Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 27.10.2023

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts[1] (BVerf-SchG-E) sowie zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes[2] (BNDG-E)

[1] BT-Drs. 20/8626.

[2] BT-Drs. 20/8627.

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

I. Vorbemerkung

Die offizielle Ressortabstimmung, an der ich gemäß §§ 45 Abs. 3 Satz 1, 21 Abs. 1 GGO frühzeitig zu beteiligen bin, war mit sieben Arbeitstagen betreffend das BNDG und mit sogar faktisch nur zwei Arbeitstagen betreffend das BVerfSchG äußerst kurz bemessen. Eine angemessene Prüfung der beiden Gesetzesentwürfe war somit nicht möglich. Ich hatte zwar die Gelegenheit, meine Hinweise schriftlich und mündlich darzulegen, allerdings war die Bereitschaft, diese umzusetzen, zu diesem späten Zeitpunkt faktisch nicht mehr gegeben. Selbst meine Hinweise auf redaktionelle Fehler blieben teilweise ungehört. Daher beschränke ich meine Stellungnahme gegenüber dem Innenausschuss ausnahmsweise nicht auf die aus meiner Sicht wichtigsten datenschutzrechtlichen Bedenken. Sondern ich erlaube mir auch, auf redaktionelle Fehler hinzuweisen, damit diese zumindest noch im parlamentarischen Verfahren bereinigt werden können.

Seit Jahren fordere ich eine umfassende Reform des Nachrichtendienstrechts und speziell auch des BVerfSchG. Ich nehme daher erfreut zur Kenntnis, dass die Bundesregierung die aktuellen Änderungen nur als ersten Teil einer solchen Reform ansieht und beabsichtigt, auch einen zweiten Teil folgen zu lassen – so ja der Gesetzestitel. Dies müsste angesichts der fortgeschrittenen Legislaturperiode und der notwendigen Vorbereitung zügig erfolgen.

Die Liste der unerledigten Aufgaben aus den verfassungsgerichtlichen Vorgaben ist lang. Nicht nur diese gilt es aber abzuarbeiten[3]. Auch im Rahmen meiner Aufsichtstätigkeit habe ich weitere regelungsbedürftige - Aspekte festgestellt. Nach meiner in 2023 abgeschlossenen Kontrolle des Gemeinsamen Terrorismusabwehrzentrums (GTAZ) habe ich die Schaffung gesetzlicher Regelungen bzw. Grundlagen für die Gemeinsamen Zentren empfohlen. Hintergrund ist, dass der in den Gemeinsamen Zentren praktizierte Informationsaustausch, also die Übermittlung personenbezogener Daten, hohe Risiken und zwar sowohl für die Rechte der betroffenen Personen als auch für die handelnden Behörden birgt. Zu schaffen sind aber auch unter anderem explizite Regelungen zum Einsatz von Künstlicher Intelligenz oder zu Verarbeitungsbeschränkungen zu Zwecken der parlamentarischen Beweissicherung („Löschmoratorien“)[4].

---

[3] Gebot zur Normenklarheit, das der Verwendung gesetzlicher Verweisungsketten Grenzen setzt, sowie daraus resultierend ein eigenständiges MADG; Regelung der Vorabkontrolle eingriffsintensiver Maßnahmen; Regelung von Erhebungs- und Speicherschwellen für Beobachtungsobjekte und die dazugehörigen Personen; Auswirkungen der verfassungsgerichtlichen Rechtsprechung zum Bereich von Polizei und Strafverfolgung auf den Nachrichtendienstebereich wie Regelungen zur automatisierten Datenanalyse; Regelungen zum Kernbereichsschutz beim Einsatz von V-Personen/Vertrauensleuten oder verdeckten Ermittlern/verdeckten Mitarbeitern.

[4] Vgl. dazu 31. TB Nr. 3.2.5 sowie Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23.03.2023.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

II. Datenschutzrechtliche Kritik an der Neuregelung der Übermittlungsvorschriften der Nachrichtendienste

1. Einleitung zu den Übermittlungsvorschriften

Im nachfolgenden werde ich mich bemühen, meine datenschutzrechtlichen Kritikpunkte an den vorgeschlagenen Übermittlungsvorschriften der beiden Entwürfe zum BVerfSchG und MADG zum einen und dem BNDG zu anderen weitestgehend zusammenzufassen, da aufgrund der gleichartigen Problemfelder die gleichen Aspekte zu diskutieren sind. Allerdings ist zu konstatieren, dass die beiden Entwürfe in ihrem Aufbau und ihrer Systematik grundlegend auseinanderlaufen und einige im Wesentlichen gleiche Aspekte verschiedene Regelungen erfahren. Hierin offenbart sich bereits die Inkonsistenz der vorgelegten Gesetzesentwürfe. Es ist nicht Ziel und auch nicht Aufgabe meiner Stellungnahme, all diese Differenzierungen herauszuarbeiten und darzulegen. Es gilt jedoch, dass gleichlaufende Vorgaben zur Regelung der Übermittlungen durch Nachrichtendienste verfassungsrechtlich geboten sind; hier besteht aus meiner Sicht umfangreicher Nachbesserungsbedarf.

In seinen Entscheidungen vom 26. April 2022 zum Bayerischen Verfassungsschutzgesetz (1 BvR 1619/17) und dem Beschluss vom 28. September 2022 zum BVerfSchG (1 BvR 2354/13) hat das Bundesverfassungsgericht (BVerfG) ausgeführt, dass es aufgrund des Aufgabenzuschnitts der Nachrichtendienste, die über keine operativen Anschlussbefugnisse verfügen, zulässig ist, die Befugnisse der Nachrichtendienste zur Datenerhebung an niedrigere Eingriffsschwellen zu knüpfen. Diese modifizierten Anforderungen an die Datenerhebungsbefugnisse sind jedoch nur verfassungsgemäß, wenn etwaige Übermittlungen der daraus erlangten Informationen an andere Stellen dann wiederum an besondere Bedingungen geknüpft werden: Zum einen ist die Übermittlung nur zum Schutz eines besonders gewichtigen Rechtsguts zulässig. Weiter müssen die Übermittlungsermächtigungen ausreichend hohe Übermittlungsschwellen vorsehen. Diese Übermittlungsschwellen unterscheiden sich nach dem Eingriffsgewicht, welches durch die Übermittlung ausgelöst wird. Dieses Eingriffsgewicht hängt auch davon ab, welche operativen Anschlussbefugnisse die empfangende Behörde hat.

Den nunmehr anstehenden Überarbeitungen des BVerfSchG und des MADG sowie des BNDG hinsichtlich der Übermittlungen kommt daher eine hohe Bedeutung zu – leider werden sie dieser nicht gerecht.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

2. Grundsätzliche systematische Fragestellungen zu Übermittlungen

a) Rückausnahme zu den Übermittlungsvorschriften im BNDG-E

§ 65 BNDG-E stellt eine offensichtliche Umgehung der vorab im Gesetzesentwurf vorgesehenen Übermittlungsvorschriften dar. Die Gesetzesbegründung zum BNDG-E lässt erkennen, dass den Vorgaben des BVerfG zur Übermittlung von mit unterschiedlichen Zwecken im Rahmen der strategischen Fernmeldeaufklärung erhobenen Daten grundsätzlich genüge getan werden soll. Das BVerfG hat für die strategische Ausland-Fernmeldeaufklärung zwischen Datenerhebungen zur Gefahrenfrüherkennung und zur politischen Unterrichtung unterschieden und sowohl die Erhebungs- als auch die Übermittlungsvoraussetzungen an unterschiedliche Vorgaben geknüpft. Daten, die zur politischen Unterrichtung der Bundesregierung ohne nennenswerte Erhebungsschwellen erhoben werden dürfen, sollen ausschließlich **zum Zweck der politischen Unterrichtung der Bundesregierung** verwendet werden. Das BVerfG (Urteil vom 19.05.2020, 1 BvR 2835/17, RN 160, 162, 223f., 228) führt dazu aus, dass „solche Berichte an die Bundesregierung [allein] der politischen Information auf Regierungsebene [dienen]. Die Versorgung der Bundesregierung mit Informationen für ihre außen- und sicherheitspolitischen Entscheidungen hilft ihr, um sich im machtpolitischen Kräftefeld der internationalen Beziehungen zu behaupten.“ Zudem sei die Nutzung „auf Entscheidungen der Bundesregierung selbst in Fragen der Außen- und Sicherheitspolitik beschränkt.“ Die Bundesregierung besteht aus dem Bundeskanzler und den Ministerinnen und Ministern. Der den Ministerien nachgeordnete Bereich ist nicht Teil der Bundesregierung im Sinne der vorgenannten Rechtsprechung. Mithin dürfen Daten, die zur politischen Unterrichtung der Bundesregierung erhoben wurden, nach der vom BVerfG zugelassenen Ausnahme nur dann an andere inländische (öffentliche) Stellen übermittelt werden, wenn „die Daten aus sich heraus eine unmittelbar bevorstehende Gefahr für Leib, Leben oder Freiheit, für lebenswichtige Güter der Allgemeinheit oder für den Bestand oder die Sicherheit des Bundes oder eines Landes erkennen lassen“ (RN 228). **§ 65 Abs. 2 S. 1 BNDG-E erfüllt diese Anforderungen nicht.** Nachdem in § 65 Abs. 1 S. 1 BNDG-E das Wort „Übermittlung“ durch „Weitergabe“ ersetzt wird, erklärt S. 2 die §§ 11 bis 11g bei der Unterrichtung inländischer öffentlicher Stellen zum Zweck der Information der Bundesregierung zur Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung für nicht anwendbar. Gleichzeitig erlaubt § 65 Abs.1 S. 2 BNDG-E eine Übermittlung personenbezogener Daten zur politischen Unterrichtung der Bundesregierung nicht mehr nur an das Bundeskanzleramt und die Bundesministerien, sondern ausdrücklich und ohne weitere Übermittlungsschwelle auch an „weitere inländische öffentliche Stellen“ und damit auch an den nachgeordneten Geschäftsbereich der Bundesministerien und dem Wortlaut nach sogar auch an eine Landesbehörde. Inwieweit Übermittlungen an nachgeordnete Behörden oder an Landesbehörden der politischen Information der Bundesregierung dienen, bleibt fraglich.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

b) Fehlende Konkretisierung der Übermittlungsschwellen hinsichtlich der Erkenntnisdichte

Die Forderung des BVerfG nach Übermittlungsschwellen, die auch Regelungen hinsichtlich der Verdichtung des Erkenntnisstandes, der bei den Nachrichtendiensten vorliegt, enthalten, wird in beiden Gesetzesentwürfen nicht erfüllt. Der Verfassungsschutz muss vor Übermittlung im Einzelfall eine Prüfung vornehmen, wie belastbar die dort vorliegenden Erkenntnisse sind, um dann die notwendige Einschätzung des Vorliegens einer konkretisierten Gefahr (bei Übermittlung an Gefahrenabwehrbehörden) bzw. den durch bestimmte Tatsachen begründeten Verdacht (bei Übermittlung an Strafverfolgungsbehörden) bzw. hinreichende tatsächliche Anhaltspunkte (bei Übermittlung an sonstige Behörden) zu treffen. Bezeichnend für die Vorfeldtätigkeit der Nachrichtendienste ist nach der Rechtsprechung des BVerfG nämlich auch, dass die weitgefassten Datenerhebungen losgelöst von jeder konkreten Rechtsgutgefährdung und teilweise auch von spezifischer Verantwortlichkeit der Betroffenen vorgenommen werden (Urteil vom 26. April 2022, RN 241). Ich vertrete daher, dass die **Übermittlung der Erkenntnisse für die Verwendung in einem konkreten Verfahren** gegen einen Betroffenen immer einer **Verhältnismäßigkeitsprüfung im Einzelfall** durch die Nachrichtendienste bedarf: Nicht jede durch die Nachrichtendienste durchgeführte Datenerhebung und daraus ergangene Speicherung in deren Systemen darf in eine Übermittlung münden, sondern der übermittelnde Dienst muss eine Überprüfung anstellen, ob die gespeicherten Fakten eine bestimmte Prognose tragen. Dies ist durch eine entsprechende gesetzlich normierte Übermittlungsschwelle sicherzustellen, die die Notwendigkeit einer solchen Einzelfallprüfung verdeutlicht.

c) Übermittlung von nicht nachrichtendienstlich erhobenen personenbezogenen Daten

§ 25d BVerfSchG-E regelt abweichend von den §§ 19ff BVerfSchG-E die Übermittlung von personenbezogenen Daten, die nicht mit nachrichtendienstlichen Mitteln erhoben wurden, dahingehend, dass diese unter lediglich der Voraussetzung „für sonstige erhebliche Zwecke der öffentlichen Sicherheit oder für sonstige erhebliche Interessen des Empfängers“ übermittelt werden dürfen. Dem Urteil des BVerfG vom 26. April 2022 lässt sich entnehmen, dass generell auch die **Trennung der Übermittlung in solche Erkenntnisse, die mit nachrichtendienstlichen Mitteln erhoben wurden, und solche, die ohne einen solchen Einsatz gesammelt wurden, nicht zulässig** ist. So führt das BVerfG in RN 238ff aus: „Aber auch nachrichtendienstliche Erkenntnisse, die aus für sich genommen jeweils weniger eingriffsintensiven Überwachungsmaßnahmen stammen, dürfen nur zum Schutz besonders hochwertiger Rechtsgüter übermittelt werden. Eine Differenzierung nach dem Eingriffsgewicht der jeweiligen Einzelmaßnahme kommt insoweit nach dem Kriterium der hypothetischen Datenneuerhebung nicht in Betracht (...). Denn durch die Betrachtung eines einzelnen, für sich genommen weniger eingriffsintensiven Datenerhebungsvorgangs würde die Grund-

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

rechtsbelastung, die von der breit angelegten, teils niederschwelligen Beobachtungstätigkeit nachrichtendienstlicher Behörden ausgeht, nicht in Gänze erfasst." Auch ist eine solche Trennung in der Praxis nicht möglich: Eine solche Unterscheidung würde voraussetzen, dass die Erkenntnisse, die mit nachrichtendienstlichen Mitteln erhoben wurden, entsprechend gekennzeichnet werden müssen, damit bei deren Übermittlung dann die höheren Voraussetzungen geprüft werden. Eine solche Kennzeichnungspflicht müsste auch nach der Vermischung mit anderen Daten und Informationen aufrechterhalten werden, um die in §§ 19 ff vorgesehenen Verwendungsbeschränkungen nicht zu unterlaufen, vgl. zum Themenkomplex bereits BVerfG zu G10, vgl. BVerfGE 100, 313 (386) = NJW 2000, 55 (67). Da ".... die Verfassungsschutzbehörden nicht so sehr Einzeldaten, sondern vielmehr analytisch aufbereitete und verdichtete Erkenntnisse übermitteln" (RN 239) wird von hier die Praktikabilität einer solchen Regelung angezweifelt.

d) Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen

§ 10a Abs. 1 S. 1 BNDG-E stellt für die Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen an andere Stellen auf die Erforderlichkeit zur Aufgabenerfüllung des BND oder der empfangenden Stelle ab. Das BVerfG hat zu der weitestgehend gleich ausgestalteten Regelung des § 24 BNDG a.F. bzw. des aktuellen § 11 Abs. 1 BNDG in der Entscheidung vom 19. Mai 2020 zur Ausland-Ausland-Fernmeldeaufklärung (Az.: 1 BvR 2835/17, RN 310 f.) festgestellt, dass das **Abstellen lediglich auf die jeweilige Aufgabenerfüllung mit dem Grundsatz der Normenklarheit und Bestimmtheit nicht vereinbar** ist.

§ 10a Abs. 2 BNDG-E regelt das Erfordernis höherer Übermittlungsschwellen für systematisiert erfasste oder zusammengeführte Daten aus allgemein zugänglichen Quellen. Durch das Erfordernis höherer Übermittlungsschwellen gibt der Gesetzgeber zu erkennen, dass er sich des erhöhten Eingriffsgewichts der systematischen Erfassung und der Zusammenführung dieser Daten bewusst ist. Das begrüße ich. **Eine spezifische Rechtsgrundlage für das systematische Erfassen und Zusammenführen öffentlich zugänglicher Daten vor deren Übermittlung fehlt indes**. Die allgemeine Ermächtigungsgrundlage ist für derartige Datenverarbeitungen unzureichend.

3. Regelungen zur Übermittlung an Nachrichtendienste

§ 11 BNDG-E stellt für die Zulässigkeit der Übermittlung personenbezogener Daten an inländische Nachrichtendienste auf die Erforderlichkeit zur Aufgabenerfüllung des BND oder der empfangenden Stelle ab. Auch wenn § 11 BNDG-E nicht wie § 10a Abs. 1 BNDG-E auf einen unbestimmten Empfängerkreis verweist, dürfte die Norm in der derzeitigen Ausgestaltung durch den **bloßen Verweis auf die jeweilige Aufgabenerfüllung** als alleinige Übermittlungsschwelle sowohl unter dem Gesichtspunkt der Normenklarheit und Bestimmtheit

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

(BVerfG aaO. RN 310f.) als auch unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes in seiner Konkretisierung durch das Kriterium der hypothetischen Datenneuerhebung einem **erhöhten verfassungsrechtlichen Risiko** ausgesetzt sein.

Die Übermittlungsvorschriften **§ 6 BVerfSchG und § 3 MADG**, die auch Übermittlungen an Nachrichtendienste regeln, werden im vorgelegten BVerfSchG-E überhaupt nicht korrigiert. Auch diese **verfehlen die Vorgaben des BVerfG**. Hierbei ist auch noch zu berücksichtigen, dass durch diese Vorschriften die Möglichkeit zur Nutzung einer gemeinsamen Datenbank geschaffen wird, das Nachrichtendienstliche Informationssystem (NADIS). Daher müssen diese Vorschriften auch hinsichtlich einer Regelung der umfänglichen Abrufmöglichkeiten aller beteiligten Behörden aus diesem System an die Rechtsprechung des BVerfG (vgl. dazu BVerfGE vom 16. Februar 2023 zur automatisierten Datenanalyse) angepasst werden.

4. Regelungen zur Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr

Das BVerfG fordert, dass für die Übermittlung durch Nachrichtendienste an eine Gefahrenabwehrbehörde eine wenigstens hinreichend konkretisierte Gefahr besteht. Die in **§ 19 BVerfSchG-E und § 11b BNDG-E** gewählte Formulierung „**einer Gefahr, die in bestimmter Art zu entstehen droht**“ und die dazu gehörigen Begründungen gehen an dem vom BVerfG geforderten Bestimmtheitsgrad vorbei und **senken die Anforderungen an eine Übermittlung zur Gefahrenabwehr zu stark ab**. Durch die anders gewählte Begrifflichkeit und die dazugehörige, sehr nebulöse Begründung (S. 19 „Das in Nr. 1 aufgenommene Tatbestandsmerkmal „in bestimmter Art“ umschreibt also, dass das prognostische Störungsgeschehen nur der Art nach konturiert sein muss, etwa gegen ein bestimmtes Rechtsgut gerichtet oder phänomenologisch umrissen, beispielsweise als terroristische Tat.“) besteht die Möglichkeit einer beliebig weiten Öffnung der Gesetzesauslegung weit in das Vorfeld einer Gefahr hinein.

Auch die Regelung des **§ 19 Abs. 1 Nr. 2 BVerfSchG-E** „**zur Verhinderung einer Straftat** …“ formuliert keinen klaren Gefahrengrad einer Straftatbegehung und bleibt damit hinter der Übermittlungsschwelle einer wenigstens konkretisierten Gefahr zurück.

§ 19 Abs. 3 BVerfSchG-E und **§ 11b Abs. 6 BNDG-E** sehen für bestimmte (Gefahren-) Konstellationen dann sogar Übermittlungspflichten vor – die gegenüber dem bisherigen Recht erweitert wurden. Insbesondere im BVerfSchG-E bleibt der **Anwendungsbereich solcher Übermittlungspflichten unklar**. Die in der Begründung vorgebrachte Verschiebung vom Gefahrenverdacht zum Störungsverdacht zu den Störungstatbeständen wie „Verletzung von Verfassungstreuepflichten“, Partei- oder Vereinsverboten irritiert: Auch zu diesen Tat-

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

beständen gilt, dass die angeblich eingetretene Störung zum Zeitpunkt der Informationssammlung durch die Nachrichtendienste noch in festgelegten Verfahren überprüft werden muss, von einer bereits festgestellten Störung daher nicht die Rede sein kann.

5. Regelungen zur Übermittlung an Strafverfolgungsbehörden

Gemäß Leitsatz 3b) des BVerfG-Urteils vom 26. April 2022 setzt eine Übermittlung an eine Strafverfolgungsbehörde voraus, „dass ein durch bestimmte Tatsachen begründeter Verdacht vorliegt, für den konkrete und verdichtete Umstände als Tatsachenbasis vorhanden sind." Das Vorliegen tatsächlicher Anhaltspunkte ist demnach nicht ausreichend. In RN 258 des o.g. Urteils verwendet das Gericht für diesen Grad der Erkenntnisverdichtung den Begriff der „hinreichenden tatsächlichen Anhaltspunkte" – wenn auch im Zusammenhang mit der Übermittlung an Stellen ohne operative Befugnisse. In **§ 21 Abs. 1 BVerfSchG-E** werden zwar als Verdachtsgrad „bestimmte Tatsachen" gefordert, die laut Gesetzesbegründung ein „mehr" zu den „tatsächlichen Anhaltspunkten" sind; der vom BVerfG verwendete **Begriff der „hinreichend tatsächlichen Anhaltspunkte" erscheint** mir jedoch klarer und daher **vorzugswürdig. Dringenden Änderungsbedarf** sehe ich bei **§ 11a Abs. 1 BNDG-E**, der lediglich das Vorliegen tatsächlicher Anhaltspunkte fordert. Unabhängig davon, dass dieser Verdachtsgrad nach der Rechtsprechung des BVerfG für die Übermittlung an Strafverfolgungsbehörden nicht ausreichend ist und daher aus meiner Sicht ein hohes verfassungsrechtliches Risiko birgt, ist nicht nachvollziehbar, warum der BNDG-E einen geringeren Verdachtsgrad vorsieht als die entsprechende Vorschrift im BVerfSchG-E**. Daher rege ich hinsichtlich des Verdachtsgrads dringend eine Angleichung des BNDG-E an das BVerfSchG-E an.**

Beide Gesetzesentwürfe sehen u.a. eine Übermittlung an Strafverfolgungsbehörden bei Straftaten mit einem Strafrahmen von bis zu fünf Jahren und dem Hinzutreten eines weiteren Qualifikationsmerkmals vor. Ich habe bereits in meiner Stellungnahme im Rahmen der Ressortbeteiligung deutlich gemacht, dass ich diese Vorschläge mittrage. Denn die strenge Anwendung der Rechtsprechung des BVerfG, nach der eine besonders schwere Straftat erst bei „einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe" vorliegt, würde in der Praxis dazu führen, dass die Nachrichtendienste zwar entsprechend ihrem jeweiligen Auftrag Informationen über bestimmte Staatsschutzdelikte oder deren geplanter Begehung sammeln, diese Erkenntnisse dann aber nicht an Strafverfolgungsbehörden übermitteln dürfen. Ich bin davon überzeugt, dass das BVerfG dies nicht gewollt haben kann, da sonst der Sicherheitsgewährleistungsauftrag des Staates gefährdet werden würde. Da diese Frage aber auch unter Juristen umstritten ist und die Äußerungen des Gerichts nicht eindeutig dafürsprechen, dass Straftaten mit einem Strafrahmen von drei bis zu fünf Jahren auf jeden Fall einbezogen werden können, weise ich ausdrücklich auf das verfassungsrechtliche Risiko, das diese Vorschläge bergen, hin.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Darüber hinaus möchte ich erneut auf die **Inkonsistenz** und die dadurch - selbst für Fachleute[5] - erschwerte Anwendung des **§ 21 BVerfSchG-E** in der Praxis aufmerksam machen. In § 21 Abs. 2 Nr. 2 ist beispielsweise § 83 Abs. 1 StGB nicht erwähnt, obwohl er neben dem Fall, der bereits unter Absatz 2 Nr. 1 fällt, auch den minder schweren Fall (bis zu fünf Jahren Freiheitsstrafe) enthält. Demgegenüber ist § 108e Absatz 1, der von der Systematik gleich aufgebaut ist, in den Katalog aufgenommen worden. Weder aus der Straftat an sich, noch aus der Gesetzesbegründung ist eine Erklärung für diese unterschiedliche Systematik erkennbar. Ebenfalls inkonsistent ist die Regelung in Bezug auf die Einbeziehung der Versuchsstrafbarkeit eines Delikts. § 109e Abs. 3 („Der Versuch ist strafbar“) ist in den Katalog aufgenommen worden, während die entsprechende Regelung bei anderen Delikten nicht gelistet ist (bspw. § 89 und 109 f). Im BVerfSchG wird in § 21 Abs. 2 lit. a folgerichtig nur § 109e Absätze 1 bis 3 und 5 aufgelistet.

Die inkonsistente Systematik wird in **§ 21 Abs. 2 Nr. 4 BVerfSchG-E** fortgeführt. Während in Buchst. a) und e) die Delikte selber aufgelistet sind, werden ansonsten nur die Abschnitte des StGB genannt und auf die zu schützenden Rechtsgüter abgestellt. Zwar betreffen die genannten Abschnitte „besonders gewichtige Rechtsgüter“ im Sinne der Rechtsprechung des BVerfG (vgl. Urteil vom 26. April 2022, RN 243), allerdings sind in den genannten Abschnitten auch immer Straftaten enthalten, deren Strafrahmen unter einer Freiheitsstrafe von bis zu fünf Jahren liegen (bspw. § 218 Abs. 1 oder § 240 StGB). Andererseits umfassen die Abschnitte auch Straftaten, die bereits unter Absatz 2 Nr. 1 fallen und für deren Übermittlung kein zusätzliches Qualifikationsmerkmal erforderlich ist (z.B. § 211 StGB). Dieses erschwert die praktische Anwendung der Norm. Aus Gründen der Normenklarheit und Bestimmtheit ist daher eine Nennung der einzelnen Vorschriften vorzugswürdig. Diesbezüglich **empfehle ich eine Angleichung an § 11a BNDG-E**, der sämtliche Straftaten auflistet. Unklar ist zudem, warum dem BND die Übermittlung von Erkenntnissen zu Straftaten gegen die sexuelle Selbstbestimmung (Dreizehnter Abschnitt des StGB) gemäß § 11a Abs. 1 Nr. 2 lit. dd sowie zu Straftaten gemäß §§ 275 Abs. 2 und 276 Abs. 2 jeweils in auch in Verbindung mit § 276a (§ 11a Abs. 1 Nr. 2 lit. gg) möglich sein soll, während diese Delikte im BVerfSchG-E nicht aufgelistet sind und dementsprechende Erkenntnisse vom BfV sowie BAMAD nicht übermittelt werden könnten. Selbiges gilt für Straftaten nach § 261 Absätze 1, 2 und 4, § 96 Abs. 1 Aufenthaltsgesetz und § 23 Abs. 4 Geschäftsgeheimnisgesetz, die im BND-G genannt sind, im BVerfSchG-E allerdings nicht. Auch wenn es sich bei den genannten Straftaten um Delikte handelt, die typischerweise durch Mitglieder der Organisierten Kriminalität begangen werden, für die das BfV und das BAMAD nicht zuständig sind, erklärt diese Tatsache allein nicht die unterschiedlichen Regelungen. Ich empfehle daher eine Angleichung der beiden Gesetzesentwürfe.

[5] DAV, Pressemitteilungen – Rechtspolitik PM 31/23, https://anwaltverein.de/de/newsroom/pm-31-23-nachrichtendienst-reform-law-and-order-statt-augenmass.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Darüber hinaus ist im Rahmen von **§ 21 BVerfSchG-E** das Verhältnis zwischen den Absätzen 1 und 2 auf der einen und Absatz 3 auf der anderen Seite unklar. Denn wenn der Bezug zu einer originären Aufgabe des Verfassungsschutzes (§ 3 Abs. 1) besteht, löst dies eine Übermittlungspflicht aus; dann ist aber der Anwendungsbereich insbesondere der Nrn. 3 und 4 des Absatzes 2 fraglich, die ja gerade auf die Aufgaben des Verfassungsschutzes gemäß § 3 BVerfSchG Bezug nehmen. Die Gesetzesbegründung gibt keinen Aufschluss über das Verhältnis der Absätze untereinander. **§ 11a BNDG-E**) regelt nur die Ermessensübermittlung, Pflichtübermittlungen gibt es nicht. **Insofern rege ich eine Angleichung des BVerfSchG-E an das BNDG-E an.**

Redaktionell ist im Hinblick auf das BVerfSchG-E anzumerken, dass auf S. 18/19 der Gesetzesbegründung ausgeführt wird, dass eine Übermittlungspflicht an Strafverfolgungsbehörden in § 21 S. 2 geregelt sei; diese Pflicht ist aber in § 21 Abs. 3 geregelt. Darüber hinaus wird auf S. 26 der Gesetzesbegründung die Negativabgrenzung zu den Straftaten mit einer Höchststrafe von 3 Jahren Freiheitsstrafe erwähnt und fälschlicherweise auf das Urteil des BVerfG vom 26. April 2022, RN 155 verwiesen. Diese Aussage des BVerfG findet sich aber im Beschluss vom 28. September 2022 unter RN 155.

6. Regelungen für sonstige Übermittlungen an inländische Stellen

Die Vorschriften der **§§ 20, 22 BVerfSchG-E sowie §§ 11b bis 11d BNDG-E** regeln in unterschiedlicher Form die Übermittlung an inländische öffentliche und nicht öffentliche Stellen. Eine exakte Vergleichbarkeit der Vorschriften ist fast unmöglich. Hier wird daher lediglich auf Einzelaspekte zu diesen Vorschriften eingegangen.

Kritisch sehe ich den Umfang, in dem nunmehr insbesondere nach den Vorgaben der §§ 20, 22 und in Teilen auch § 25a BVerfSchG-E **der Informationsfluss auch an private Stellen** möglich ist. Diese Möglichkeit ist nach der bisherigen Gesetzeslage in § 19 Abs. 4 BVerfSchG als absolute Ausnahme in besonderen Fällen vorgesehen mit besonderen Verfahrensregelungen (die hier nur zum Teil in § 25c Abs. 3 BVerfSchG-E aufgenommen werden), unter anderem auch mit einer (nachträglichen Information) an den Betroffenen. Dieses **Regel- Ausnahme-Verhältnis** (Verbot ist Regel, Übermittlung in besonderen Fällen nur ausnahmsweise) **wird nunmehr umgekehrt**. Diesseits wird bezweifelt, dass der für Übermittlungen notwendige Schutz von besonders gewichtigen Rechtsgütern überhaupt in einer Vielzahl von Fällen – die eine solche Änderung des Grundsatzes rechtfertigen könnte - durch private Stellen besorgt werden kann. Auf die Notwendigkeit einer nochmals vertieften Verhältnismäßigkeitsprüfung an private Stellen sei hingewiesen, vgl. hierzu z.B. BVerwG, Urteil vom 19. November 1997, AZ 1 C 25/95 zur fehlerhaften Übermittlung des BfV an einen privaten Arbeitgeber.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

§ 20 Ab. 2 BVerfSchGE schreibt eine Übermittlungspflicht bzgl. gesetzlich besonders geregelter Fälle vor, gemeint sind hier nach der Gesetzesbegründung Überprüfungen von Personen, in die die Erkenntnisse von Nachrichtendiensten Eingang finden wie beispielshaft die Vorschriften § 73 AufenthaltG, §§ 32, 37 StAG, § 7 LuftSiG, § 5 WaffG, § 34a GewO etc. **Nach meiner Ansicht bedürfen auch alle diese spezialgesetzlichen Vorschriften einer Überarbeitung und einer Anpassung an die Rechtsprechung des BVerfG**.

Redaktionell: In der Begründung zu § 20 Abs. 2 BVerfSchGE S. 25 geht der Verweis auf § 19 Abs. 4 Nr. 1 c) BVerfSchG-E fehl, es ist wohl § 19 Abs. 3 Nr. 1a) BVerfSchG-E gemeint.

Den Bedarf zur Übermittlung der nachrichtendienstlichen Erkenntnisse an andere Stellen als Hintergrundinformation oder zur Erstellung von Lagebildern und ähnlichem - wie in z.B. § 22 BVerfSchG-E und § 11b Abs. 2 BNDG-E vorgesehen - sehe ich. Kritisieren muss ich jedoch, dass nach Übermittlung der Daten durch die Nachrichtendienste eine Nicht-Verwendung der Informationen für weitere Maßnahmen kaum sichergestellt werden kann. Enge Verwendungsregelungen für die Verwendung für die wissenschaftliche Forschung wie § 21 BKAG oder § 476 StPO wären aufgrund der Sensibilität der Daten und der tiefen Grundrechtseingriffe bei der nachrichtendienstlichen Erhebung nach hiesiger Ansicht sehr wohl geboten. In der Begründung zu § 22 BVerfSchG-E wird auf S. 28 beschrieben, dass unter Abs. 3 Nr. 2 auch der allgemeine Austausch z.B. mit der FIU fallen soll. Die FIU ist nach GwG grundsätzlich zur Übermittlung strafrechtlich relevanter Informationen an die Strafverfolgungsbehörden verpflichtet. Würde sie nach § 22 Abs. 3 Nr. 2 BVerfSchG-E personenbezogene Daten vom BfV erhalten, die Hinweise auf Geldwäschestraftaten enthalten, die das BfV aber nur wegen des Zwecks der besseren künftigen Abstimmung übermittelt hat, bliebe offen, wie die FIU mit dem Verbot der Weiterverwendung umgehen soll. Sie hat die gesetzliche Pflicht zur Übermittlung an Strafverfolgungsbehörden nach GwG, aber gleichzeitig das Verbot der Weiterwendung nach § 22 Abs. 3 Satz 2 BVerfSchG. Es ist unklar, wie dieses Dilemma aufgelöst werden soll.

§ 11b BNDG-E regelt die Übermittlung personenbezogener Daten an inländische öffentliche Stellen und damit auch die Übermittlung an die Bundeswehr, konkret auch an Stellen des Militärischen Nachrichtenwesens. Weder in § 11b BNDG-E noch in der Gesetzesbegründung wird das Militärische Nachrichtenwesen konkret genannt. Da die Tätigkeit des Militärischen Nachrichtenwesens nicht einfachgesetzlich normiert ist, dieses jedoch ähnlich einem Nachrichtendienst personenbezogene Daten verarbeitet, **fehlt es an einer Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten durch Stellen des Militärischen Nachrichtenwesens**. Dies habe ich im vergangenen Jahr förmlich beanstandet. Die Schaffung einer einfachgesetzlichen Regelung für das Militärische Nachrichtenwesen ist dringend angezeigt.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

§ 11b Abs.1 S.3 BNDG-E verstößt gegen das Gebot der Normenklarheit. Die Vorschrift regelt, dass andere Rechtsvorschriften, die die Übermittlung personenbezogener Daten durch den BND an inländische öffentliche Stellen vorsehen, unberührt bleiben. Welche Rechtsvorschriften hierunter fallen, bleibt unklar. Die Aufzählung von Beispielen in der Gesetzesbegründung zu § 11b Abs.1 S.1 BNDG-E ist nicht abschließend.

7. Regelungen zum Übermittlungsverbot, § 23 BVerfSchG-E

Die von mir unter Punkt II.2b) kritisierte unvollständige Prüfung der Verdichtung des Erkenntnisstandes soll nach Aussagen im Rahmen der Ressortabstimmung in der Verhältnismäßigkeitsprüfung des § 23 Nr. 2 BVerfSchG-E erfolgen, insbesondere unter dem Punkt Nr. 2b) „Wertigkeit“. Nach der Gesetzesbegründung ist dies auch unter Nr. 2d) „drohender, insbesondere verdachtsgegründeter Anschlussmaßnahmen“ zu fassen, die Gesetzesbegründung sieht das Risiko aber schon im jeweiligen Fachrecht abgefangen („Eingriffe bereits mit Verdachtserkenntnissen zu rechtfertigen“). Auch in der Vorschrift § 9e BNDG-E ist die von mir geforderte Prüfung nicht ausreichend gesetzlich abgesichert. Aus meiner Sicht gehören diese Punkte bereits in die Übermittlungsschwellen.

Der Sinn von § 23 Nr. 4 BVerfSchG-E erschließt sich nicht. Er ist offenbar eine Rückausnahme vom Übermittlungsverbot und passt daher nicht unter die Überschrift. Auch die Begründung (S. 29) hilft nicht weiter. Es wird abstrakt von Dienstleisterrolle“ (wohl des BfV) und „Bedarfsträgerinteressen“ (wohl Polizei und Strafverfolgung) gesprochen. Es kann allenfalls erahnt werden, dass der Vorwurf entkräftet werden soll, der Verfassungsschutz würde zum Wahrung seiner eigenen Interessen (z.B. laufende Observation oder V-Person-Einsatz) die Begehung von Straftaten nicht übermitteln. Ich verweise auf das verfassungsrechtliche Risiko, weil damit Straftaten übermittelt werden, die im Höchstmaß nicht mit einer Strafe von 10 Jahren bedroht sind und damit unklar ist, ob sie besonders schwere Straftaten nach der Rechtsprechung des BVerfG darstellen.

8. Minderjährigenschutz, § 24 BVerfSchG-E

Die Vorschrift zum Minderjährigenschutz in Bezug auf Übermittlungen zieht lediglich eine Altersgrenze bei den unter 14-jährigen, parallel zu der Rechtsgrundlage für die Speicherung gemäß § 11 Abs. 1 S. 1 BVerfSchG. Nur für diese Personengruppe finden die gesteigerten Voraussetzungen des § 24 BVerfSchG-E für eine Übermittlung Anwendung. Ein weiterer, ggf. gestaffelter Schutzmechanismus für die Übermittlung personenbezogener Daten minderjähriger Personen ab 14 Jahren fehlt. Eine **weitere Differenzierung** ist aus hiesiger Sicht aufgrund des besonderen Schutzbedürfnisses minderjähriger Personen **erforderlich.** Auch die Vorschrift des § 9g BNDG-E lässt eine weitergehende Staffelung der Altersgrenzen vermissen.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

In Bezug auf die Systematik fällt die **Zersplitterung der Vorschriften** zu den minderjährigen Personen auf. Durch die allgemeine Überschrift „Minderjährigenschutz“ in dem Abschnitt der Übermittlungen wird dem Gesetzesanwender suggeriert, dass es sich um eine zentrale Vorschrift zum Schutz minderjähriger Personen handelt, unabhängig an welche Behörde übermittelt wird. In § 25a Abs. 4 Satz 2 BVerfSchG-E findet sich jedoch eine Spezialregelung für die Fälle einer Übermittlung an ausländische Stellen. Eine gesetzliche Klarstellung könnte beispielsweise durch einen Zusatz in der Überschrift erfolgen: „Minderjährigenschutz bei Inlandsübermittlungen“ oder durch einen Verweis auf die Regelung des § 25a Abs. 4 Satz 2 BVerfSchG-E. Eine solche Klarstellung findet sich inzwischen im BNDG-E in der Überschrift zu **§ 9g BNDG-E,** die lautet: „Schutz von minderjährigen Personen bei Übermittlungen an inländische Stellen“. **Diese klarstellende Änderung würde ich auch im BVerfSchG begrüßen.**

9. Weiterverarbeitung durch den Empfänger, § 25 BVerfSchG-E

Bei der Möglichkeit einer pauschalen Zustimmung des BfV nach § 25 Abs. 2 Satz 1 Nr. 2 BVerfSchG-E in Bezug auf „eine Reihe gleichgelagerter Fälle“ wären Beispiele zur Erläuterung hilfreich. Ohne diese vermag ich das Risiko, das im Verzicht auf eine Einzelfallentscheidung liegt, nicht abzuschätzen. Einen solchen Ausnahmetatbestand sieht beispielsweise in § 9a BNDG-E, der ebenfalls den Grundsatz der Zweckbindung regelt, nicht vor.

In Bezug auf die Gesetzesbegründung zu Abs. 2 (S. 30) möchte ich darauf hinweisen, dass eine einfache Sachbeschädigung gem. § 303 StGB keine besonders schwere Straftat im Sinne der Ausführungen des BVerfG ist (siehe meine Ausführungen zu § 21). Die strengen Voraussetzungen des BVerfG für Datenübermittlungen des BfV an eine Strafverfolgungsbehörde, die in § 21 Niederschlag finden müssen, dürfen hierüber nicht ausgehebelt werden. Auch wenn es sich für eine Strafverfolgungsbehörde für die konkrete Strafzumessung um ein strafrechtlich relevantes Delikt handelt, dürfen Informationen dazu nur übermittelt werden, wenn es sich gleichzeitig um ein Delikt handelt, das von § 21 BVerfSchG-E umfasst ist. Es dürfen nicht über die „strafrechtliche Würdigung einer Tat“ Daten zu Delikten übermittelt werden, deren Übermittlung nach § 21 BVerfSchG-E ausgeschlossen sind.

Ergänzend schlage ich vor, die Ausführungen in der Begründung in den Gesetzestext aufzunehmen: „Entsteht nachträglich eine Gefahr im Sinne des § 20 Absatz 1 (bzw. werden die gefahrbegründenden Informationen nachträglich bekannt) kann mithin im Wege der Zustimmung nach § 25 Absatz 2 Satz 1 Nummer 2 der Ausschluss einer Weiterverarbeitung zur Zwangsausübung aufgehoben werden“. Diese Aussage kann dem bisherigen Wortlaut nicht entnommen werden.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

In Bezug auf den Abs. 2 Satz 4 gehe ich davon aus, dass das Auskunftsverlangen des BfV sowie die darauf ergehende Antwort des Empfängers von den allgemein geltenden verwaltungsrechtlichen Dokumentationspflichten abgedeckt ist, sodass eine dahingehende gesetzliche Klarstellung entbehrlich sein dürfte. **Ein entsprechender Hinweis auf die Dokumentation dieses Prozesses wäre aus hiesiger Sicht in der Gesetzesbegründung zu begrüßen.**

Die **Erweiterung des Auskunftsrechts** gemäß § 25 Abs. 3 BVerfSchG-E wird von hier begrüßt, **sie sollte jedoch für alle Anwendungsbereiche von Übermittlungen durch eine entsprechende Streichung im § 15 Abs. 3 BVerfSchG ausgedehnt werden**. Den Geheimhaltungsbedürfnissen kann dann wie gewohnt gemäß der Regelung des § 15 Abs. 2 BVerfSchG Rechnung getragen werden.

10. Übermittlung zum Schutz der betroffenen Person, § 25b BVerfSchG-E

Die Struktur des § 25b Satz 1 BVerfSchG-E ist verbesserungsbedürftig. Erst durch die Gesetzesbegründung wird das Verhältnis zu § 8 Abs. 1 Satz 1, 2. Halbsatz BVerfSchG-E herausgestellt, wonach vorrangig der tatsächliche Wille der betroffenen Person abgefragt werden muss und nur für den Ausnahmefall des § 25b Satz 1 BVerfSchG-E die Einwilligung nicht eingeholt werden muss, sondern auf das mutmaßliche Interesse der betroffenen Person abgestellt werden kann. **Der § 9h Abs. 1 BNDG-E enthält beispielsweise eine deutlich normenklarere Struktur.**

Der Satz 2 ist lex specialis und stellt im Gegensatz zu Satz 1 bei nicht auf den mutmaßlichen Willen der betroffenen Person ab. Eine Übermittlung ist nur zu dem konkreten Zweck, wie der im Wortlaut genannten Jugendhilfe, erlaubt. Problematisch ist, dass die Zwecke nicht abschließend aufgelistet sind. Durch das Wort „insbesondere“ wird deutlich, dass auch andere Zwecke als die Jugendhilfe für eine Übermittlung denkbar sind. Die Gesetzesbegründung nennt jedoch ebenfalls lediglich den gesetzlich normierten Fall der Jugendhilfe. Zumindest in der Gesetzesbegründung sollten darüberhinausgehende denkbare Anwendungsfälle aufgelistet werden. **Sofern die Jugendhilfe als einziger Anwendungsfall für den Satz 2 in Frage kommt, empfehle ich das Wort „insbesondere“ zu streichen.**

Vor allem der Satz 2 dürfte in der Praxis überwiegend dem Schutz minderjähriger Personen dienen, sodass auch insofern die Gesetzessystematik mit Blick auf den § 24 fraglich erscheint, der mit seiner Überschrift „Minderjährigenschutz“ und ohne Verweis auf die hiesige Vorschrift einen abschließenden Charakter suggeriert.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

11. Weitere Verfahrensregelungen

Zunächst ist aus dem Zusammenspiel des Wortlauts des § 25c Abs. 1 BVerfSchG-E und der Gesetzesbegründung fraglich, ob teilweise die Begrifflichkeiten der Protokollierung mit der der Dokumentation synonym verwendet wurden. Beispielsweise wird in der Gesetzesbegründung zu Absatz 1 ausgeführt, dass sich die Protokollierungspflicht auch auf mündliche Auskünfte beziehe. In diesem Zusammenhang stellt sich die Frage, wie eine Protokollierung von mündlichen Auskünften in der Praxis erfolgt und ob hier nicht vielmehr eine Dokumentation in der Akte gemeint ist, deren Eintrag wiederum von den fachlichen Systemen protokolliert wird. Ausführungen zu der konkreten Umsetzung lässt die Gesetzesbegründung vermissen.

Aus hiesiger Sicht ist anzumerken, dass eine datenschutzrechtliche Bewertung in Bezug auf die Rechtmäßigkeit der Übermittlungen allein anhand der Protokolldaten nicht möglich sein wird, wenn ausschließlich der Empfänger, die Rechtsgrundlage sowie der Zeitpunkt der Übermittlung und nicht hingegen der Grund der Übermittlung protokolliert werden. Für eine Kontrolle müssen dann immer auch die Akten oder deren Protokolldaten hinzugenommen werden, die aufgrund der allgemein geltenden Speicher- und Löschfristen parallel vorhanden sein müssen.

In der Gesetzesbegründung zu § 9b BNDG-E wurde auf meine Anregung hin der Zusatz aufgenommen, dass die Protokollierung nach § 9b BNDG-E nicht die Dokumentation der Übermittlungen ersetzt. Eine solche ausdrückliche Klarstellung fordere ich auch in Bezug auf den § 25c BVerfSchG.

Ich weise darauf hin, dass im BNDG-Entwurf in § 9b Abs. 2 die Frist nach Ablauf des zweiten Kalenderjahres enden soll, also länger ist als im BVerfSchG. Ich rege eine einheitliche Frist für alle Nachrichtendienste des Bundes an. Aus Kontrollsicht wäre eine Frist wie im BNDG-E vorgesehen sinnvoll, um eine effektive Kontrolle gewährleisten zu können.

Bei der Möglichkeit einer pauschalen Zustimmung des BfV nach § 25c Abs. 3 S. 2 BVerfSchG-E in Bezug auf „eine Reihe gleichgelagerter Fälle“ wären Beispiele zur Erläuterung hilfreich. Ohne diese vermag ich das Risiko, das im Verzicht auf eine Einzelfallentscheidung liegt, nicht abzuschätzen. Aus Klarstellungsgründen soll vor dem Wort „Zustimmung“ jeweils das Wort „vorherige“ ergänzt werden.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

III. Datenschutzrechtliche Kritik an den Regelungen zur Eigensicherung

1. Einleitung zu den Eigensicherungsregelungen

Grundsätzlich rege ich an, dass der Gesetzgeber **einheitliche Regelungen für alle im Sicherheitsüberprüfungsverfahren** nach § 2 Abs. 2 und 3 SÜG **mitwirkenden Behörden** (BfV, BAMAD, BND) schafft, die ein besonderes Bedürfnis haben, ihre Verschlusssachen und Funktionsfähigkeit im Rahmen der Eigensicherung effektiv zu sichern. Der effektive Schutz von Verschlusssachen funktioniert nur in der Zusammenschau zwischen personeller und materieller Sicherheit. Mit Blick auf die beiden Gesetzesentwürfe zum BNDG und BVerfSchG muss hervorgehoben werden, dass sich die neu einzuführenden Regelungen zur Eigensicherung und zum Verschlusssachenschutz im Hinblick auf wesentliche Reglungen zur Datenverarbeitung nicht unwesentlich voneinander unterscheiden.

Die datenschutzrelevanten Abweichungen zwischen beiden Gesetzesentwürfen betreffen (a) die offene Videoüberwachung, (b) Kennzeichnungspflicht, (c) Aufbewahrungs- und Löschpflichten, (d) Zweckbindung, (e) die Protokollierung personenbezogener Daten, die aus den Eigensicherungsmaßnahmen gewonnen werden, (f) die Dauer der Anordnung von Maßnahmen, (g) das Anwesenheitsrecht betroffener Personen und (h) den Minderjährigenschutz. Es gibt keine erkennbare Rechtfertigung für eine ungleiche Regelungslage.

2. Im Einzelnen zu den datenschutzrelevanten Abweichungen

(a) Offene Videoüberwachung

Beide Gesetzesentwürfe lassen eine offene optisch-elektronische Überwachung zur Eigensicherung zu (vgl. **§ 65c Abs. 2 BNDG-E, § 26b Abs. 6 BVerfSchG-E**), aber zugleich wesentliche gesetzgeberische Vorgaben an Umfang und Durchführung vermissen**. Es bedarf jeweils einer Speicherfrist und Zweckbegrenzung sowie einer Pflicht zur Kenntlichmachung der Maßnahme**. Insoweit sind beide Gesetzentwürfe nachzubessern.

Nach den vorgeschlagenen Regelungen sind die Voraussetzungen, das Verfahren und die Grenzen der Überwachung jeweils in einer Dienstvorschrift zu regeln. Ich halte es für höchst bedenklich, dass die Entwürfe, abgesehen von der Klarstellung, dass eine Überwachung höchstpersönlicher Räume unzulässig ist, keine weiteren Vorgaben aufstellen. Insbesondere das Fehlen von klaren Speicherfristen bewerte ich als unzulässig. Einschränkungen in das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und erkennbar ergeben und die damit dem rechtsstaatli-

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

chen Gebot der Normenklarheit entspricht. Der Gesetzgeber muss insbesondere entscheiden, wie lange die erhobenen Daten gespeichert werden dürfen. Eine Dienstvorschrift ist hierfür völlig unzureichend. Dies gilt schon deshalb, weil zwar überwiegend nur Beschäftigte der jeweiligen Nachrichtendienste von den Maßnahmen betroffen sein werden, sich jedoch auch Dritte (z.B. Beschäftigte von Fremdfirmen oder anderen Behörden) im Eigensicherungsbereich des jeweiligen Nachrichtendienstes aufhalten können. Diese Personen können Voraussetzungen und Umfang der Grundrechtsbeschränkung aus einer internen Dienstvorschrift nicht entnehmen.

Eine gesetzliche Speicherbegrenzung ist also zwingend erforderlich und entgegen der in den Ressortberatungen vertretenen Auffassung auch praktikabel. Der Gesetzgeber sieht bereits an anderen Stellen gesetzliche Speicherfristen für verdachtsunabhängige Überwachungen vor (vgl. u.a. § 27 Satz 3 BPOLG, § 27a Abs. 4 S. 1 BPOLG). § 4 Abs. 5 BDSG spricht von einer unverzüglichen Löschung, wenn die Daten zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der betroffenen Personen einer weiteren Speicherung entgegenstehen. Hier werden in der Regel 72 Stunden angenommen (siehe dazu DSK, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, S. 22f.).

Die Vorgabe, dass die Videoüberwachung kenntlich zu machen ist, wurde im Verlauf der Ressortberatungen aus dem BNDG-E gestrichen. Dies ist nicht nachvollziehbar. **Die Transparenz ist essentiell für eine offene Überwachungsmaßnahme** (vgl. § 4 Abs. 2 BDSG). Erforderlich ist, dass die Überwachung für die betroffenen Personen ohne weiteres wahrnehmbar ist. Die Wahrnehmung der Überwachungstechnik selbst ist dafür nicht ausreichend.

Zusätzlich ist **für BfV und BAMAD eine enge Zweckbegrenzung für die Verarbeitung der entsprechenden Daten** vorzusehen (vgl. Ziff. 4).

(b) Kennzeichnungspflicht

Anders als für den BND in § 65g Abs. 1 Satz 2 BNDG-E ist für das BfV und das BAMAD keine **Kennzeichnungspflicht** für personenbezogene Daten vorgesehen, die im Rahmen von Eigensicherungsmaßnahmen erhoben worden sind. Nur eine solche Kennzeichnung erlaubt jedoch die eindeutige Zuordnung der personenbezogenen Daten und ist Voraussetzung für die Beachtung weiterer datenschutzrechtlichen Verpflichtungen (z.B. Zweckbindung und Lösch-verpflichtung). Eine Abweichung zwischen den verschiedenen nachrichtendienstlichen Regelungen kann nicht nachvollzogen werden. **Demnach empfehle ich eine Angleichung an den BNDG-E**.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

(c) Aufbewahrungs- und Löschpflichten

Allein der Entwurf zum BND sieht Regelungen zur Aufbewahrung und Löschung personenbezogener Daten vor, die im Zusammenhang mit Eigensicherungsmaßnahmen erhoben worden sind (**§ 65g Abs. 2 BNDG-E**). Diese sind bis zum Ablauf des Kalenderjahres aufzubewahren, das auf das Kalenderjahr der Erhebung folgt. Nach Ablauf der Aufbewahrungsfrist sind die Daten unverzüglich und unwiederbringlich zu löschen, es sei denn, die Daten sind für den Schutz des BND (Mitarbeitende, Einrichtungen, Gegenstände und Quellen) gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten oder für die Sicherheitsüberprüfung von Personen, die für den BND tätig sind oder tätig werden sollen erforderlich. Gemäß § 65g Abs. 2 Satz 3 BNDG-E dürfen die Daten ebenfalls nicht gelöscht werden, solange und soweit die Daten für eine gerichtliche Nachprüfung der Rechtmäßigkeit erforderlich sind.

Klare Aufbewahrungs- und Löschregelungen sind aus datenschutzrechtlicher Sicht zwingend erforderlich. Aus diesem Grund ist nicht nachvollziehbar, warum vergleichbare Regelungen für das BfV und das BAMAD nicht vorgesehen worden sind. Ein pauschaler Verweis auf allgemeine datenschutzrechtliche Grundsätze, insbesondere dem Grundsatz der Erforderlichkeit, ist aus hiesiger Sicht nicht ausreichend. Mangels klarer Zweckbestimmung wird es im Einzelfall nicht immer möglich sein, die Erforderlichkeit der weiteren Datenverarbeitung festzustellen.

Insoweit empfehle ich eine Angleichung an den BNDG-E, allerdings mit einer weiteren Anpassung. Die gem. § 65g Abs. 2 BNDG-E vorgesehene Speicherfrist erscheint zu lang und im Einzelfall unverhältnismäßig. **Ich empfehle, hier keine starre Frist zum Ablauf des Kalenderjahres vorzugeben, sondern eine Frist ab Erstellung und somit Durchführung der Maßnahme.** Ansonsten divergiert die Speicherdauer ohne sachlichen Grund zwischen eins und zwei Jahren. Hier sollte eine einheitliche Frist normiert werden. **Ich rege an, die Frist in beiden Gesetzen auf sechs Monate festzulegen.**

(d) Zweckbindung

§ 65g Abs. 3 Satz 1 BNDG-E sieht eine Zweckbindung für die personenbezogenen Daten vor, die im Rahmen der Eigensicherung generiert worden sind. Eine Weiterverarbeitung darf nur zum Zwecke des Schutzes des BND gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten oder für die Sicherheitsüberprüfung von Personen, die für den BND tätig sind oder tätig werden sollen, erfolgen. § 65g Abs. 3 Satz 2 BNDG-E verkürzt die Prüffrist des § 7 BNDG auf sechs Monate.

Die sehr weitgehenden Datenerhebungsbefugnisse in den §§ 65b bis 65d BNDG-E können nur dadurch rechtfertigt werden, wenn sichergestellt wird, dass die Daten nicht zu anderen

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

sachfremden Zwecken verarbeitet werden. **Demnach ist die Zweckbindungsvorschrift im BNDG-E zu begrüßen. Nicht nachvollziehbar ist die dahingehende Abweichung für das BfV und BAMAD. Eine Angleichung dieser Bestimmungen ist dringend empfohlen**. Der pauschale Verweis auf allgemeine datenschutzrechtliche Grundsätze erachte ich als nicht ausreichend.

(e) Protokollierung

Der BNDG-E enthält in **§ 65 k Vorgaben zur Protokollierung**. Danach hat der BND die Erhebung, Veränderung, Abfrage sowie Löschung personenbezogener Daten aus Maßnahmen nach den §§ 65b bis 65d (Kontrolle und Durchsuchung von Personen, Taschen und Fahrzeugen, Kontrolle und Durchsuchung von Räumen, IT-Kontrollen), die in automatisierten Dateien verarbeitet werden, zu protokollieren. Bei Daten, die den Kernbereich privater Lebensgestaltung berühren, hat der BND zusätzlich auch den Grund der Löschung zu protokollieren. Die Speicherfrist der Protokolldaten ist dabei nach § 65 k Abs. 3 Satz 1 BNDG-E bis zum Ablauf des zweiten Kalenderjahres, das auf das Kalenderjahr der Protokollierung folgt, begrenzt. **Das BVerfSchG-E enthält keine entsprechende Regelung**. Es regelt in § 26c Abs. 6 Sätze 5 bis 7 BVerfSchG-E lediglich die Dokumentation der Erlangung und Löschung von Daten, die den Kernbereich privater Lebensgestaltung berühren, gibt dabei aber eine kürzere Speicherfrist von maximal 6 Monaten vor.

Die Protokollierung der Datenverarbeitung hat grundsätzlich den Zweck, eine Kontrolle zu ermöglichen, ob die verantwortliche Stelle personenbezogene Daten innerhalb der materiell-rechtlich zulässigen Grenzen bzw. Zwecke verarbeitet. Diese Kontrolle ist für BfDI nur möglich, wenn die Datenverarbeitung revisionssicher protokolliert wird. Die Protokolldaten müssen darüber Auskunft geben können, wer (oder was) wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Nur auf diese Weise ist es möglich, im Rahmen einer Datenschutzkontrolle den Weg der Daten nachzuvollziehen. Ebenfalls kann nur auf diese Weise sichergestellt werden, dass Datenlöschungen nachvollzogen werden können. Verarbeitet eine Sicherheitsbehörde personenbezogene Daten, greift dies in die Grundrechte der betroffenen Personen ein. Protokollierung soll diesen Grundrechtseingriff abmildern und ist deshalb eine verfahrenssichernde Maßnahme. Aus diesem Grund sollte aus meiner Sicht zwingend **in das BVerSchG-E eine vergleichbare Regelung aufgenommen werden und nicht nur für den Fall der Betroffenheit des Kernbereichs privater Lebensführung.**

Ich begrüße auch die Klarstellung in **§ 65 k Abs. 2 Satz 3 BNDG-E**, dass die Protokolle der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen ihrer oder seiner Zuständigkeit nach § 63 zur Verfügung zu stellen sind und **rege an, die Klarstellung auch im BVerfSchG-E aufzunehmen.**

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

(f) Dauer der Anordnung von Maßnahmen

Beide Gesetzesentwürfe enthalten Vorgaben zur Anordnung von Maßnahmen der Durchsuchung von Personen, Taschen und sonstigen Gegenständen sowie Fahrzeugen, der Sicherstellung von Gegenständen insbes. IT-Kontrollen und der offenen optisch-elektronischen Überwachung des Eigensicherungsbereichs. Dies ist als Instrument zur Wahrung der Betroffenenrechte grundsätzlich zu begrüßen. Im Gegensatz zum BVerfSchG-E enthält der BNDG-E darüber hinaus eine Anordnungspflicht bei der Raumdurchsuchung und eine Begrenzung auf maximal 6 Monate im Falle der Anordnung von verdachtsunabhängigen Raumkontrollen zum Auffinden von Geräten der Informations- und Kommunikationstechnik (§ 65e Abs. 1 Satz 4 BNDG-E). Das BMI sah keine Notwendigkeit zur **Regelung verdachtsunabhängiger Raumkontrolle**n beim BfV und MAD, sondern sieht dies vom Hausrecht des BfV bzw. MAD abgedeckt. Dem kann ich nicht beipflichten.

Bei Maßnahmen, die auf das Hausrecht gestützt werden, sind Umfang und Grenzen der Datenverarbeitung nicht klar geregelt. Beispielsweise kann dadurch das Durchführen stichprobenartiger Raumkontrollen zur Aufrechterhaltung des Dienstbetriebes, keinesfalls aber ein permanenter Überwachungsdruck für die Mitarbeitenden gerechtfertigt werden. Deshalb und aufgrund des Parlamentsvorbehalts bedarf es für Raumkontrollen zum Zwecke der Eigensicherung und des Verschlusssachenschutzes einer eindeutigen Regelung im Hinblick auf Häufigkeit, Dauer sowie der Pflicht zur vorherigen Anordnung auf Gesetzesebene. Die Regelungen im BNDG-E sind hier vorzugs-würdig, zumal der Gesetzestext des BVerfSchG-E sehr leicht den Eindruck beim BfV- bzw. MAD-Mitarbeitenden erwecken kann, dass (Büro-) Raumkontrollen überhaupt nicht stattfinden.

(g) Anwesenheitsrecht

Beide Gesetzesentwürfe regeln ein Anwesenheitsrecht der betroffenen Person. Dies ist als Ausgestaltung der Betroffenenrechte ausdrücklich zu begrüßen, sollte aber auch hier für alle inländischen Nachrichtendienste gleich ausgestaltet werden. Unterschiede bestehen laut der vorliegenden Entwürfe hinsichtlich der Durchsuchung von Gegenständen, die nicht von Personen mitgeführt werden. Dieser Sachverhalt ist nicht von § 26b Abs. 2 Nr. 2 BVerfSchG-E erfasst, sondern vielmehr in § 26 b Abs. 4 geregelt, für den § 26c Abs. 4 kein Anwesenheitsrecht vorsieht. Praktische Relevanz hat dies beispielsweise bei der Durchsuchung von Gegenständen im Büro des Mitarbeitenden. Der BNDG-E sieht nach **§ 65f Abs. 5** ein Anwesenheitsrecht der betroffenen Person vor. Gründe für eine unterschiedliche Ausgestaltung sind nicht ersichtlich. **Deshalb sollte hier die betroffenenfreundlichere Regelung des BNDG-E für BfV und BAMAD übernommen werden**.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

(h) Minderjährigenschutz

§ 65 j BNDG-E enthält klare Weiterverarbeitungsschranken hinsichtlich der durch die Eigensicherungsmaßnahmen erhobenen personenbezogener Daten Minderjähriger, die im BVerfSchG-E für das BfV und den MAD gänzlich fehlen. Die Regelungslücke wird auch nicht durch die Übermittlungsvorschrift in § 24 BVerfSchG-E bzw. § 7 MADG aufgefangen.

Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind (so auch der Wortlaut des Erwägungsgrundes 38 der DSG-VO). Gerade bei der Sicherstellung und Spiegelung von Telekommunikationsendgeräten ist nicht auszuschließen, sondern in vielen Fällen sogar sehr wahrscheinlich, dass personenbezogene Daten von Kindern und Jugendlichen in großem Umfang erhoben und weiterverarbeitet werden. Beispielhaft sei hier an Kinderfotos auf dem Mobiltelefon zu denken. **Daher begrüße ich die Einschränkung im BNDG-E und fordere eine entsprechende Regelung für alle inländischen Nachrichtendienste gleichermaßen.**

IV. Datenschutzrechtliche Kritik zu weiteren Vorschriften des BVerfSchG-E

Die Frist zur Aufbewahrung von Protokolldaten aus dem NADIS soll (verkürzt gesagt) von zwei Jahren auf fünf Jahre hochgesetzt werden, so **§ 6 Abs. 3 Satz 5 BVerfSchG-E.** Begründet wird dies u.a. mit der Eigensicherung. Im BNDG-E, welches ebenfalls diesem Ziel dient, ist keine Anhebung der Aufbewahrungsfrist von Protokolldaten vorgesehen, weder speziell bei der Übermittlung (§ 9b Abs. 2 – nach Ablauf des zweiten Kalenderjahres) noch bei Maßnahmen zur Eigensicherung (§ 65k Abs. 2 – nach Ablauf des zweiten Kalenderjahres). Warum hier unterschiedliche Aufbewahrungsfristen gewählt werden, ist nicht nachvollziehbar, zumal jedenfalls nach medialem Kenntnisstand der BND zuletzt mehr mit Innentätern zu kämpfen hatte als das BfV. Ich verschließe mich dieser **Verlängerung** nicht grundsätzlich, sie **müsste** aber aus meiner Sicht **für alle Nachrichtendienste einheitlich** sein.

Problematisch wird bei einer Hochsetzung der Aufbewahrungsfrist die **sehr weite Vorschrift § 6 Abs. 3 S. 4 zur möglichen Verwendung der Protokolldaten**: Diese sieht eine Verwendung für die Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage vor. Diese an sich schon ungewöhnliche Regelung zur Nutzung der Protokolldaten birgt nunmehr aufgrund der langen Aufbewahrungsfrist ein gesteigertes Risiko, dass eigentlich (rechtmäßig) gelöschte Daten wieder rekonstruiert werden könnten. Dem sollte vorgebeugt werden, indem eine **verpflichtende Einschaltung der Datenschutzbeauftragten im Gesetz** mit vorgesehen wird.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

In diesem Zusammenhang wird seitens BfDI im Übrigen erneut auf die Notwendigkeit einer ausdrücklichen Regelung im Zusammenhang mit den sog. **Löschmoratorien** aufgrund von Parlamentarischen Untersuchungsausschüssen hingewiesen. § 6 Abs. 3 Satz 4 und Verbindung mit Satz 5 darf keinesfalls als Möglichkeit genutzt werden, an sich rechtmäßig gelöschte Daten nachträglich wiederherzustellen.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de