits- und Ordnungsgesetzes und weiterer Gesetze im Rahmen der Verbandsanhörung. Insbesondere freuen wir uns über die erstellte Synopse, die die beabsichtigten Änderungen gut nachvollziehbar macht. Festzustellen ist, dass dieser Gesetzentwurf nur sehr wenige unserer im Rahmen der Ressortanhörung geäußerten Kritikpunkte aufgreift und sich auch sonst nicht wesentlich von der im Rahmen der Ressortanhörung bekannten Vorlage dieses Gesetzentwurfs unterscheidet. Daher wiederholen wir viele unserer Ihnen gegenüber bereits geäußerten Kritikpunkte und ergänzen unsere Bedenken insbesondere zu § 43a SOG-E und zu unseren Befugnissen als Aufsichtsbehörde (§ 48b SOG-E).

Allgemeine Hinweise zu diesem Gesetzentwurf

Das in der Gesetzesbegründung erklärte Ziel des Gesetzentwurfes, den „Gesetzesanwendern weitestgehend ein ständiges „Hineinspringen“ in verschiedene datenschutzrechtliche Regelungswerke“ zu ersparen „und so die bessere praktische Handhabung“ zu gewährleisten, ist positiv herauszustellen. Der LfDI M-V unterstützt dieses Ziel, auch um, wie weiter in der Gesetzesbegründung ausgeführt, „eine möglichst einheitliche Verfahrensweise bei Polizei und Ordnungsbehörden im Land Mecklenburg-Vorpommern mit Blick auf die notwendige Zusammenarbeit im Bereich der Gefahrenabwehr“ sicherzustellen. Nicht zuletzt soll und muss dieses Gesetz aufgrund der Eingriffsintensität der geregelten Maßnahmen nicht nur den Rechtsanwendern absolute Rechtsklarheit verschaffen, sondern auch die betroffenen Bürgerinnen und Bürger in die Lage versetzen, die Rechtmäßigkeit der gegen sie ergriffenen Maßnahmen einzuschätzen. Es steht für den LfDI M-V vor diesem Hintergrund außer Frage, dass dieses Gesetz vor allem leicht verständliche, klare und präzise Regelungen enthalten muss.

Leider müssen wir aber auch konstatieren, dass der Gesetzentwurf diesen Anforderungen bisher nicht gerecht wird. Der SOG-E macht es den Anwendern kaum möglich, rechtsfehlerfrei ihre Aufgaben zu erfüllen. Bei dieser im Nachfolgenden noch präzisierten Kritik geht es daher weder um Formalien oder „Schönheitsfehler“ noch um die zuweilen „akademisch“ anmutende Frage, wann eine Regelung gegen das europarechtliche Wiederholungsverbot verstößt. Bei einem eingriffsintensiven Gesetz wie dem SOG ist es schlicht ein Gebot der Rechtstaatlichkeit, dass das Gesetz möglichst gut verständlich, lesbar und anwenderfreundlich ist.

Bei der nachfolgenden Kritik ist uns bewusst, dass das Gesetzgebungsvorhaben durch eine denkbar schlechte Ausgangslage erschwert wird. So gibt es in Mecklenburg-Vorpommern einerseits kein „Polizei- und Ordnungsbehördengesetz“, dessen Regelungen hier zur Vereinfachung hätten beitragen können. Zudem ist in Mecklenburg-Vorpommern die Richtlinie (EU) 2016/680 (JI-Ri) bisher nicht bzw. nur sehr rudimentär mit § 3 DSG M-V in innerstaatliches Recht umgesetzt worden. Diese Versäumnisse oder bewussten Entscheidungen der Vergangenheit dürfen jedoch nicht zu Lasten der Bürgerinnen und Bürger gehen, die von diesem Gesetz betroffen sind.

Die Hauptursache für die nachfolgende Kritik ist unseres Erachtens aber darin zu sehen, dass mit dem SOG-E versucht wurde, dem Anwender auch bei Verarbeitungen im Anwendungsbereich der DS-GVO den Blick in die DS-GVO selbst zu ersparen. Dieser Versuch kann nur scheitern: Um das Schutzniveau der DS-GVO zu wahren hätten deren Regelungen vollständig im SOG-E aufgenommen werden müssen, was wiederum europarechtlich kaum zulässig ist. Wir plädieren nach wie vor dafür, im SOG-E, wie bereits in § 3 DSG M-V geschehen, die DS-GVO auch im Anwendungsbereich der JI-Ri für anwendbar zu erklären und im SOG-E lediglich die Verarbeitungsbefugnisse zu regeln sowie – soweit erforderlich – Betroffenenrechte einzuschränken. In dieser Variante müsste der Anwender nach wie vor die DS-GVO zusätzlich zum SOG heranziehen. Der vorliegende SOG-E kann das aber ebenfalls nicht vermeiden, indem er vielfach, allerdings auch nicht abschließend und ohne erkennbares System, auf die DS-GVO verweist. In der Praxis führt der SOG-E vielmehr dazu, dass der Anwender und die betroffenen Bürgerinnen und Bürger überhaupt nicht mehr entscheiden können, wann welche Regelungen der DS-GVO anzuwenden sind.

Die nachfolgende Stellungnahme ist in zwei Teile untergliedert. Im ersten Teil werden die von uns als besonders kritisch erachteten Mängel des Entwurfs zusammengefasst dargestellt, im zweiten Teil der Stellungnahme gehen wir konkret auf die jeweiligen Regelungen ein.

Teil 1 – Zusammenfassung der Kritikpunkte

Bei der vorläufigen Bewertung des Gesetzesentwurfs ist insbesondere darauf hinzuweisen, dass der SOG-E auf Kosten von Lesbarkeit und Verständlichkeit nicht den Standards moderner Gesetzgebung genügt (a). Die fehlende Differenzierung zwischen den erforderlichen Anpassungen des SOG an die DS-GVO und der notwendigen Umsetzung der JI-Ri wirkt sich ebenso negativ auf die Lesbarkeit und Verständlichkeit des Gesetzentwurfs aus (b). Zudem setzt der SOG-E die JI-Ri nur unvollständig um (c). Mit Blick auf das Urteil des Bundesverfassungsgerichts vom 18. Dezember 2018 zur automatisierten Kraftfahrzeugkennzeichenkontrolle lässt sich auch die Regelung in § 43 a Abs. 1 Nr. 6 SOG-E nicht mehr halten (d). Auch sind die Befugnisse der Datenschutzaufsichtsbehörde entgegen der ausdrücklichen Vorgabe in der JI-Ri stark eingeschränkt (e). Im Anwendungsbereich der DS-GVO sind Betroffenenrechte unzulässig eingeschränkt (f). Zudem fehlt es hier an notwendigen Anpassungen an die DS-GVO (g).

a) Standards moderner Gesetzgebung

Der SOG-E genügt nicht den Anforderungen moderner Gesetzgebung.

Der SOG-E enthält zunächst keinen Anwendungsbereich. Wann das SOG gelten soll, ergibt sich nach wie vor nur aus einer Gesamtschau von Aufgaben und Zuständigkeiten. Erschwerend kommt hinzu, dass damit weder der Anwendungsbereich der JI-Ri noch der der DS-GVO im SOG-E selbst definiert werden, in den einzelnen Regelungen des SOG-E ausgehend von dem jeweiligen Anwendungsbereich aber unterschiedliche Anforderungen an die Datenverarbeitung gestellt werden. Einige Regelungen sollen die auf die „Verarbeitung zu Zwecken der Richtlinie (EU) 2016/680 personenbezogener Daten“ (vgl. §§ 45 c, 48 b, 48 c, 76 SOG-E) beschränkt sein. Innerhalb eines Paragraphen werden teilweise unterschiedliche Regelungen für den „Anwendungsbereich der Richtlinie (EU) 2016/680“ und den „Anwendungsbereich der Verordnung (EU) 2016/679“ getroffen. Die datenschutzrechtlich besonders sensiblen Übermittlungsbefugnisse in Drittstaaten der §§ 39 d ff. SOG-E sind auf den Anwendungbereich der Richtlinie (EU) 2016/680 beschränkt. Der Rechtsanwender kann aber allein aus dem SOG-E gar nicht herleiten, welche der von ihm vorgenommenen Verarbeitungen in den Anwendungsbereich der JI-Ri oder aber in den der DS-GVO fallen. Hinzu kommt, dass der SOG-E mit der komplizierten und aus unserer Sicht überflüssigen Regelung in § 25 SOG-E den Eindruck erweckt, in der Regel wäre der Anwendungsbereich der DS-GVO eröffnet, während die Gesetzesbegründung davon ausgeht, dass regelmäßig der Anwendungsbereich der JI-Ri greift und die DS-GVO ohnehin nur in Ausnahmefällen anzuwenden ist.

Zudem machen viele Verweise und Verweisketten das Gesetz unleserlich und schwer handhabbar.

Die Gliederung des SOG-E ist unübersichtlich und für den Anwender teilweise nicht nachvollziehbar. Regelungen von zentraler Bedeutung („Kernbereich privater Lebensgestaltung“, „Schutz von zeugnisverweigerungsberechtigten Personen“) werden entweder vor die Klammer gezogen oder als allgemeine Pflichten des Verantwortlichen ausgestaltet (z. Bsp. „Löschung“). Bei der konkreten Befugnisnorm wird, entgegen der aktuellen Regelungen im SOG M-V, teilweise nicht mehr darauf verwiesen. Aber auch hier ist wiederum kein System erkennbar, warum bei einigen Regelungen verwiesen wird und bei anderen wiederum nicht. Beim Anwender wird so der Eindruck erzeugt, dass die vor die Klammer gezogenen Regelungen nicht immer zu beachten sind, sondern nur dann, wenn der Regelungstext ausdrücklich darauf verweist. Zur Vermeidung rechtswidriger Datenverarbeitungen und vor dem Hintergrund der Eingriffsintensität des Gesetzes plädieren wir unbedingt dafür, die umfangreichere normspezifische Ausgestaltung der Befugnisnormen beizubehalten oder zumindest konsequent bei den Befugnisnormen auf die Regelungen zu verweisen, die beachtet werden müssen.
Ebenso verwirrend sind die Begriffsbestimmungen am Anfang des Gesetzes. Mangels einer Regelung zum Anwendungsbereich bleibt so unklar, ob die Begriffsbestimmungen auch im Anwendungsbereich der DS-GVO gelten sollen. Nach der Gesetzesbegründung ist das zwar gewollt, eine entsprechende Regelung enthält aber erst § 25 SOG-E. Damit wird jedenfalls der Eindruck erzeugt, dass erst die §§ 25 ff. SOG-E auch im Anwendungsbereich der DS-GVO gelten sollen.
Hinzu kommt, dass Paragraphen mit Buchstaben über Unterabschnitte hinweg weitergeführt werden. So regeln beispielsweise die §§ 47 - 48 a SOG-E die Rechte der betroffenen Person. § 48 b SOG-E regelt in einem neuen Unterabschnitt die Befugnisse der Aufsichtsbehörde. Auch das trägt wenig dazu bei, dass Anwender die Normen verinnerlichen und logisch nachvollziehen können, wo im Gesetz eine relevante Regelung zu finden ist.

An vielen Stellen ist der SOG-E auch aufgrund des Satzbaus kaum lesbar. Zudem erstrecken sich die unterschiedlichen Paragraphen über ungewöhnlich viele Absätze. § 25 SOG-E ist als besonders eindrucksvolles Beispiel hervorzuheben.

Die Rechtsklarheit und Anwenderfreundlichkeit des SOG-E werden weiterhin durch fehlerhafte oder fehlende Begriffsbestimmungen reduziert. Es werden Begriffe von zentraler Bedeutung nicht definiert (z. Bsp. „Kernbereich privater Lebensgestaltung“, „Bildaufnahme“, „Bildaufzeichnung“). Für den Begriff des „Dritten“ werden hingegen gleich zwei Definitionen angeboten und mit einem „oder“ verbunden. Der Anwender muss sich ohne weitere Hilfestellung im Gesetz für eine Definition entscheiden.

b) Fehlende Differenzierung zwischen der Umsetzung der JI-Ri und der Anpassung an die DS-GVO

Der Versuch, mit dem Entwurf im Sinne der Anwenderfreundlichkeit auch Regelungen für Sachverhalte zu schaffen, die von der DS-GVO erfasst sind, wird bereits im SOG-E nicht konsequent beibehalten.
Ohne erkennbares System wird im SOG-E die DS-GVO teilweise für anwendbar erklärt oder gar darauf verwiesen. Der nicht DS-GVO-versierte Anwender wie auch die betroffenen Personen werden damit darüber im Unklaren gelassen, dass die DS-GVO aufgrund ihres europarechtlichen Anwendungsvorrangs immer gilt und nicht nur dann, wenn eine Regelung im SOG-E ausdrücklich darauf verweist.
Durch die schwer verständliche Regelung in § 25 SOG-E wird bei Rechtsanwendern und betroffenen Personen zudem der Eindruck verstärkt, die in § 25 SOG-E genannten Regelungen der DS-GVO würden vollständig durch die Regelungen im SOG-E ersetzt.

c) Umsetzung der JI-Ri

Die Regelungen der JI-Ri sind in innerstaatliches Recht umzusetzen. Im SOG-E gelingt dies jedoch nur teilweise. So ist beispielsweise die Umsetzung von Art. 4 JI-Ri, der wie Art. 5 DS-GVO elementare Datenschutzgrundsätze regelt, nicht erfolgt. Ebenso fehlt es an der Umsetzung von Art. 11 JI-Ri, der verlangt, dass betroffene Personen nicht zum Objekt automatisierter Entscheidungsfindung degradiert werden dürfen. Der SOG-E enthält mit § 25 a Abs. 6 lediglich eine unzureichende Einschränkung für Kinder. Weiterhin sind entgegen Art. 12 JI-Ri die Modalitäten der Bearbeitung von geltend gemachten Betroffenenrechten nicht näher ausgestaltet. Die Befugnisse der Datenschutzaufsichtsbehörde im SOG-E bleiben schließlich weit hinter den Anforderungen von Art. 47 JI-Ri zurück und gewährleisten entgegen Art. 46 Abs. 1 lit. a JI-Ri nicht, dass die Datenschutzaufsichtsbehörde die Anwendung der nach der JI-Ri erlassenen Vorschriften auch durchsetzen kann.

d) Nichtbeachtung der Vorgaben des Bundesverfassungsgerichts

Nach der Entscheidung des Bundesverfassungsgerichts vom 18. Dezember 2018 (1 BvR 142/15) zur automatisierten Kraftfahrzeugkennzeichenkontrolle ist diese verfassungsrechtlich unbedenklich, „soweit die Kennzeichenkontrolle in einem Grenzgebiet bis zu einer Tiefe von 30 km oder an öffentlichen Einrichtungen des internationalen Verkehrs durchgeführt wird“ (Pressemitteilung Nr. 8/2019 vom 5. Februar 2019). Diesen Anforderungen genügt die Regelung des § 43 a Abs. 1 Ziffer 6 SOG-E nicht. Diese Vorschrift bestimmt, dass Kennzeichenkontrollen im Grenzgebiet „von der Bundesgrenze bis einschließlich der Bundesautobahn A 20“ zulässig sein sollen.

e) Einschränkung von Betroffenenrechten im Anwendungsbereich der DS-GVO

Die vorgenommenen Einschränkungen der Betroffenenrechte im Anwendungsbereich der DS-GVO genügen nicht den Anforderungen von Art. 23 DS-GVO.

Der EuGH hat in ständiger Rechtsprechung, u. a. in der Entscheidung zu Safe-Harbor, klare Anforderungen an Unionsregelungen aufgestellt, die, wie in den **§§ 25 ff. des Entwurfs beabsichtigt, einen Eingriff in die von Art. 7 und 8 GrCh geschützten Grundrechte der** betroffenen Person darstellen:

1. Die Regelung muss klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und ausreichende Garantien zum Schutz der Daten vor Missbrauch enthalten.
2. Die Mitgliedstaaten können Beschränkungen der Rechte der betroffenen Person nur in dem Umfang vorsehen, wie sie zur Wahrung der genannten Zwecke notwendig sind. Eine Notwendigkeit muss konkret für den Einzelfall bestimmt werden.
3. Darüber hinaus verlangt der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene vor allem, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken.

Daraus ergibt sich, dass pauschale Ausnahmen für bestimmte Organe oder Aufgaben unzulässig sind. Ein Eingriff muss stets verhältnismäßig sein. In diesem Sinne genügt es nicht, dass die Gesetzesbegründung dem Verantwortlichen aufgibt, stets zu prüfen, in welchem Umfang und für welche Dauer eine Gefährdung vorliegt, wenn das Gesetz selbst auf Tatbestandsebene nicht einmal mehr an eine Gefährdung anknüpft. Die Norm selbst muss bereits nach Art. 23 Abs. 1 DS-GVO eine verhältnismäßige und in einer demokratischen Gesellschaft notwendige Maßnahme darstellen.
Das setzt weiterhin voraus, dass die Normen die gemäß Art. 23 DS-GVO bestimmten Mindestinhalte aufweisen. So müssen Art und Umfang der Verarbeitung benannt werden, Garantien gegen Missbrauch aufgenommen und Speicherfristen festgelegt werden. Darüber hinaus muss eine Risikobewertung für die Rechte und Freiheiten der betroffenen Person enthalten sein. Diese Inhalte sind zwingend in die Norm, die das Betroffenenrecht einschränkt, aufzunehmen. Das Wort „gegebenenfalls“ in Art. 23 Abs. 2 DS-GVO erlaubt lediglich eine Abwägung, ob die einzelne Festlegung mit dem jeweiligen Zweck vereinbar ist, keinesfalls jedoch einen pauschalen Verzicht.

f) Fehlende Regelungen bei der Anpassung an die DS-GVO

Schließlich fehlen notwendige Regelungen, um das SOG an die DS-GVO anzupassen. Bedeutsam ist hier insbesondere, dass mit dem SOG-E gerade keine Befugnis geschaffen wird, im Anwendungsbereich der DS-GVO auch besondere Kategorien personenbezogener Daten zu verarbeiten. Der SOG-E schafft diese Befugnis nicht für Datenverarbeitungsvorgänge im Anwendungsbereich der DS-GVO, da § 27 SOG-E an die *„Abwehr der Gefahr für die öffentliche Sicherheit“* und damit an die Gefahrenabwehr im Anwendungsbereich der JI-Ri anknüpft.

Teil 2 - Konkrete Hinweise

Zu § 3 SOG-E (Begriffsbestimmungen):

a) § 3 Absatz 4 SOG-E:

Die Regelung in Absatz 4 zum „Dritten“ ist unzulässig, eine Begriffsbestimmung muss eine eindeutige Definition enthalten. Hier hätte eine Ergänzung, wie beispielsweise der „Dritte im datenschutzrechtlichen Sinn“ und der „Dritte im ordnungsrechtlichen Sinn“ zur Rechtsklarheit beigetragen. Zudem verstößt die Regelung gegen das Wiederholungsverbot. Im Anwendungsbereich der DS-GVO ist eine Wiederholung nur dann zulässig, wenn eine Spezifizierungsklausel den nationalen Gesetzgeber ermächtigt, eine Regelung der DS-GVO zu konkretisieren und diese Wiederholung der Verständlichkeit und kohärenten Anwendung dient. Vorliegend fehlt es bereits an einer Spezifizierungsklausel. Zudem führt die Wiederholung lediglich zur Verwirrung, da in § 3 Abs. 4 SOG-E nunmehr zwei unterschiedliche Definitionen des Dritten, die mit einem „oder“ verbunden werden, enthalten sind.

b) § 3 Absatz 5 SOG-E:

Die Definition besonderer Kategorien personenbezogener Daten in Buchstabe c) ist zu unbestimmt und führt zu Rechtsunsicherheit. Es bleibt völlig unklar, was unter „speziellen technischen Verfahren“ zu verstehen ist. Lichtbilder zählen dann zu den besonderen Kategorien personenbezogener Daten, wenn sie dem Zweck der eindeutigen Identifizierung der betroffenen Person dienen (vgl. Art. 9 Abs. 1 DS-GVO, Art. 10 JI-Ri). Es kommt daher nicht nur auf die konkrete Verwendung, sondern auch auf die Verwendungsabsicht an. Insoweit sollte der Zusatz zu den Lichtbildern gestrichen werden. Zudem fehlt es auch hier an einer Spezifizierungsklausel, um die Definition im Anwendungsbereich der DS-GVO überhaupt zu wiederholen.

Zu § 25 SOG-E (Bestimmungen zur Anwendbarkeit der Vorschriften dieses Gesetzes im Anwendungsbereich der Verordnung (EU) 2016/679):

Es wurde bereits ausgeführt, dass diese Regelung aus unserer Sicht überflüssig, unleserlich und schwer verständlich ist. Zwar ist die Vorschrift im Gegensatz zum Vorentwurf in Absatz 2 zur Verbesserung der Verständlichkeit umgestellt worden. Allerdings bleibt die Unsicherheit beim Anwender bestehen, ob die in § 25 SOG-E genannten Artikel der DS-GVO noch unmittelbar anwendbar sind oder durch den SOG-E verdrängt werden sollen. Europarechtlich besteht indes kein Zweifel, dass die vermeintlich im SOG-E „konkretisierten“ Regelungen ihre unmittelbare Geltung behalten.
Zudem genügt die Einschränkung von Betroffenenrechten in § 25 Abs. 2 S. 2 SOG-E nicht den Anforderungen von Art. 23 DS-GVO.

Zu den §§ 26 a (Schutz des Kernbereiches privater Lebensgestaltung), 26 b (Schutz von zeugnisverweigerungsberechtigten Personen) SOG-E:

Die Schaffung solcher, vor die Klammer gezogenen Normen, auf die erschwerend ohne erkennbares System teilweise verwiesen wird, führt zu erheblicher Rechtsunklarheit. Wir plädieren dafür, wie bisher, den Kernbereichsschutz normspezifisch zu regeln oder jedenfalls konsequent auf § 26 a SOG-E zu verweisen. Bei den Anwendern darf nicht der Eindruck entstehen, der Kernbereichsschutz bestünde nur im Zusammenhang mit den Normen im SOG-E, die ausdrücklich darauf verweisen. Gleiches gilt für die Reglung zum Schutz von zeugnisverweigerungsberechtigten Personen in § 26b SOG-E.

Zu 31 a SOG-E (Molekulargenetische Untersuchung zur Identitätsfeststellung):

In § 31a **Absatz 1** wurde die bisher in Absatz 1 enthaltene Regelung, dass die zum Zweck des Abgleichs in einem Dateisystem gespeicherten DNA-Identifizierungsmuster zu löschen sind, wenn sie zur Identitätsfeststellung nicht mehr benötigt werden, gestrichen. Dies könne mit Blick auf § 45 Absatz 2 Satz 1 Nummer 4 erfolgen. Dem stimmen wir nicht zu.
Bei DNA- Identifizierungsmustern handelt es sich um genetische Daten i. S. d. Art. 3 Nr. 12 JI-Richtlinie, die als besondere Kategorie personenbezogener Daten besonders strengen Anforderungen an die Verarbeitung unterliegen. Für solche Daten sind insbesondere geeignete Garantien für die Rechte und Freiheiten der betroffenen Person i. S. d. Art. 10 JI-Richlinie vorzusehen. Daher ist eine Regelung zur Speicherdauer der DNA-Identifizierungsmuster, die wie bisher auch normenspezifisch im Gesetz verankert ist, absolut wünschenswert und unterstreicht den besonders schutzwürdigen Charakter dieser Daten.
Aus den gleichen Gründen ist eine normspezifische Regelung zur Löschung der Datenidentifizierungsmuster angezeigt.

Zu § 32 SOG-E (Einsatz technischer Mittel zur offenen Bild- und Tonaufnahme sowie zur Bild- und Tonaufzeichnung):

Diese Vorschrift ist neu strukturiert und ergänzt und erweitert die bislang geltende Regelung deutlich.

a) § 32 Abs. 1 Nr. 3 SOG-E:

Neu eingefügt ist zunächst die Regelung in Abs. 1 Nr. 3, wonach zukünftig Bildaufnahmen und Übersichtsaufnahmen bei öffentlichen Veranstaltungen und Ansammlungen zur Lenkung und Leitung des Einsatzes gemacht werden dürfen. Bildaufzeichnungen dürfen von Verhaltens- oder Zustandsstörern unter den Voraussetzungen des Abs. 2 gemacht werden.

Die Gesetzesbegründung sollte hier klarer formuliert werden. In der Begründung wird nicht hinreichend deutlich, dass Aufzeichnungen nur unter eingeschränkten Voraussetzungen zulässig sind und das bei der Bildaufnahme eine Speicherung ausgeschlossen ist und diese erst vorgenommen werden darf, wenn die Voraussetzungen von Abs. 1 Nr. 2 vorliegen. Wünschenswert wäre es, wenn die Gesetzesbegründung kurz den Unterschied zwischen Aufnahme und Aufzeichnung darlegen würde. So würde eine missverständliche Interpretation der Gesetzes-begründung vermieden.

Bereits die Anfertigung von Bild- und Übersichtsaufnahmen nach § 32 Abs.1 Nr. 3 SOG-E berührt den Schutzbereich des Grundrechts auf informationelle Selbst-bestimmung. Nach dem Kamera-Monitor-Prinzip wird dadurch eine Übertragung und Beobachtung in Echtzeit ermöglicht.
Bei öffentlichen Veranstaltungen und Ansammlungen erfolgt dadurch ein Eingriff in das Grundrecht der allgemeinen Handlungsfreiheit nach Art. 2 Abs. 1 GG und das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung. Denn wer sich zu einer öffentlichen Veranstaltung begibt, muss nach § 32 Abs. 1 Nr. 3 SOG-E damit rechnen, dass das Geschehen an eine Leitstelle übermittelt wird und auch damit, dass es aufgezeichnet wird. Dies ist zwar nicht ohne weitere Voraussetzung möglich. Das ist dem Grundrechtsträger aber nicht bekannt: Er hat die Befürchtung, staatlicherseits registriert zu werden, allein durch die Wahrnehmung der Kamera, wenn dies zur Lenkung und Leitung des Einsatzes erforderlich ist, was im Ermessen der Polizei liegt. Der Eingriff in das Grundrecht der allgemeinen Handlungsfreiheit ist darin zu sehen, dass das Bewusstsein der

potentiellen Beobachtung den Betroffenen faktisch von der Ausübung grundrechtlicher Freiheiten abhalten kann.

Problematisch ist, dass diese Maßnahmen wie auch die Maßnahmen nach Abs. 1 und 4 in ihrer Intensität gesteigert werden können, weil zusätzlich die Beobachtung nach den Abs. 1, 3 und 4 gemäß § 34 Nr. 1 SOG-E mittels unbemannter Luftfahrtsysteme (Drohnen) durchgeführt werden kann. Dies wird bei Besuchern öffentlicher Veranstaltungen die Besorgnis, jederzeit beobachtet werden zu können, verstärken. Eine über den Köpfen auftauchende Drohne verstärkt das Gefühl des Ausgeliefertseins, die Besorgnis, unter steter potentieller Beobachtung zu stehen. Es handelt sich zudem um einen Eingriff von erheblicher Streubreite, die durch § 32 Abs. 6 SOG-E auch ausdrücklich gebilligt wird. Insofern sollte diese Steigerungsmöglichkeit mittels Drohnen nicht zulässig sein.

b) § 32 Abs. 7 SOG-E:

Die Löschfristen in § 32 Abs. 7 SOG-E ist im Fall der Absätze 3 und 4 verdoppelt worden. Zur Begründung wird auf die Notwendigkeit einer längeren Speicherdauer zur Sichtung und Auswertung verwiesen, dies vermag nicht zu überzeugen.

c) 32 Abs. 8 SOG-E:

Neu gefasst ist auch die Regelung § 32 Abs. 8 SOG-E, eine Ermächtigungsgrundlage für die Installation fester Videoüberwachungstechnik an Einsatzfahrzeugen. Darin wird bestimmt, dass die Polizei an öffentlichen Orten, im Rahmen der Gefahrenabwehr und bei der Verfolgung von Straftaten und Ordnungswidrigkeiten technische Mittel zur offenen Bild- und Tonaufzeichnung in oder an Fahrzeugen verwenden darf. Neben einer kritisch zu bewertenden Ausweitung von Bildaufzeichnungen mit rein optisch-technischen Mitteln auf nunmehr Bild- und **Ton**aufzeichnungen, gibt es weiterhin eine unverhältnismäßige Erweiterung der Speicherdauer. Sofern keine Straftat vorlag, sind nach der bisherigen Regelung die Aufzeichnungen unverzüglich, bis spätestens zum Ende der Dienstschicht zu löschen. Dies entspricht auch dem neu eingefügten Abs. 1 in § 46h SOG-E, welcher den in der JI-Ri verankerten Datenschutzgrundsatz der Datensparsamkeit (*Art 4 Abs. 1 Buchstabe c JI-Ri)* zum Mittelpunkt jedweder Verarbeitung von personenbezogenen Daten macht. Die nun vorgesehene pauschalisierte Speicherdauer von zwei Wochen trägt diesem Datenschutzgrundsatz nicht Rechnung. Fraglich ist weiterhin, wie die neu und zusätzlich eingeführte Tonaufnahme gerechtfertigt werden kann. Da regelmäßig davon auszugehen ist, dass die Straftaten und Ordnungswidrigkeiten an den öffentlichen Orten mehrheitlich außerhalb und vom Fahrzeug entfernt stattfinden und demzufolge nur selten oder bruchstückhaft Gespräche aufgezeichnet werden können, ist ein Mehrwert nicht ersichtlich. Vielmehr ist davon auszugehen, dass eher unerwünschte Tonaufzeichnungen von Gesprächen im Auto aufgezeichnet werden, die mit einer Straftat oder Ordnungswidrigkeit nichts zu tun haben und damit in das Recht der betroffenen Personen auf informelle Selbstbestimmung eingreifen. Hier ist dem Gebot der Datensparsamkeit Rechnung zu tragen und auf die Tonaufzeichnungen sollte weiterhin verzichtet werden.

d) § 32 Abs. 9 SOG-E:

Ganz neu eingefügt ist mit § 32 Absatz 9 SOG-E eine Ermächtigungsgrundlage zur Videoüberwachung in polizeilichen Räumen. Diese ist zu begrüßen, denn hierdurch kann auch aus Sicht der Beschuldigten der Verlauf der Vernehmung dokumentiert werden.

Zu § 32 a SOG-E (Einsatz körpernah getragener Aufnahmegeräte):

a) § 32 a Abs. 4 SOG-E:

§ 32 a Abs. 4 SOG-E verweist nunmehr auf § 32 Abs. 6 SOG-E. In der – gerade mal ein halbes Jahr alten – Regelung sind normspezifisch die Kennzeichnungspflicht (Transparenzgebot), der Kernbereichsschutz und Löschungsverpflichtungen geregelt. Der neu ausgestaltete Absatz 4 ist eine Verschlechterung gegenüber der erst vor einem halben Jahr gerade neu geschaffenen Regelung. Wegen der Eingriffstiefe der Maßnahme ist aus unserer Sicht eine normspezifische Regelung wünschenswert. Hinsichtlich der Erkennbarkeit der Maßnahme würde eine normspezifische Regelung insbesondere auch Art. 12 Abs. 1 JI-Ri Rechnung tragen.

b) § 32a Abs. 5 SOG-E:

§ 32 a Abs. 5 SOG-E 5 regelt die Löschung der gespeicherten Daten nach 2 Wochen. Die normspezifische Regelung zur Dokumentationspflicht der Löschung soll mit Blick auf § 46 d entfallen. Dies sehen wir als nicht überzeugend an: Die Beibehaltung der Regelung „Die Löschung ist zu dokumentieren“, würde systematisch passen und die Anwendbarkeit der Vorschrift übersichtlich gestalten. Sie ist nicht länger als die jetzt vorgesehene Formulierung „§ 32 Absatz 7 Satz 3 gilt entsprechend“, aber präzisier und übersichtlicher, insbesondere für die Gesetzesanwender.

Zu § 33 c SOG-E (Einsatz technischer Mittel zum Eingriff in informations-technische Systeme):

Die in § 33 c SOG-E neu eingeführte Online-Durchsuchung stellt einen äußerst schwerwiegenden Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG) dar. Entsprechend hohe Anforderungen stellt das Bundesverfassungsgericht an die Rechtfertigung eines solchen Eingriffs.

Zwar sieht die Norm nunmehr in Absatz 2 Satz 3 vor, dass, soweit möglich, technisch sicherzustellen ist, dass Daten, die kernbereichsrelevante Informationen betreffen, nicht erhoben werden.
Es fehlt aber an verfassungsrechtlich hinreichenden Vorkehrungen auf der Ebene des nachgelagerten Kernbereichsschutzes. Die Vorschrift des § 26 a Abs. 5 SOG-E, nach der die erhobenen Daten der oder dem behördlichen Datenschutzbeauftragten zur Auswertung und Entscheidung über die Rechtmäßigkeit dieser Datenerhebung vorzulegen sind, sieht keine hinreichend unabhängige Kontrolle vor. Laut Bundes-verfassungsgericht dient die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle neben der Rechtmäßigkeitskontrolle maßgeblich dem Ziel, kernbereichsrelevante Daten so frühzeitig herauszufiltern, dass sie den Sicherheits-behörden nach Möglichkeit nicht offenbar werden. Dies setzt voraus, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird. Das ist hier jedoch nicht der Fall. Die vorliegende Regelung überlässt die Sichtung einer oder einem Bediensteten der Behörde. Dass diese oder dieser als behördeninterne Datenschutzbeauftragte oder behördeninterner Datenschutzbeauftragter weisungsfrei ist, reicht für eine unabhängige Kontrolle nicht aus.
Die Gewährleistung einer wirksamen aufsichtlichen Kontrolle setzt nach den Ausführungen des Bundesverfassungsgerichts zunächst eine mit wirksamen Befugnissen ausgestattete Stelle voraus. Dazu ist erforderlich, dass die Daten-erhebungen vollständig protokolliert werden. Es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Daten-schutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält.

Auch nach Art. 47 Abs. 1 JI-Ri haben die Mitgliedstaaten durch Rechtsvorschriften vorzusehen, dass jede Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt. Diese Befugnisse umfassen zumindest die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten, die verarbeitet werden, und auf alle Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten.
Darüber hinaus haben die Mitgliedstaaten gemäß Art. 47 Abs. 2 JI-Ri durch Rechtsvorschriften vorzusehen, dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse verfügt, die es ihr unter anderem gestatten, den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung, und eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen.
Nach § 48 b SOG-E übt der Landesbeauftragte demgegenüber jedoch nur die Befugnisse entsprechend Artikel 58 Absatz 1, Absatz 2 Buchstabe a und b, Absatz 3 Buchstabe a und b der Verordnung (EU) 2016/679 aus.

Zu § 34 SOG-E (Einsatz unbemannter Luftfahrtsysteme):

Dieser Einsatz stellt einen Eingriff mit erheblicher Streubreite dar, da nicht nur einzelne Personen, sondern in erheblichem Maße auch Dritte erfasst werden. Schon die Videoüberwachung ist ein Eingriff, dem sich Betroffene nur begrenzt entziehen können. Die Beobachtung aus der Luft stellt hierzu eine Steigerung dar, da sie den gesamten aus der Luft kontrollierbaren Bereich flächendeckend erfassen kann. Erfolgt der Einsatz aus großer Distanz, so ist er für Betroffene zudem nicht bemerkbar. Erfolgt der Einsatz aus der Nähe, ist in der Regel nicht zu erkennen, dass es sich um eine polizeiliche Maßnahme handelt. Dem Einsatz unbemannter Fluggeräte kommt daher eine eigenständige zusätzliche Eingriffsqualität zu, weshalb an dessen Zulässigkeit strenge Anforderungen zu stellen sind. Insbesondere fehlt eine Regelung, die den Hinweis auf die unbemannten Luftfahrtsysteme regelt. Der Drohneneinsatz muss als polizeiliche Maßnahme wahrnehmbar sein, neben dem Flugsystem muss auch die verantwortliche Stelle erkennbar sein. Problematisch ist vor allem der Einsatz in Verbindung mit § 32 Abs. 1 Ziff. 3 SOG-E (dazu oben).

Zu § 37 a SOG-E (Verarbeitung zu Zwecken der wissenschaftlichen und historischen Forschung, Aus- und Fortbildung und Statistik):

§ 37 a Abs. 3 SOG-E regelt abweichend von § 4 des Landesdatenschutzgesetzes die Verwendung von Daten zu Zwecken der Aus- und Fortbildung. Eine Verwendung von Bild- und Tonaufzeichnungen aus polizeilichen Einsatzgeschehen zu Zwecken der Aus- und Fortbildung unterfällt zweifelsfrei nicht der JI-Richtlinie, sondern der DS-GVO, mit der Folge, dass für die Rechtmäßigkeit dieser Vorschrift die Maßstäbe der DS-GVO heranzuziehen sind. Die Verwendung von Bild- und Tonaufzeichnungen aus polizeilichen Einsatzgeschehen zu Zwecken der Aus- und Fortbildung verstößt gegen den Zweckbindungsgrundsatz in Artikel 5 Abs. 1 lit b DS-GVO. Zweck der Aufzeichnungen ist die Aufklärung oder Verhinderung von Straftaten oder der Schutz von Polizeibeamtinnen und Polizeibeamten. Eine Nutzung der gewonnenen Aufzeichnungsdaten für andere als diese festgelegten, eindeutigen und legitimierten Zwecke ist eine unrechtmäßige Zweckänderung und stellt darüber hinaus auch einen Verstoß gegen das Datenminimierungsgebot des Art. 5 Abs. 1 lit. c DS-GVO dar, denn nach diesem Grundsatz müssen die Daten im Rahmen der Zweckbindung qualitativ und quantitativ begrenzt werden, wobei das Wort Minimierung auf eine möglichst weitgehende Begrenzung abzielt. Darüber hinaus ist davon auszugehen, dass zum

einen regelmäßig nicht nur die polizeilichen Gegenüber auf den Bild- und Tonaufzeichnungen erscheinen werden, sondern auch unbeteiligte Dritte, quasi als Beiwerk, in Aufzeichnungen auftauchen. Für die beteiligten Personen ist bei der Aufnahme zu keiner Zeit nachvollziehbar gewesen, dass ihre Aufnahme für die Aus- und Fortbildung weiterverwendet werden könnten. Vor diesem Hintergrund ist es bemerkenswert, dass die Gesetzesbegründung dann auch noch eine Verpixelung der Aufnahmen wegen zu hohen Aufwandes ausdrücklich ausschließt. Es gibt mittlerweile Programme (z. B. das Programm KIWI), welche innerhalb kürzester Zeit Verpixelungen herstellen können. Auch die Abwägung zwischen dem öffentlichen Interesse an Aus- und Fortbildung und den schutzwürdigen Interessen der betroffenen Personen fällt zugunsten der schutzwürdigen Interessen der betroffenen Personen aus. Es ist davon auszugehen, dass diese Personen ggf. bei zukünftigen Kontrollen bereits stigmatisiert sind, da sie in Aus- und Fortbildungen schon als polizeiliche Gegenüber ausgewiesen wurden. Ihr Recht auf informationelle Selbstbestimmung wird somit unmittelbar eingeschränkt.

Zu § 43 SOG-E (Datenabgleich):

Die Regelung in § 43 Abs. 1 S. 5 SOG-E passt nach unserer Auffassung systematisch nicht in die Regelung des § 43 Abs. 1 SOG-E und sollte normspezifisch in § 27 SOG-E geregelt werden.

Zu § 43 a SOG-E (Datenerhebung und Datenabgleich zur Erkennung von Kraftfahrzeugkennzeichen):

In § 43 a Abs. 1 Nr. 6 SOG-E ist die Bezeichnung des Gebiets „von der Bundesgrenze bis einschließlich der Bundesautobahn A 20“ zu unbestimmt und daher verfassungswidrig. Hier ist eine kilometermäßige Begrenzung angezeigt. Dies gilt insbesondere mit Blick auf die Entscheidung des Bundesverfassungsgerichts vom 18. Dezember 2018 (Pressemitteilung Nr. 8/2019 des Bundesverfassungsgerichts vom 5. Februar 2019). Das Gericht hat ausgeführt, dass es verfassungsrechtlich unbedenklich ist, Kennzeichenkontrollen in einem Grenzgebiet bis zu einer Tiefe von 30 km durchzuführen. In der Entscheidung ist ausdrücklich benannt, dass die Befugnis zu Kennzeichenkontrollen hinreichend bestimmt und begrenzt sein sowie einen klaren Grenzbezug aufweisen muss. Diesen Anforderungen genügt die Formulierung im SOG-E „bis einschließlich der Bundesautobahn A 20“ nicht. Die A 20 zieht sich vom Grenzgebiet im Stettiner Raum hoch nach Greifswald und dann quer durch Mecklenburg-Vorpommern in Richtung Lübeck. Auf dieser gesamten Strecke sind nach dem Wortlaut des § 43 a Abs. 1 Nr. 6 SOG-E Kennzeichenkontrollen möglich. Diese Regelung steht damit im klaren Widerspruch zu den vom Bundesverfassungsgericht festgelegten Vorgaben für die Zulässigkeit einer Kennzeichenkontrolle und ist unzulässig.

Zu § 44 SOG-E (Rasterfahndung):

§ 44 Abs. 7 SOG-E regelt die Dokumentation der Löschung.
Hier ist – anders als im ersten Entwurf – nicht mehr die Streichung des ganzen Absatzes 7 vorgesehen, sondern nur noch die Streichung von Absatz 7 Satz 2, der die Dokumentation der Löschung und Vernichtung regelt. Warum diese Regelung gestrichen werden soll, erschließt sich nicht und verstößt gegen Artikel 4 Abs. 1 Buchstabe e) JI-Ri. Auch in den Polizeigesetzen anderer Bundesländer ist die Dokumentation der Löschung und Vernichtung gesetzlich geregelt (z. B. Art. 46 Abs. 4 des bayerischen PAG).

Zu § 45 SOG-E (Berichtigung, Ergänzung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten):

In § 45 Abs. 2 SOG-E sind nur eingeschränkte Löschpflichten bestimmt. Die Bestimmung „aus Anlass einer Einzelfallprüfung“ ist dabei zu unbestimmt und offen und genügt nicht den Anforderungen von Art 16 Abs. 2 JI-Ri. In § 45 Abs. 2 S. 2 SOG-E heißt es: „Kommt eine Löschung zum Zeitpunkt der Überprüfung nicht in Betracht, ist eine neue Prüffrist festzulegen.“ Es gibt keine Eingrenzung und keine Abwägungskriterien, wann dies der Fall sein kann. Dies genügt nicht den Bestimmtheitsanforderungen und verstößt gegen Art. 4 Abs. 1 Buchstabe c) JI-Ri.

Zu § 45a SOG-E (Festlegung von Prüffristen):

In § 45 a Abs. 2 SIG-E vermissen wir eine Regelung zum Ende der Speicherfrist, diese endet nie. Dies ist ein Verstoß gegen Art 5 JI-Ri.

§ 45 a Abs. 2 Nr. 1 SOG-E geht von einem „besonderen Fall“ aus, ohne dass erläutert wird, was darunter zu verstehen oder wann dieser Fall gegeben ist. Diese Formulierung ist zu unbestimmt und verstößt gegen Art. 4 Abs. 1 Buchstabe b) JI-Ri.

Zu § 46 SOG-E (Allgemeine Informationspflicht):

In § 46 Abs. 2 SOG-E ist ein Verstoß gegen das Wiederholungsverbot gegeben. Art. 13, 14 DS-GVO werden für anwendbar erklärt. Das ist unzulässig, da der Gesetzgeber Anwender und Bürger nicht darüber täuschen darf, dass die DS-GVO auch ohne entsprechende Erklärung selbstverständlich unmittelbar gilt. Der Verweis ist zudem schwer nachvollziehbar, da im SOG-E der Anwendungsbereich der DS-GVO nicht definiert wird.

Zu § 46 i SOG-E (Anforderung an die Sicherheit der Datenverarbeitung):

Die Gewährleistung der Sicherheit der Datenverarbeitung ist ein zentraler Aspekt um die Rechte und Freiheiten natürlicher Personen zu schützen. Insofern begrüßen wir ausdrücklich die Anforderungen in § 46 i SOG-E. Wir regen jedoch folgende Ergänzungen an, um die Anforderungen von Artikel 4 JI-RL zu präzisieren. In Absatz 1 Satz 1 sollte anstelle von „verbundenen Gefahren für die Rechtsgüter der betroffenen Personen“ eine Konkretisierung auf die gängige Sprachweise „verbundenen Gefahren für die Rechte und Freiheiten der betroffenen Personen“ erfolgen. In Satz 2 sollten neben den Technischen Richtlinien und Empfehlungen des BSI auch die einschlägigen Standards berücksichtigt werden: „Die verantwortliche Stelle hat hierbei die einschlägigen Standards, Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.“ Absatz 3 bezieht sich auf die technischen und organisatorischen Maßnahmen aus dem Bundesdatenschutzgesetz. Hier regen wir an, dass anstelle der 14 numerisch aufgeführten nicht abschließenden Maßnahmen die sieben Gewährleistungsziele normiert werden, die auch die Basis für das Standard-Datenschutzmodell bilden. Diese sieben Gewährleistungsziele beschreiben die Schutzrichtung des Datenschutzes, so dass aus ihnen sämtliche notwendigen technischen und organisatorischen Maßnahmen abgeleitet werden können. Die Gewährleistungsziele sind vollständig in Art. 5 DS-GVO enthalten und mittlerweile auch in diversen Dokumenten des IT-Planungsrates verankert (etwa in der Nationalen E-Government-Strategie).

Wir empfehlen daher Absatz 2 und 3 wie folgt zusammenzulegen: (1) Die Maßnahmen nach Absatz 1 sollen gewährleisten, dass
1. grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden; diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihrer Speicherfrist und ihrer Zugänglichkeit (Datenminimierung),
2. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
3. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell und die zu ihrer Verarbeitung eingesetzten Systeme und Dienste integer bleiben (Integrität),
4. personenbezogene Daten und die zu ihrer Verarbeitung vorgesehenen Systeme und Dienste zeitgerecht zur Verfügung stehen (Verfügbarkeit),
5. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten einschließlich der zur ihrer Umsetzung getroffenen technisch-administrativen Voreinstellungen vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können, personenbezogene Daten ihrem Ursprung zugeordnet werden können und festgestellt werden kann, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat (Transparenz),
6. die Datenverarbeitung so organisiert und die eingesetzten technischen Systeme so gestaltet sind, dass sie der betroffenen Person die Ausübung der ihr zustehenden Rechte nach Kapitel 3 der Verordnung (EU) 2016/679 wirksam ermöglichen (Intervenierbarkeit), und dass
7. jede Verarbeitung von personenbezogenen Daten ausschließlich im Rahmen im Vorhinein bestimmter Befugnisse für vorab festgelegte rechtmäßige Zwecke erfolgt und die Daten hierfür nach den jeweiligen Zwecken und nach unterschiedlichen betroffenen Personen getrennt werden können (Nichtverkettung).

Zu § 48 SOG-E (Recht auf Auskunft und Akteneinsicht):

In § 48 Abs. 5 SOG-E fehlt die Benennung einer Frist, innerhalb der dem Recht auf Auskunft entsprochen werden muss. Zwar heißt es in Absatz 5 „unverzüglich“. Aus unserer Praxis im Rahmen der Bearbeitung von Petitionen ist aber bekannt, dass Anfragen von Antragstellern tatsächlich über Monate nicht beantwortet werden, nicht einmal eine Eingangsbestätigung wird erteilt, Nachfragen bleiben ebenfalls unbeantwortet. Vor diesem Hintergrund ist die Festlegung einer konkreten Frist geboten. Wir schlagen daher die Einfügung einer Monatsfrist vor.

Zu § 48b SOG-E (Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz über die Datenverarbeitung):

Diese Vorschrift beschränkt die Befugnisse der Aufsichtsbehörde. Dies verstößt gegen Art. 47 der JI-Ri. Die Regelung ist „systemwidrig“, weil sie Verweise auf die DS-GVO im Anwendungsbereich der JI-Ri vornimmt. Dies ist nur schwer verständlich, was auch daraus resultiert, dass die jeweiligen Anwendungsbereiche im SOG-E nicht definiert sind.

a) § 48 b Absätze 1 und 2 SOG-E:

Nach Art. 47 Abs. 2 JI-Ri sieht jeder Mitgliedstaat durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse wie Warnung, Anweisung und Verhängung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung verfügt. Diese Vorschrift wird mit dem in § 48 b Abs. 1 SOG-E enthaltenen Verweis auf Art. 58 Abs. 2 lit. a und b DS-GVO nur unzureichend in innerstaatliches Recht umgesetzt.

Die Einschränkung der Befugnis der Datenschutzaufsichtsbehörde, Verantwortliche mit einem förmlichen Verwaltungsakt anzuweisen, Verarbeitungsvorgänge mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, verstößt gegen Art. 47 Abs. 2 lit. b der JI-Ri. Dort ist ausdrücklich geregelt, dass die Mitgliedstaaten entsprechende „Anweisungsbefugnisse“ schaffen müssen. Insbesondere ist der Ausschluss der Anordnung einer Löschung unzulässig. Art. 47 Abs. 2 lit. b JI-Ri verlangt ausdrücklich Regelungen in den Mitgliedstaaten, die die Aufsichtsbehörde ermächtigen, auch die Löschung von Daten anzuordnen. Die Einschränkung der Befugnis der Datenschutzaufsichtsbehörde, eine vorübergehende oder endgültige Beschränkung der Verarbeitung zu verhängen, verstößt gegen Art. 47 Abs. 2 lit. c der JI-Ri. Dort ist vorgesehen, dass die Mitgliedstaaten entsprechende „Verhängungsbefugnisse“ schaffen müssen.

b) § 48 b Absatz 3 SOG-E:

Die in Absatz 3 geregelte Befugnis, bei Verstößen, die eine entsprechende Anordnung erfordern würden, stattdessen eine Beanstandung auszusprechen und nach weiterer Fristsetzung den Landtag bzw. die Landesregierung zu informieren, regelt ein „Spiel auf Zeit“, das keineswegs geeignet ist, die Anforderungen von Art. 47 Abs. 2 lit. b und c JI-Ri zu erfüllen.

c) § 48 b Absatz 5 und 6 SOG-E:

Die Absätze 5 und 6 sind mit der in Art. 42 JI-Ri geregelten Unabhängigkeit der Datenschutzaufsichtsbehörde unvereinbar. Ob, wann und wie die Datenschutzaufsichtsbehörde kontrolliert, ist in der DS-GVO i. V. m. dem Landesdatenschutzgesetz geregelt. Weitergehende Einschränkungen oder Verpflichtungen sind unzulässig.

Zu § 48 c SOG-E (Zusammenarbeit mit der oder dem Landesbeauftragten für den Datenschutz und deren oder dessen Anhörung)

Aufgrund des Verweises in Absatz 4 auf die europarechtswidrig eingeschränkten Befugnisse der Datenschutzaufsichtsbehörde in § 48 b SOG-E ist die Regelung insgesamt europarechtswidrig. Gelangt die Aufsichtsbehörde im Anwendungsbereich der DS-GVO im Rahmen der Konsultation nach Art. 36 DS-GVO zu dem Ergebnis, dass eine Verarbeitung gegen die DS-GVO verstößt, muss und wird die Aufsichtsbehörde diese Verarbeitung untersagen. Diese Kompetenz ergibt sich unmittelbar aus der DS-GVO und kann durch die nationalen Gesetzgeber nicht eingeschränkt werden. Wegen Art. 288 AEUV dürfte diese Regelung weder von der Datenschutzaufsichtsbehörde noch von einem Gericht, dass eine entsprechende Anordnung überprüfen würde, angewendet werden und muss schlicht ignoriert werden. Im Anwendungsbereich der JI-Ri muss der nationale Gesetzgeber entsprechende Befugnisse schaffen. Art. 28 der JI-Ri regelt ausdrücklich, dass die Aufsichtsbehörde neben angemessenen Empfehlungen auch Maßnahmen nach Art. 47 JI-Ri anordnen kann. Dazu gehört nach Art. 47 Abs. 2 lit. c ausdrücklich auch die Befugnis, eine Verarbeitung zu verbieten.

Zu § 57 SOG-E (Durchsuchung von Sachen):

Der durch den Gesetzentwurf neu eingefügte § 57 Abs. 2 SOG-E gestattet die Erstreckung der Durchsuchung auf „räumlich getrennte Speichermedien“, also die Durchsuchung der „Cloud“. Dies berührt den Schutzbereich des aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme („Computer-Grundrecht“) als Ausprägung des allgemeinen Persönlichkeitsrechts.

Nach Auffassung des Bundesverfassungsgerichts bewahrt dieses Grundrecht den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten. Eine Einschränkung im Hinblick auf die Art und Weise des Zugriffs nimmt das Bundesverfassungsgericht bei der Schutzbereichsbestimmung nicht vor. Das Auslesen der Festplatten von Personalcomputern, der Speichereinheiten von Mobiltelefonen oder von anderen externen Datenträgern erlaubt grundsätzlich einen umfassenden Zugriff auf die dort gespeicherten Daten und gibt damit einen Einblick in wesentliche Teile der Lebensgestaltung einer Person. Soweit durch das Auslesen Zugriffsbeschränkungen überwunden, zum Beispiel Passwörter „gehackt“ werden müssen, ist dadurch auch die Integrität des Systems betroffen. Entsprechend hohe Anforderungen sind daher an die Rechtfertigung eines solchen Eingriffs zu stellen.

Der Kernbereich privater Lebensgestaltung ist auch bei der nicht verdeckten Durchsuchung elektronischer Speichermedien zu schützen. Der damit verbundene, wenn auch nur einmalige, Zugriff trägt typischerweise die Gefahr in sich, dass höchstpersönliche, dem Kernbereich privater Lebensgestaltung zuzurechnende Daten, die der Nutzer im Vertrauen, dass sie geschützt sind, dem Computer bzw. der Cloud anvertraut hat, offenbar werden. Wenn diese Informationen gleichwohl erhoben werden, so bedeutet auch dies einen Eingriff in den geschützten Kernbereich des Rechts auf die Vertraulichkeit informationstechnischer Systeme. Dem ist durch geeignete Vorkehrungen vorzubeugen, die sicherstellen, dass kernbereichsrelevante Daten nicht erhoben werden oder aber dass dann, wenn sie nicht bei Erhebung ausgesondert werden können, diese Aussonderung auf der Verwertungsebene erfolgt. Daher sollte eine entsprechende Geltung des § 26 a SOG-E geregelt werden, bzw. eine entsprechende normspezifische Regelung getroffen werden.

Insbesondere die systematische Durchsuchung und Auswertung von Festplatten und Clouds mit Analysetools stellt einen erheblichen Grundrechtseingriff dar. Mit der Durchsuchung von Sachen kann eine derart eingriffsintensive Maßnahme nicht gleichgesetzt werden. Daher ist die Befugnis zur Durchsuchung elektronischer Speichermedien und Clouds unter einen Richtervorbehalt zu stellen. Zwar handelt es sich bei der Durchsuchung nach § 57 Abs. 2 SOG um eine offene Maßnahme. Aufgrund ihrer Eingriffsintensität hat jedoch grundsätzlich ein Richter, in Eilfällen die Leitung der zuständigen Polizeibehörde oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter, darüber zu entscheiden. Auch § 110 Abs. 3 StPO setzt grundsätzlich eine vom Ermittlungsrichter angeordnete Durchsuchung voraus (§ 105 Abs. 1 StPO).

Zudem sollten Maßnahmen nach § 57 Abs. 2 SOG-E aufgrund ihrer Eingriffsintensität protokolliert und die betroffenen Personen im Falle ihrer Abwesenheit über die Durchsuchung benachrichtigt werden.

Zu § 61 SOG-E (Sicherstellung von Sachen):

§ 61 Abs. 1 S. 2 SOG-E erstreckt die Befugnis zur Sicherstellung von Sachen auch auf elektronische Speichermedien und auf Daten auf von diesem räumlich getrennten Speichermedien, soweit auf sie vom elektronischen Speichermedium aus zugegriffen werden kann. Außerdem kann nach Satz 3 der weitere Zugriff auf diese Daten ausgeschlossen werden. Entgegen dem Vorentwurf hat die sicherstellende Behörde nunmehr die richterliche Bestätigung der Rechtmäßigkeit der Maßnahmen nach Satz 2 und 3 unverzüglich zu beantragen. Eine präventive Kontrolle durch eine richterliche Anordnung ist jedoch nach wie vor nicht vorgesehen.

Im Unterschied zum Vorentwurf wird nicht mehr die entsprechende Anwendung der §§ 26 a, 26 b, 46 d, 46 g, 46 i angeordnet, damit ist der Kernbereichsschutz nicht mehr geregelt.
Der Kernbereich privater Lebensgestaltung ist aber – wie im Vorentwurf vorgesehen – auch bei der Sicherstellung von elektronischen Speichermedien zu schützen. Der damit verbundene Zugriff trägt typischerweise die Gefahr in sich, dass höchstpersönliche, dem Kernbereich privater Lebensgestaltung zuzurechnende Daten, die der Nutzer im Vertrauen, dass sie geschützt sind, dem Computer bzw. der Cloud anvertraut hat, offenbar werden. Wenn diese Informationen gleichwohl erhoben werden, so bedeutet auch dies einen Eingriff in den geschützten Kernbereich des Rechts auf die Vertraulichkeit informationstechnischer Systeme. Dem ist durch geeignete Vorkehrungen vorzubeugen, die sicherstellen, dass kernbereichsrelevante Daten nicht erhoben werden oder aber dass dann, wenn sie nicht bei Erhebung ausgesondert werden können, diese Aussonderung auf der Verwertungsebene erfolgt. Daher sollte eine entsprechende Geltung des § 26 a SOG-E geregelt werden, bzw. eine entsprechende normspezifische Regelung getroffen werden, wie dies im ersten Entwurf bereits vorgesehen war. Im Falle ihrer Abwesenheit sollten die betroffenen Personen außerdem über die Sicherstellung benachrichtigt werden müssen.

Zu § 76 SOG-E (Schadensersatzansprüche und Entschädigung aus der Verarbeitung von Daten):

§ 76 SOG-E soll Art. 56 der JI-Ri umsetzen. Problematisch ist hier wiederum, dass die Regelung auf den Anwendungsbereich der JI-Richtlinie beschränkt ist, dieser Anwendungsbereich im Gesetz aber nicht definiert wird. Zudem wäre in der Begründung ein erläuternde Hinweis zur Beweislast wünschenswert: Bei der automatisierten Verarbeitung wird eine verschuldensunabhängige Gefährdungshaftung eingeführt, während bei der nicht automatisierten Verarbeitung eine Exkulpationsmöglichkeit besteht. Hier wird das Verschulden der verantwortlichen Stelle zu Gunsten der betroffenen Person vermutet. Im Streitfall muss sich die verarbeitende Stelle entlasten (vgl. BeckOK-BDSG/Wolff/Brink § 83 Rn. 51).

Zu § 85 SOG-E (Vollzug gegen Träger der öffentlichen Verwaltung):

Für den Vollzug von Verwaltungsakten, die auf Herausgabe einer Sache oder auf Vornahme einer Handlung oder auf Duldung oder Unterlassung gerichtet sind, gelten gemäß § 110 VwVfG M-V die §§ 79 bis 100 SOG. Nach § 85 SOG-E ist der Vollzug gegen Träger der öffentlichen Verwaltung nur zulässig, soweit er durch Rechtsvorschrift ausdrücklich zugelassen ist. Das ist in den Anwendungsbereichen von DS-GVO und JI-Ri jedoch nicht der Fall.
Im Zusammenspiel zwischen DSG M-V und dem SOG-E werden die Abhilfe- und Sanktionsbefugnisse des LfDI gegenüber Behörden im Anwendungsbereich der DS-GVO stark eingeschränkt und bleiben entscheidend hinter den Forderungen der DS-GVO zurück. Diese fordert in Art. 57 Abs. 1 lit. a DS-GVO, dass jede Aufsichtsbehörde in ihrem Zuständigkeitsbereich die Anwendung der DS-GVO überwachen und durchsetzen kann. In Mecklenburg-Vorpommern sind allerdings keinerlei Maßnahmen vorgesehen, die den LfDI in die Lage versetzen würden, Datenschutzverstöße bei öffentlichen Stellen abzustellen. Der LfDI kann zwar gegen eine Behörde einen Verwaltungsakt erlassen und zu einem bestimmten Tun oder Unterlassen anweisen, er hat aber keine Möglichkeiten, die Umsetzung des rechtskräftigen Verwaltungsaktes sicherzustellen. Wie bei der Videoüberwachung auf dem Schweriner Marienplatz zu beobachten war, reicht die Befugnis zum Erlass eines Verwaltungsakts zur Durchsetzung der DS-GVO im öffentlichen Bereich nicht aus. Obwohl der LfDI ein vorübergehendes Verbot der Verarbeitung verhängt hatte, wurde die Videoüberwachung auf dem Schweriner Marienplatz unverändert fortgesetzt.

Wir regen daher an, in § 85 SOG-E den folgenden Satz 2 zu ergänzen: „Satz 1 gilt nicht für Maßnahmen nach Art. 58 Abs. 2 der Verordnung (EU) 2016/679.“ Im Anwendungsbereich der JI-Ri besteht die gleiche Situation. Nach Art. 46 Abs. 1 lit. a JI-Ri hat jeder Mitgliedstaat vorzusehen, dass jede Aufsichtsbehörde in seinem Hoheitsgebiet die Anwendung der nach dieser Richtlinie erlassenen Vorschriften sowie deren Durchführungsvorschriften überwacht und durchsetzt. Auch in diesem Bereich ist jedoch der Vollzug gegen Träger der öffentlichen Verwaltung unzulässig.
Dies wirkt sich nach den Ausführungen des Bundesverfassungsgerichts in seiner Entscheidung vom 20. April 2016 – Aktenzeichen 1 BvR 966/09 – zur verfassungsgemäßen Ausgestaltung bestimmter Regelungen im Bundeskriminalamtgesetz (BKAG) auf die Verhältnismäßigkeit der im SOG-E geregelten Überwachungsmaßnahmen aus. Weil eine Transparenz der Datenerhebung und -verarbeitung sowie die Ermöglichung individuellen Rechtsschutzes für heimliche Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden können, kommt der Gewährleistung einer effektiven aufsichtlichen Kontrolle nach Ansicht des Bundesverfassungsgerichts umso größere Bedeutung zu. Der Verhältnismäßigkeitsgrundsatz stelle für tief in die Privatsphäre reichende Überwachungsmaßnahmen deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen. Die Gewährleistung einer wirksamen aufsichtlichen Kontrolle setzt, so das Bundesverfassungsgericht, eine mit wirksamen Befugnissen ausgestattete Stelle voraus. Diese Voraussetzung ist im öffentlichen Bereich jedoch nicht gegeben.
Im nicht-öffentlichen Bereich besteht demgegenüber die Möglichkeit der Vollziehung von Verwaltungsakten. Handelt ein Unternehmen nicht entsprechend eines vollziehbaren Verwaltungsaktes, können gegen das Unternehmen beispielsweise Zwangsgelder verhängt werden. Außerdem steht dem LfDI im nicht-öffentlichen Bereich noch ein zweites Instrument zur Verfügung: Werden Anordnungen des LfDI nicht befolgt, stellt dies nach Art. 83 Abs. 5 lit. e DS-GVO eine Ordnungswidrigkeit dar, die mit hohen Bußgeldern sanktioniert werden kann. Gegen Behörden oder sonstige öffentliche Stellen werden jedoch nach § 22 Abs. 3 DSG M-V keine Geldbußen verhängt.
Zwar kann nach Art. 83 Abs. 7 DS-GVO jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können. Eine pauschale Ausnahme für den öffentlichen Bereich kann damit aus unserer Sicht jedoch nicht gemeint gewesen sein. Dafür spricht auch der Wortlaut des Art. 57 JI-Ri, wonach die Mitgliedstaaten festlegen, welche Sanktionen bei einem Verstoß gegen die nach der Richtlinie erlassenen Vorschriften zu verhängen sind. Das „Ob“ der Verhängung von Sanktionen steht hier nicht in Frage, obwohl die JI-Ri ausschließlich im öffentlichen Bereich Anwendung findet. Eine Vorschrift über die Verhängung von Sanktionen für Verstöße gegen nach der Richtlinie erlassene Vorschriften enthält der SOG-E jedoch nicht. Auch insoweit wird die JI-Ri nur unzureichend in innerstaatliches Recht umgesetzt.
Hinzukommt, dass eine verhältnismäßige Ausgestaltung von Überwachungsmaßnahmen nach der Rechtsprechung des Bundesverfassungsgerichts wirksame Sanktionen bei Rechtsverletzungen voraussetzt. Würden auch schwere Verletzungen der Eingriffsvoraussetzungen im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts angesichts der immateriellen Natur dieses Rechts verkümmern würde, widerspräche dies der Verpflichtung der staatlichen Gewalt, die Entfaltung der Persönlichkeit wirksam zu schützen. Dies könne insbesondere der Fall sein, wenn, wie hier, eine unberechtigte Erhebung oder Verwendung der Daten mangels materiellen Schadens regelmäßig ohne einen der Genugtuung der Betroffenen dienenden Ausgleich bliebe.

Damit bleibt der SOG-E nicht nur hinter den Anforderungen von DS-GVO und JI-Ri, sondern auch hinter denen des Bundesverfassungsgerichts zurück.

Mit freundlichen Grüße
im Auftrag

[redacted]