

Bonn, den 18.02.2026

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages, LT-Drs. 20/3754

zum Entwurf eines Gesetzes zur Stärkung des Verfassungsschutzes im Lande

Schleswig-Holstein

Diese Stellungnahme beschränkt sich auf diejenigen Punkte, die aus hiesiger Sicht besonders wichtig erscheinen, insbesondere im Vergleich mit den Vorschriften des Bundesverfassungsschutzgesetzes (BVerfSchG) und des Gesetzes über den Militärischen Abschirmdienst (MADG). Wie erbeten, geht diese Stellungnahme auch auf § 69 LVerfSchG-E ein. Diese Stellungnahme orientiert sich an der Gliederung des Gesetzentwurfs. Vorangestellt ist eine Zusammenfassung der wesentlichen Punkte der Stellungnahme.

Zusammenfassung der Stellungnahme der BfDI zum Entwurf des LVerfSchG

1. Mitteilungspflichten (§ 23 LVerfSchG-E):

Es wird empfohlen, die Mitteilungspflichten gemäß § 23 so zu gestalten, dass die Entscheidung über eine Zurückstellung oder das Absehen von Mitteilungen einer unabhängigen gerichtlichen Kontrolle unterliegt, ähnlich wie im Bundesrecht (§ 23 MADG). Dies würde den Grundrechtsschutz der Betroffenen erhöhen.

2. Erhebung aus elektronischen Quellen (§ 34 LVerfSchG-E):

Die Voraussetzungen für die Nutzung elektronischer Quellen, insbesondere das Abgreifen von Social-Media-Daten, muss klarer im Gesetz geregelt werden. Zudem sollte der Einsatz virtueller Agenten und ähnlicher Technologien unter die Mitteilungspflicht und die richterliche Anordnung gestellt werden.

3. Richterliche Anordnung (§ 36 LVerfSchG-E):

Besonders eingriffsintensive Maßnahmen müssen nach den Vorgaben des BVerfG vorab von einem unabhängigen Gericht überprüft werden. Es wird empfohlen, eine vergleichbare Regelung wie § 45 Abs. 2 MADG zu schaffen.

4. Einsatz von Personen zur Informationsbeschaffung (§ 37 LVerfSchG-E):

Der Einsatz verdeckter Mitarbeiter oder Vertrauenspersonen ist eine besonders eingriffsintensive Maßnahme. Diese sollten zwingend der richterlichen Anordnung unterliegen. Ebenso sollte der Einsatz von virtuellen Agenten unter diese Regelung fallen.

IT-gestützte Informationsanalyse und Datenverarbeitung (§ 69 LVerfSchG-E):

5. Datenquellen und Zweckbindung (§ 69 Abs. 1):

Die Nutzung von bereits erhobenen Daten soll klar auf den Aufgabenbereich der Verfassungsschutzbehörde beschränkt werden. Insbesondere müssen Daten aus sensiblen Quellen wie Wohnraumüberwachungen und Online-Durchsuchungen ausgeschlossen werden.

6. Eingriffsschwellen (§ 69 Abs. 2 und 4):

Die Eingriffsschwellen für die IT-gestützte Analyse müssen präziser festgelegt

werden, um Missbrauch und weitreichende Datenanalysen zu verhindern. Eine Abgrenzung zwischen „Internetquellen“ und „Internetdiensten“ sollte klar definiert werden.

7. Nachvollziehbarkeit und Transparenz (§ 69 Abs. 3 und 8):

Die Nachvollziehbarkeit der automatisierten Auswertungen ist entscheidend für die Rechtmäßigkeit der Maßnahmen. Es wird empfohlen, diese Transparenz zu stärken und den Einsatz nicht nachvollziehbarer Systeme zu vermeiden.

8. Drittbetroffenheit (§ 69 Abs. 5):

Daten von unbeteiligten Dritten sollten sofort gesperrt oder gelöscht werden, um Missbrauch zu verhindern.

9. Verwendung zu Trainingszwecken (§ 69 Abs. 6):

Die Nutzung synthetischer oder öffentlich verfügbarer Daten sollte rechtlichen Vorrang haben vor der Nutzung von Echtdaten zum Training von Systemen.

10. Dienstanweisung (§ 69 Abs. 10):

Die Anhörungspflicht bei Erlass der Dienstanweisung soll sich auf den bzw. die Landesdatenschutzbeauftragte erstrecken. Das Gesetz sollte die wesentlichen Eckpunkte der Dienstanweisung regeln und ausschließen, dass die Befugnis des § 69 untergesetzlich erweitert werden kann.

Weitere Empfehlungen und Datenschutzkontrollen:

11. Übermittlungsauftrag (§ 70 LVerfSchG-E):

Die Protokollierung und Dokumentation von Datenübermittlungen muss vollständig sein, um die Anforderungen des BVerfG zu erfüllen. Die Rechtsgrundlage für jede Übermittlung sollte immer dokumentiert werden.

12. Minderjährigenschutz (§ 71 LVerfSchG-E):

§ 71 Abs. 2 Satz 2 sollte nur bei Übermittlungen an inländische Strafverfolgungsbehörden greifen, während Übermittlungen an Strafverfolgungsbehörden im Ausland nur möglich sein sollten, wenn ein dringender Tatverdacht einer besonders schweren Straftat vorliegt.

13. Unabhängige Datenschutzkontrolle, Allgemeines Datenschutzrecht (§§ 92, 93 LVerfSchG-E):

Die Kontrolle durch den/ die Landesdatenschutzbeauftragte sollte nicht eingeschränkt werden. Insbesondere in Bezug auf die Speicherung und Weiterverarbeitung von Daten muss diese oder muss dieser weiterhin umfassende Kontrollrechte haben.

14. G10-Kommission und Anwendung des Datenschutzes (§ 101, 102 LVerfSchG-E):

Es wird empfohlen, die Zusammensetzung der G10-Kommission so anzupassen, dass eine richterliche Perspektive vertreten ist, um den Anforderungen des Bundesverfassungsgerichts zu entsprechen.

1. Mitteilung an betroffene Personen, § 23

Ich habe der Begründung entnommen, dass die Mitteilungspflicht nach § 23 weitgehend der Vorgängervorschrift entspricht. Inhaltlich begrüße ich, dass in Schleswig-Holstein, anders als im Bund, grundsätzlich auch Personen über Maßnahmen unterrichtet werden müssen, wenn sie unvermeidbar betroffene Dritte sind.

Allerdings trifft nach dem Gesetzentwurf die Entscheidung darüber, ob eine Mitteilung bspw. bei besonderen Auskunftsverlangen (bis zu fünf Jahre) zurückgestellt werden muss sowie darüber, ob dann ggf. ganz von ihr abgesehen werden kann, die Verfassungsschutzbehörde selbst. In § 23 Abs. 2 und 3 MADG erfolgt die Zurückstellung grds. nur maximal 12 Monate durch den MAD selbst, danach bedarf sie gerichtlichen Zustimmung. Das Gericht bestimmt dann auch die Dauer der weiteren Zurückstellung oder das endgültige Absehen von der Mitteilung grundsätzlich selbst. Es erfolgt hier also eine Überprüfung durch eine unabhängige Stelle, was für die Betroffenen ein Mehr an Grundrechtsschutz darstellt.

Ich empfehle daher, § 23 LVerfSchG-E an der Regelung von § 23 MADG zu orientieren.

2. Informationserhebung aus elektronischen Quellen, § 34

Nach der Gesetzesbegründung trug die vergleichbare Vorgängernorm die Bezeichnung „Heimliches Aufklären des Internets“. Gegenstand sollen z.B. Quellen aus dem „Internet sowie ferner elektronische Zeitungen/Zeitschriften, Internetradio oder CD-ROMs“ sein (Drs. 20/3754, S. 102). Ob damit das Ziel erreicht werden kann, genauer als bislang zu beschreiben, welche Befugnisse der Verfassungsschutzbehörde insoweit zustehen, ist allerdings fraglich. „Das Internet“ ist ein Begriff, der konkretisiert werden müsste. Insbesondere sofern darunter auch bspw. Social-Media-Profile inklusive Posts und Fotos gefasst werden sollen, würde es sich anbieten, dies zumindest in der Gesetzesbegründung zu konkretisieren.

Da gemäß § 34 die Informationserhebung aus elektronischen Quellen nicht von der Mitteilungspflicht nach § 23 sowie von der gerichtlichen Anordnungspflicht nach §§ 35 Abs. 4, 36 umfasst ist, definiert der Gesetzgeber diese Form der Informationserhebung prinzipiell nicht als besonders eingriffsintensiv. So ist jedenfalls die Bezugnahme in § 36 Abs. 1 zu lesen, der regelt, dass Mittel mit besonderer Eingriffsintensität nach §§ 38 bis 43 sowie nach § 46 vorbehaltlich des Absatzes 5 nur auf richterliche Anordnung eingesetzt werden dürfen. Aus hiesiger Sicht kann die Informationsbeschaffung aus elektronischen Quellen aber sehr wohl besonders eingriffsintensiv sein. Insbesondere, wenn von § 34 auch der Einsatz von sog. virtuellen Agenten umfasst sein sollte, gilt es zu bedenken, dass eine solche Kommunikation sowohl

höchstpersönliche Informationen als auch solche Informationen umfassen kann, die zur Bildung eines Persönlichkeitsprofils führen können.

Ich empfehle daher, § 34 mit in die Pflichtenkataloge von §§ 23 sowie 35 Abs. 4 und 36 Abs. 1 aufzunehmen.

Dasselbe gilt, sofern der Einsatz von virtuellen Agenten unter § 37, Einsatz von Personen zur Informationsbeschaffung, hier verdeckte Mitarbeiterinnen und Mitarbeiter (Abs. 1 Nr. 1) fallen sollte. Auch § 37 wird in § 36 nicht als eine solche Maßnahme erwähnt, vgl. dazu auch unter 4.

3. Richterliche Anordnung, § 36

Nach der Rechtsprechung des Bundesverfassungsgerichts¹ müssen bestimmte eingriffsintensive Maßnahmen vorab von einer unabhängigen Stelle kontrolliert werden. Nach § 36 Abs. 3 Satz 5 ist die Verfassungsschutzbehörde nicht zur Vorlage von Akten oder zu Auskünften verpflichtet, wenn das Bekanntwerden des Inhalts dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen. Diese Einschränkung ist nicht mit der verfassungsgerichtlichen Vorgabe in Einklang zu bringen, weil die weiten nachrichtendienstlichen Maßnahmen bereits im Vorfeld einer konkreten Gefahr stattfinden und das BVerfG klargestellt hat, dass der Vorabkontrolle eine besondere Bedeutung zukommt und die Vertraulichkeit der Arbeit des Verfassungsschutzes einer unabhängigen Kontrolle nicht entgegensteht². Das BVerfG hat dem Gesetzgeber in der Auswahl der zuständigen Stelle einen Gestaltungsspielraum eingeräumt.³ Wenn der Gesetzgeber sich für das Amtsgericht als zuständige Stelle für die Vorabkontrolle entscheidet, widerspricht es der Bedeutung der Vorabkontrolle eine Ausnahmeregelung, wie in §§ 36 Abs. 3 Satz 5, vorzusehen. Im aktuellen § 45 Abs. 2 MADG konnten die Geheimhaltungserfordernisse mit der Notwendigkeit der gerichtlichen Vorabkontrolle in Einklang gebracht werden. In der Praxis bedeutet das, dass der zuständige Amtsrichter in die Liegenschaft des MAD kommt, dort alle Unterlagen einsieht und der MAD ihm (sicherheitsüberprüftes) Geschäftsstellenpersonal stellt.

Ich empfehle daher, eine vergleichbare Regelung wie § 45 Abs. 2 MADG zu schaffen, um eine umfassende Vorabkontrolle durch das Amtsgericht zu ermöglichen.

¹ BVerfG, 1 BvR 1619/17, Rn. 213 ff.

² a.a.O., Rn. 224.

³ vgl. BVerfG, 1 BvR 1619/17, Rn. 224.

4. Einsatz von Personen zur Informationsbeschaffung, § 37

§ 37 regelt verschiedene Möglichkeiten, wie Personen zur Informationsbeschaffung eingesetzt werden können: angefangen von verdeckten Mitarbeiterinnen und Mitarbeitern (Abs. 1 Nr. 1), über Vertrauenspersonen (Nr. 2), sonstige geheime Informantinnen und Informanten (Nr. 3), übergeworbene Agentinnen und Agenten (Nr. 4) bis hin zu sog. Gewährspersonen (Nr. 5). Absatz 3 legt fest, dass Nr. 3 und 5 keine eingriffsintensiven nachrichtendienstlichen Mittel sind und dass in diesen Fällen sowie in den Fällen von Nr. 4 keine richterliche Anordnung erfolgt.

Die Aussagen von § 37 Abs. 3 und § 36 Abs. 1 stehen in Widerspruch zueinander. Während nach § 37 Abs. 3 der Einsatz von z.B. verdeckten Mitarbeiterinnen und Mitarbeitern oder Vertrauenspersonen durchaus ein Mittel mit besonderer Eingriffsintensität sein kann – und dies in aller Regel auch tatsächlich so sein wird –, liest sich § 36 mangels Erwähnung von § 37 so, dass der Einsatz dieser Personen jedenfalls keiner richterlichen Anordnung bedarf.

Ich empfehle, auch aufgrund meiner Einschätzung zu virtuellen Agenten (siehe Nr. 2), § 36 Abs. 1 wie folgt zu fassen:

„Mittel mit besonderer Eingriffsintensität dürfen vorbehaltlich des Absatzes 5 sowie weiterer, in diesem Gesetz ausdrücklich genannter Ausnahmen nur auf richterliche Anordnung eingesetzt werden.“

Diese Formulierung trägt dem Gedanken des Gesetzgebers aus § 35 Rechnung, dass letztlich in jedem Einzelfall eine Abwägung zu erfolgen hat, wie eingriffsintensiv das jeweilige nachrichtendienstliche Mittel ist, und daher eine richterliche Anordnung erforderlich ist. Der Gesetzgeber hat sich dazu entschieden, den Rechtsanwendern wenig konkrete Vorgaben dazu zu machen, welche Mittel in welchem Umfang einer richterlichen Anordnung bedürfen. Dieses Ziel kann so beibehalten werden. Gleichzeitig schließt es kein Mittel als solches aus.

5. Weiterverarbeitung personenbezogener Informationen, § 64

Nach § 64 Abs. 5 sind personenbezogene Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, zu kennzeichnen. Ich begrüße diese Regelung.

Nach Absatz 6 Satz 1 darf die Weiterverarbeitung zum Zwecke der Datenschutzkontrolle protokolliert werden. Die Regelung entspricht nach der Gesetzesbegründung dem bisherigen § 11 Abs. 4.

Ich empfehle, § 64 Abs. 6 wie folgt zu formulieren:

„Die Weiterverarbeitung der Informationen wird protokolliert. Die Protokolldaten dürfen nur zum Zwecke der Datenschutzkontrolle sowie zur Aufklärung eines Verdachts

auf Datenmissbrauch verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.“

Die Protokollierung sollte nicht im Ermessen stehen. Bei der Formulierung sowie bei der Ergänzung einer Löschfrist habe ich mich an den vergleichbaren Vorschriften von § 63 Abs. 1 Sätze 7 und 8 sowie § 36 Abs. 7 orientiert. Insofern empfehle ich zu prüfen, ob mit meinem Vorschlag alle Verwendungszwecke abgedeckt sind und ob die Löschfrist angemessen ist.

6. IT-gestützte Informationsanalyse, § 69

§ 69 LVerfSchG-E soll die Weiterverarbeitung bereits erhobener Informationen mittels technischer Systeme (einschließlich mathematisch-statistischer Verfahren, maschinellen Lernens und KI) normieren und wird in der Begründung ausdrücklich auf das Urteil des BVerfG vom 16. Februar 2023 („Hessen-Data“) gestützt.

a. § 69 Abs. 1 LVerfSchG-E – Datenquellen und Zweck

Abs. 1 beschreibt den Zweck und die zulässigen Auswertungsschritte. Dies entspricht den Vorgaben des BVerfG, welches zu dem Risiko einer „Datennutzung ins Blaue hinein“ ausgeführt hat, dass es „[f]ür die Wahrung der Zweckbindung [...] demnach darauf an[kommt], dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt. Diese Anforderungen sind erforderlich, aber grundsätzlich auch ausreichend, um eine weitere Nutzung der Daten im Rahmen der Zweckbindung zu legitimieren⁴“.

Gleichwohl empfehle ich, diese Zweckbindung im Gesetzestext besser zum Ausdruck zu bringen. Hierzu empfehle ich die folgende Formulierung:

„Die Verfassungsschutzbehörde darf zur Erfüllung ihrer gesetzlichen Aufgaben nach §§ 8 bis 14 bereits erhobene Informationen einschließlich personenbezogener Daten, insbesondere [...]“

Bereits in Abs. 1 sollte die Nutzung von Daten aus Wohnraumüberwachungen und Online-Durchsuchungen ausgeschlossen werden.

Insofern Abs. 1 ausführt, dass auch Daten aus dem nachrichtendienstlichen Informationssystem („NADIS“) oder anderer Verbundsysteme genutzt werden, so sind dort grundsätzlich Informationen des Verfassungsschutzverbundes vorhanden. Die

⁴ BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19 ,1 BvR 2634/20, Rn.58

Rechtsprechung des BVerfG spricht allerdings ausdrücklich von der Legitimation der Zweckbindung bei der ursprünglich „erhebungsberechtigten Behörde“. Dies kann nur das jeweils zuständige LfV oder aber auf Bundesebene das BfV sein.

Ich empfehle daher klarzustellen, dass in jedem Fall nur Informationen einschließlich personenbezogener Daten verarbeitet werden, die die Verfassungsschutzbehörde in eigener Zuständigkeit zur Erfüllung ihrer gesetzlichen Aufgaben mittels eigener Befugnisse erhoben hat.

b. § 69 Abs. 2 und Abs. 4 LVerfSchG-E – Eingriffsschwellen

Abs. 2 normiert ausweislich der Gesetzesbegründung die „Eingriffsschwellen“ für die IT-gestützte Informationsauswertung. Kritisch ist, dass die Norm die Schwellen im Wortlaut relativ offenhält („... für die Aufklärung im Einzelfall erforderlich sind.“), während das BVerfG in „Hessen-Data“ die Zulässigkeit automatisierter Auswertung abgestuft nach Eingriffsgewicht und – bei schwerwiegenden Eingriffen – an besonders gewichtige Rechtsgüter sowie eine hinreichend bestimmte Einsatzschwelle knüpft⁵. Gerade „anspruchsvoll ausgestaltete Eingriffsschwellen“⁶ können die Eingriffsqualität von automatisierten Auswertungen umfangreicher Datenbestände abmildern.

Das BVerfG hat hierzu – zur Bestimmung der notwendigen Eingriffsschwellen – ein Stufenmodell entwickelt, welches die Eingriffsintensität automatisierter Datenanalysen anhand bestimmter Faktoren (z.B. Art und Umfang der genutzten Daten, aber auch den Einsatz von KI) bemisst, um dann Eingriffsschwellen zu definieren, die den Eingriff – die Datenverarbeitung – rechtfertigen können.

Der Entwurf bildet dieses „Stufenmodell“ vor allem über Abs. 4 (Datenherkunft/Intensität) ab, nicht aber durch eine klare, an Eingriffsintensitäten orientierten Eingriffsschwellen für die Analyse als solche.

Dass Abs. 4 vor allem die Einbeziehung besonders sensibler Daten begrenzt, ist wichtig und entspricht den Vorgaben des BVerfG. Dies ersetzt jedoch nicht die Frage, wann und für den Schutz welcher Rechtsgüter eine potenziell sehr eingriffsintensive „Zusammenführung“ großer Datenbestände überhaupt stattfinden darf.

⁵ BVerfG, a.a.O. zur Eingriffsintensität und deren Bestimmungsfaktoren insb. Rn. 78 f.; ferner zu Kontrolle/Absicherung insb. Rn. 106 f., 109; zur Normierung zentraler Leitplanken insb. Rn. 110, 112.

⁶ BVerfG, a.a.O. Rn. 95, 104 ff.

Eine Norm zur allgemeinen Regelung von Eingriffsintensitäten und Eingriffsschwellen könnte sich z.B. an § 8 MADG orientieren.

Die „Einbeziehung von Datensätzen aus Internetquellen“ ist im Einzelfall zulässig, während „unmittelbarer automatisierter Abgleich aus Internetdiensten“ unzulässig ist. Diese Unterscheidung ist nicht ganz eindeutig **und** auslegungsbedürftig (z.B. Import lokaler OSINT-Auswertungen, automatisierte Matching-Routinen). Unklar sind hierbei bereits die genutzten Begrifflichkeiten. Wann liegt eine „Internetquelle“ vor und wann ein „Internetdienst“? **Es ist m.E. erforderlich, diese Begrifflichkeiten legal zu definieren oder sich an bestehenden Definitionen – etwa am TKG oder am TDDDG zu orientieren.** Gerade weil Abs. 1 eine „systemübergreifende Zusammenführung“ erlaubt, kann das Verständnis der beiden Begrifflichkeiten von Bedeutung sein. Unklare Abgrenzungen bergen das Risiko, dass die Norm im Ergebnis weiterwirkt, als es die Begründung („keine willkürliche Vorratsdatennutzung“) intendiert.

c. § 69 Abs. 3 und Abs. 8 LVerfSchG-E – Einschränkung der Nachvollziehbarkeit

Abs. 3 enthält viele sehr begrüßenswerte Regelungen, die den Vorgaben des BVerfG genügen. So ist stets die abschließende Bewertung durch Mitarbeitende (menschliche Aufsicht) erforderlich und die Ergebnisse der automatisierten Datenverarbeitung müssen nachvollziehbar sein. Abs. 8 enthält dann flankierende Regelungen zur Protokollierung, zu Rechte-/Rollenkonzepten und zur Löschung von Protokolldaten.

Unklar ist die Formulierung, dass der Einsatz von selbst weiter lernenden Systemen ausgeschlossen wird. Es wird davon ausgegangen, dass hiermit adaptive Systeme gemeint sind. Es sollte darauf geachtet werden, dass unterscheidungskräftige und hinreichend eindeutige Begrifflichkeiten konsistent verwendet werden.

Allerdings wird die Nachvollziehbarkeit von Auswertungen in Abs. 3 relativiert („so weit technisch möglich“). Nach der Rechtsprechung des BVerfG stellt der Verhältnismäßigkeitsgrundsatz in jedem Fall auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle.⁷

Wenn ein Verfahren in der Praxis nur begrenzt oder gar nicht nachvollziehbar ist, dann kann sein Einsatz jedenfalls in Konstellationen mit hohem Eingriffsgewicht dazu führen, dass die fehlende Nachvollziehbarkeit zur Unverhältnismäßigkeit führt. Gleichzeitig kommen hier auch die fehlenden Eingriffsschwellen erneut zum Tragen, die die eingesetzten Verfahren vorliegend nicht verfassungsrechtlich beschränken.

⁷ BVerfG, a.a.O. Rn. 109.

Die hier vom Gesetzgeber verwendete Formulierung kann also zum Einfallstor für gerade solche Systeme werden, die wegen der fehlenden Nachvollziehbarkeit verfassungsrechtlich besonders problematisch sind und zudem schon nicht an verfassungsrechtlich gebotene Eingriffsschwellen gekoppelt sind.

d. § 69 Abs. 5 LVerfSchG-E – Drittbetroffenheit

Abs. 5 untersagt die Weiterverarbeitung von Informationen zu unbeteiligten Personen, die durch die Analyse gewonnen wurden. Das Verbot adressiert die Weiterverarbeitung, lässt aber offen, wie mit Drittbetroffenheit in der „Entstehungsphase“ der Analyse (Trefferlisten oder Korrelationen) umzugehen ist. Bei automatisierter Analyse sind Drittbetroffenheiten typischerweise systemimmanent und nicht zuverlässig zu vermeiden.

Sehr fraglich ist jedoch, wer im Anwendungsbereich der Norm als „unbeteiligt“ gilt. Eine Legaldefinition ist nicht ersichtlich. Wenn im Endeffekt jede Person, über die bei der Beobachtung Daten gesammelt wird, als in irgendeiner Weise beteiligt gilt (z.B. „nützliche Idioten“⁸), läuft die Regelung größtenteils ins Leere. Wünschenswert und für einen klaren Anwendungsbereich der Norm sinnvoll wäre eine hinreichende Definition des „unbeteiligten Dritten“, dessen Daten dann nach Möglichkeit unverzüglich für eine weitere Verarbeitung zu sperren sind oder im besten Fall unverzüglich gelöscht werden.

e. § 69 Abs. 6 LVerfSchG-E – Zweckverändernde Nutzung / Training

Abs. 6 erlaubt die Verwendung personenbezogener Daten zur Entwicklung/Überprüfung/Änderung/Training von IT-Produkten; die Begründung betont, dass für valide Ergebnisse teils „Originalinformationen“ erforderlich seien und nennt als Beispiel Trainingsbedarf mit Daten aus Telekommunikationsüberwachungsmaßnahmen; Wohnraumüberwachungsdaten sind ausgeschlossen.

Zu begrüßen ist zunächst, dass Abs. 6 Vorgaben zur Minimierung von Bias und den daraus möglicherweise resultierenden Diskriminierungen enthält. Daneben enthält die Norm auch keine Möglichkeiten zur Weitergabe von Trainingsdaten an Dritte.

Mit Blick auf die Nutzung von Trainingsdaten empfehle ich, hier nicht auf die Erforderlichkeit der Nutzung zu Trainingszwecken abzustellen, sondern auf die Erforderlichkeit des späteren Einsatzes des trainierten Systems. Ist nämlich der

⁸ Vgl. BVerwG NVwZ 2005, 451 (453); OVG Münster 13.2.2009 – 16 A 845/08, BeckRS 2009, 31498.

Einsatz des trainierten Systems nicht erforderlich, so kann auch die Datennutzung zu Trainingszwecken nicht erforderlich sein⁹.

Daneben sollten auch Daten aus TKÜ-Maßnahmen wegen des besonders schweren Eingriffs in Art. 10 GG von der Nutzung zu Trainingszwecken ausgeschlossen werden.¹⁰

Grundsätzlich sollten in der Regel zu Trainingszwecken synthetische Daten oder – falls zulässig – frei verfügbare öffentliche Daten genutzt werden. Auch allgemein im Internet verfügbare personenbezogene Daten fallen in den Schutzbereich des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

Wesentliche Grundzüge des Entscheidungsprozesses für die Auswahl und die spätere Nutzung von Trainingsdaten sind nachvollziehbar zu dokumentieren. Erst wenn feststeht, dass der Einsatz synthetischer Daten ausscheidet und eine Anonymisierung oder Pseudonymisierung von Echtdaten nicht möglich ist (weil dies zB die Zuverlässigkeit eines erforderlichen KI-Systems beeinträchtigt), können auch Echtdaten eingesetzt werden.

In seiner bestehenden Form macht der Abs. 6 die Nutzung von Echtdaten eher zum Regelfall. Diese Systematik sollte umgekehrt werden. Denkbar wäre beispielsweise, eine kaskadenartige Prüfung vorzusehen, wonach vorrangig synthetische Daten eingesetzt werden sollten. Diese können ohne Beschränkungen für Entwicklungs- und Testzwecke eingesetzt werden.

Macht die Entwicklung eines (KI-) Systems im Einzelfall ein Training mit personenbezogenen Daten erforderlich, weil synthetische Daten nicht in geeigneter Art und Weise genutzt werden können, so ist zu prüfen, ob überhaupt die Nutzung von personenbezogenen Daten geeignet und erforderlich ist. Es ist zu dokumentieren, weshalb personenbezogene Daten zu Trainingszwecken im Rahmen der Entwicklung eines konkreten (KI-)Systems herangezogen werden müssen. Für Einzelheiten zu einer möglichen Prüffolge wird auf die Kurzposition der BfDI vom 16.05.2025: „Personenbezogenen Daten bei Software-Entwicklung und -Tests“ verwiesen¹¹.

⁹ Kühne/Golla/Schäfer, GSZ 2025, 272, 281.

¹⁰ Das BVerfG hat die Nutzung von Telekommunikationsdaten im Hessen-Data Urteil ausdrücklich ausgeschlossen (BVerfG, - 1 BvR 1547/19 -, - 1 BvR 2634/20 -, Rn. 176).

¹¹ https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Themen/Technik/Kurzposition_Testdaten.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 19.02.2026

f. § 69 Abs. 10 LVerfSchG-E - Dienstanweisung

Nach Abs. 10 ist eine Dienstanweisung zur Nutzung der automatisierten Verfahren zu erlassen, diese ergeht nach Anhörung des Parlamentarischen Kontrollgremiums. **Ich empfehle, die Anhörungspflicht auf die bzw. den Landesdatenschutzbeauftragten zu erweitern.** Alle Landes- sowie die Bundesdatenschutzbeauftragte haben Erfahrung in der Beratung zum Einsatz von verschiedensten technischen Systemen, inklusive auch von Datenanalyse-Systemen und KI-basierten Systemen. Auch wenn die KI-Verordnung der EU im Bereich der nationalen Sicherheit und damit im Bereich des Verfassungsschutzes keine Anwendung findet, hilft die Kenntnis entsprechender Wertungen weiter. Gleichzeitig entspricht es meiner Erfahrung, dass insbesondere Produkte zur Datenanalyse von ein und demselben Anbieter häufig sowohl von Polizei- oder Strafverfolgungsbehörden als auch Nachrichtendiensten angewendet werden. Das Wissen um technische Möglichkeiten oder praktischen Schwierigkeiten kann dann behördenübergreifend genutzt werden.

Angesichts der Grundrechtsrelevanz automatisierter Analysen spricht zudem der Wesentlichkeitsgedanke dafür, dass zentrale Regelungsgegenstände der Dienstanweisung gesetzlich und nicht nur untergesetzlich vorgegeben werden¹². **Ich empfehle daher klarzustellen, dass die Dienstanweisung lediglich Regelungen zur technischen Umsetzung enthalten darf. Die materiellen Eingriffsvoraussetzungen des § 69 sowie die zu beachtenden Eingriffsschwellen können durch die Dienstanweisung nicht erweitert und/oder abgesenkt werden.**

7. Übermittlungsauftrag, Verfahren und Dokumentation, § 70

Nach § 70 Abs. 2 Sätze 4 und 5 muss die Entscheidung über sowie die Übermittlung (auch personenbezogener) Daten selbst aktenkundig gemacht werden. Aus meiner Sicht werden damit die Anforderungen des Bundesverfassungsgerichts an die Übermittlungsvorschriften nicht vollständig erfüllt. Das Gericht stellt in seiner Entscheidung zum BVerfSchG das Erfordernis einer Protokollierung von Übermittlungen inklusive der Nennung der entsprechenden Rechtsgrundlage auf.¹³ Zwar lässt sich darüber streiten, ob das Gericht tatsächlich eine technische Protokollierung gemeint hat oder es nicht vielmehr auf die Dokumentation ankommt. Mindestens müsste von der Dokumentation aber nach dem vorher Gesagten auch die einschlägige Übermitt-

¹² BVerfG, Urt. v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, zur Zulässigkeit administrativer Konkretisierung nur innerhalb gesetzlicher Leitplanken insb. Rn. 118; zur Notwendigkeit gesetzlicher Regelung der grundlegenden Züge und Begrenzungen insb. Rn. 110, 112.

¹³ 1 BvR 2354/13 Rn. 107.

lungsgrundlage umfasst sein. Diese Angabe dient der zielgerichteten Kontrolle, sowohl für den internen Datenschutz der Verfassungsschutzbehörde, als auch für die/den Landesdatenschutzbeauftragten und für das Parlamentarische Kontrollgremium.

Ich empfehle daher, § 70 Abs. 2 Satz 5 wie folgt zu fassen:

„In der entsprechenden Datei ist die Übermittlung sowie die Rechtsgrundlage für die Übermittlung zu vermerken.“

8. Minderjährigenschutz, § 71

Ich begrüße ausdrücklich, dass nach dieser Vorschrift personenbezogenen Informationen über das Verhalten Minderjähriger grundsätzlich nicht übermittelt werden dürfen und somit der Schutz Minderjähriger weiter gestärkt wird. Die in Abs. 1 Nrn. 1 bis 3 genannten Ausnahmen von diesem Grundsatz entsprechen weitestgehend den bundesgesetzlichen Regelungen und sind nachvollziehbar. Positiv hervorzuheben ist ferner, dass gemäß Absatz 2 Satz 1 Übermittlungen zur Strafverfolgung sowie zum administrativen Rechtsgüterschutz an die Mindestaltersgrenze von 14 Jahren gebunden sind. Kritisch sehe ich allerdings die Regelung in Abs. 2 Satz 2, die eine Übermittlung auch vor dem 14. Lebensjahr ermöglicht, wenn „die Übermittlung der strafrechtlichen Verfolgung volljähriger Täterinnen oder Täter oder Teilnehmerinnen oder Teilnehmern der Tat dient.“ Dies insbesondere unter dem Aspekt, dass § 71 beim Minderjährigenschutz, anders als bspw. § 36 und § 38 Abs. 5 MADG, nicht nach Inlands- und Auslandsübermittlungen bzw. nach Übermittlungen an einen Staat, der unmittelbar an die Bundesrepublik Deutschland angrenzt oder Mitgliedstaat der Europäischen Union oder des Nordatlantikvertrages ist, unterscheidet. Zwar teile ich die in der Gesetzesbegründung zu § 86 (S. 166) dargelegte Einschätzung, dass Übermittlungen ins Ausland für die Verfassungsschutzbehörde des Landes einen geringen Praxisbezug haben, dennoch sind solche Übermittlungen grundsätzlich möglich. Die besondere Sensibilität von Auslandsübermittlung sollte daher auch beim Minderjährigenschutz berücksichtigt werden.

Ich empfehle daher, die Möglichkeit des § 71 Abs. 2 Satz 2 nur bei Übermittlungen an inländische Strafverfolgungsbehörden zu eröffnen. Ferner sollte die Übermittlung an Strafverfolgungsbehörden im Ausland an die zusätzliche Voraussetzung gebunden werden, dass ein dringender Tatverdacht einer besonders schweren Straftat vorliegt.

9. Unabhängige Datenschutzkontrolle, § 92

Nach § 92 Abs. 1 kann sich jede Person, die der Auffassung ist, bei der Weiterverarbeitung ihrer personenbezogenen Daten durch die Verfassungsschutzbehörde in ihren Rechten verletzt zu sein, an den oder die Landesdatenschutzbeauftragte wenden. Zunächst begrüße ich ausdrücklich die nun im LVerfSchG-E Schleswig-Holstein niedergelegte Regelung zu den Kompetenzen und Aufgaben der/des Landesdatenschutzbeauftragten.

Ausweislich der Begründung zu § 64 Abs. 1 soll die Weiterverarbeitung „neben der Speicherung weitere Formen der weiteren Informationsverarbeitung, wie etwa die Nutzung oder Berichtigung“ erfassen (S. 137). Damit ist allerdings die *Erhebung* der Daten kein Aspekt, mit dem sich Betroffene an die/den Landesdatenschutzbeauftragten wenden können.

Ich empfehle zu prüfen, ob dies dem tatsächlichen Willen des Gesetzgebers entspricht.

Nach § 92 Abs. 2 Satz 2 erfolgt eine Abgrenzung zwischen den Kompetenzen der/des Landesdatenschutzbeauftragten, der G 10-Kommission und dem zuständigen Gericht: für die Einhaltung von Vorschriften der richterlichen Kontrolle nach § 36 ist ausschließlich das zuständige Gericht, für die Einhaltung von Vorschriften nach §§ 101 und 102 ausschließlich die G 10-Kommission zuständig. Die Gesetzesbegründung spricht insoweit von der „gerichtlichen Vorab- und Begleitkontrolle“ (S. 176). Wenn ich es richtig verstehe, ist mit Begleitkontrolle diejenige Kontrolle gemeint, die sich anschließt, sobald eine Maßnahme durch das Gericht genehmigt wurde, häufig auch als Ex-post-Kontrolle bezeichnet. Kontrolliert werden könnte insoweit z.B. die ordnungsgemäße Weiterverarbeitung der durch die jeweilige Maßnahme erhobenen Daten: wo werden die Daten gespeichert? Erfolgt eine rechtskonforme zweckändernde Nutzung? Werden die Vorschriften zum Minderjährigenschutz eingehalten? Erfolgt eine Löschung, sofern die Daten nicht mehr erforderlich sind?

Diese Arten von datenschutzrechtlicher Kontrolle kann ein Gericht meines Erachtens nicht leisten. Ich möchte auch der Aussage entgegenreten, dass es sich bei der Kontrolle durch das Gericht oder die G 10-Kommission um das stärkere Instrument mit einer größeren Prüfungstiefe handelt und dass eine zusätzliche datenschutzrechtliche Kontrolle daneben nicht erforderlich ist (S. 176). Dies mag für den Aspekt der Genehmigung einer solchen Maßnahme zutreffen.¹⁴ Aber gerade die anschließende

¹⁴ Vgl. allerdings den Abschlussbericht des Max-Planck-Instituts zur Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO aus 2003, wonach es bei den Begründungen der richterlichen Beschlüsse an Transparenz, Nachvollziehbarkeit und Kontrolle mangelt, <https://static.mpicc.de/shared/data/pdf/k115.pdf>, S. 467, sowie die Entschließung der 66.

Speicherung der erhobenen Daten z.B. im NADIS sowie die Übermittlung an andere Stellen kann für die Betroffenen aufgrund der Möglichkeit von sich anschließenden Maßnahmen anderer Stellen ebenfalls erheblich sein. Im Zusammenhang mit Übermittlungen würde sich dann auch die Frage stellen, wie die Abgrenzung der Kontrollkompetenzen erfolgt. Denn für die datenschutzrechtliche Kontrolle derjenigen Daten, die nicht durch eine G10-Maßnahme oder durch eine durch richterlichen Beschluss genehmigte Maßnahme erhoben wurden, bleibt ja nach dem Gesetzentwurf die/der Landesdatenschutzbeauftragte zuständig.

Denkbar ist zwar, dass nach § 92 Abs. 2 Satz 2, 2. Halbsatz das Gericht oder die G 10-Kommission die/den Landesdatenschutzbeauftragten ersucht, entsprechend zu kontrollieren. Eine entsprechende Vorschrift existiert auf Bundesebene für die Abgrenzung zwischen G 10-Kommission und BfDI ebenfalls. Sie ist aber nach meinem Kenntnisstand noch nie zur Anwendung gekommen. Es droht insoweit eine deutliche Verschlechterung des Datenschutzniveaus mangels entsprechender datenschutzrechtlicher Kontrollen.

Ich empfehle daher, § 92 Abs. 2 Satz 2 zu streichen.

Nach § 92 Abs. 3 Satz 3 kann die Verfassungsschutzbehörde die Auskunft oder Einsicht unterlassen oder verweigern, soweit dies aus zwingenden Gründen u.a. des Staatswohls notwendig ist. Im Vergleich zur bisherigen Vorschrift des § 18 Abs. 2 LDSG ist das eine Verschlechterung der Rechte des/der Landesdatenschutzbeauftragten. Nach der Gesetzesbegründung soll die Einschränkung u.a. deshalb notwendig sein, weil dem/der Landesdatenschutzbeauftragten keine weiter reichenden Kontrollbefugnisse zustehen dürfen als dem Parlamentarischen Kontrollgremium als zuständiger Kontrollinstanz der Legislative.

Diese Annahme überzeugt nicht. Zunächst besteht kein Zweifel, dass auch Datenschutzbeauftragte sowie deren Mitarbeitende ihre Arbeit im Interesse des Staatswohls verrichten. Sofern diese entsprechend sicherheitsgeprüft sind, liegen auch formell die Voraussetzungen vor. Legislative und administrative Kontrolle verfolgen unterschiedliche Zwecke. Es sind keine Gründe ersichtlich, weshalb die unabhängige Kontrolle durch Datenschutzbeauftragte nicht jedenfalls die gleichen Rechte und Befugnisse haben sollen wie auf administrativer Ebene stattfindende fachaufsichtliche Kontrolle.¹⁵

Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2003 zu den Konsequenzen dieser Untersuchung, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/66DSK-KonsequenzenAusDerUntersuchungDesMax-Planck-InstitutsUeberRechtswirklichkeitUndEffizienzDerUeberwachungDerTelekommunikation.pdf?__blob=publicationFile&v=7.

¹⁵ Jedenfalls auf Bundesebene gibt es eine Fachaufsicht, wenn die Aufgaben des Verfassungsschutzes durch das BfV und damit durch eine andere Behörde wahrgenommen werden als die Fachaufsicht (Bundesministerium des Innern).

Die Regelung in § 92 Abs. 3 Satz 3 sollte daher gestrichen werden.

10. Anwendung des allgemeinen Datenschutzes, § 93

Bei der Inbezugnahme des LDSG und des BDSG sollten noch folgende Änderungen geprüft werden.

- § 16 Abs. 3 BDSG sollte entsprechend anwendbar sein, und zwar auch, sofern die gesetzgeberische Absicht beibehalten wird, die sog. Begleitkontrolle von G 10-Maßnahmen nicht der/dem Landesdatenschutzbeauftragten zuzuweisen. Um prüfen zu können, ob die eigene Zuständigkeit gegeben ist, ist ein weites Einsichtsrecht erforderlich. Ich habe mich in der Vergangenheit aufgrund dieser Problematik wiederholt an den Bundesgesetzgeber gewandt, weil mir das BfV Einsicht in Unterlagen verweigert hatte, die nach seiner Aussage G10-Daten beinhalteten. Der G10-Kommission wurde wiederum die Einsicht in Unterlagen verweigert, die nach Aussage des BfV keine G 10-Daten beinhalteten. Hier drohten Kontrolllücken. Erst mit der Erwähnung dieses Themas in der Gesetzesbegründung zu § 26a BVerfSchG a.F. erledigte sich das Problem¹⁶. Ich hätte mir zwar eine ausdrückliche Erwähnung im Gesetz selbst gewünscht, allerdings ist mir seitdem die Einsicht insoweit nicht mehr verweigert worden.
- Positiv ist zu erwähnen, dass auch § 67 BDSG (Pflicht zur Durchführung einer Datenschutzfolgenabschätzung) entsprechend anwendbar ist.

11. G10-Kommission, §§ 101, 102

Das Bundesverfassungsgericht hat in seiner Entscheidung aus 2024 zur strategischen Inland-Ausland-Fernmeldeaufklärung des BND festgestellt, dass die G 10-Kommission auf Bundesebene nicht die Anforderungen an eine unabhängige Vorabkontrolle erfüllt, weil die Mitglieder ihre Tätigkeit lediglich als Ehrenamt ausüben und weil nicht gewährleistet ist, dass in der Kommission eine richterliche Perspektive vertreten ist.¹⁷ Zwar ist diese Entscheidung nur für spezielle Maßnahmen des BND er-

¹⁶ BT-Drs. 18/11325, S. 122; vgl. auch Nr. 10.2.10.3 des 26. Tätigkeitsberichts 2025-2026, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/26TB_15_16.pdf?__blob=publicationFile&v=9.

¹⁷ BT-Drs. 18/11325, S. 122; vgl. auch Nr. 10.2.10.3 des 26. Tätigkeitsberichts 2025-2026, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/26TB_15_16.pdf?__blob=publicationFile&v=9.

¹⁷ 1 BvR 1743/16 Rn. 207ff.

gangen, sie ist aber dennoch übertragbar auf Befugnisse der Verfassungsschutzbehörden zu Eingriffen in Art. 10 GG und damit auch auf die entsprechende Vorabkontrolle.

Nach § 101 Abs. 1 Satz 1 besteht die G 10-Kommission in Schleswig-Holstein aus der oder dem Vorsitzenden mit der Befähigung zum Richteramt und zwei Beisitzern. Das Kriterium der Befähigung zum Richteramt genügt ausweislich der o.g. Entscheidung nicht für die richterliche Perspektive. Das Bundesverfassungsgericht stellt dabei auf eine tatsächliche Erfahrung als Richter ab. Da die Mitglieder der schleswig-holsteinischen G 10-Kommission diese Aufgabe ebenfalls als Ehrenamt erfüllen, bedarf es hier einer Anpassung an die verfassungsgerichtliche Rechtsprechung.

Rein vorsorglich weise ich darauf hin, dass aufgrund der erwähnten Rechtsprechung die Normen des G 10-Gesetzes geändert werden müssen, und zwar bis zum 31. Dezember 2026. Alle Verweise im LVerfSchG-E auf das G 10-Gesetz werden ab diesem Zeitpunkt ins Leere gehen.

Sofern die Möglichkeit besteht, schon in diesem Gesetzgebungsvorhaben eine Ablösung vom G 10-Gesetz vorzunehmen, sollte dies umgesetzt werden.