25.xxx

Botschaft zur Änderung des Nachrichtendienstgesetzes

vom 28. Januar 2026

Sehr geehrter Herr Nationalratspräsident
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf einer Änderung des Bundesgesetzes über den Nachrichtendienst.

Gleichzeitig beantragen wir Ihnen, die folgenden parlamentarischen Vorstösse abzuschreiben:

2018	M	17.3862	Ausreisesperren für potenzielle Gewaltextremisten (S 13.12.17, Rieder; N 12.6.18)

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

…

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Guy Parmelin
Der Bundeskanzler: Viktor Rossi

Übersicht

Diese Vorlage hat zum Ziel, das Nachrichtendienstgesetz insbesondere in den folgenden Bereichen anzupassen und zu verbessern: Datenhaltung, Datenschutz, genehmigungspflichtige Beschaffungsmassnahmen, Kabelaufklärung, Eindringen in Computersysteme im Ausland, Aufsicht über die Funk- und Kabelaufklärung, politische Steuerung durch den Bundesrat sowie Durchsetzung von Verfügungen.

Ausgangslage

Das heutige Nachrichtendienstgesetz (NDG) trat am 1. September 2017 in Kraft. Schon während der parlamentarischen Beratung wurde die spätere Prüfung einzelner Regelungen angeregt, so namentlich die Zusammenlegung der Unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND) mit der Unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung (UKI).

Ferner soll die Vorlage mehrere Verbesserungsvorschläge berücksichtigen, die vor allem durch externe Stellen wie die Geschäftsprüfungsdelegation der eidgenössischen Räte (GPDel), das Bundesverwaltungsgericht und die kantonalen Vollzugsbehörden (KND) aufgrund erster praktischer Erfahrungen beim Vollzug des NDG eingebracht wurden. Insbesondere sollen die Regelung der Informationssysteme des Nachrichtendienstes des Bundes (NDB) sowie das Auskunftsrecht neu konzipiert werden.

Inhalt der Vorlage

Datenhaltung*: Schranken bezüglich der Bearbeitung von Daten über politische Tätigkeiten und die Wahrnehmung der Meinungs-, Versammlungs- und Vereinigungsfreiheit (Art. 5 Abs. 5 NDG) sollen nur für die nachrichtendienstlichen Tätigkeiten des NDB gelten, nicht aber für dessen allgemeine Verwaltungstätigkeiten. Die Konzeption der Datenhaltung wird erneuert. Die Arten und Kategorien von nachrichtendienstlichen Daten werden festgelegt und anstelle der Definition einzelner Informationssysteme wird der Zugriff auf die Daten geregelt.*

Datenschutz*: Das Auskunftsrecht wird an das revidierte Datenschutzgesetz angepasst und gleichzeitig vereinfacht.*

Genehmigungspflichtige Beschaffungsmassnahmen: *Eine neue genehmigungspflichtige Beschaffungsmassnahme zum Einholen von Daten bei Finanzintermediären soll es bei schweren Bedrohungen der inneren oder äusseren Sicherheit der Schweiz ermöglichen, z. B. Finanzflüsse von Terrororganisationen oder Spionagenetzwerken aufzuklären. Der Anwendungsbereich soll gemäss dem Postulat Glanzmann-Hunkeler vom 28. September 2017 (17.3831, «Griffige Instrumentarien gegen Gewaltextremismus») auf gewalttätigen Extremismus ausgeweitet werden. Zudem soll das Freigabeverfahren punktuell vereinfacht werden.*

Genehmigungsfreie Beschaffungsmassnahmen*: Es wird eine Grundlage für den Einsatz von elektronischen Ortungsgeräten bei Observationen geschaffen. Gewerbliche Beherbergungsbetriebe werden neu zur Auskunftserteilung über vorhandene Daten verpflichtet.*

Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten: *Die Aufgaben der heutigen UKI werden vollumfänglich der AB-ND übertragen. Die UKI wird aufgehoben. Zudem regelt das NDG neu, dass die AB-ND für ihr Budget selbst verantwortlich ist und international mit ausländischen Aufsichtsbehörden über Nachrichtendienste zusammenarbeiten sowie kantonale Aufsichtsbehörden direkt über ihre Empfehlungen nach Kontrollen der KND informieren kann.*

Kabelaufklärung*: Die Höchstdauer der Verlängerung von Kabelaufklärungsaufträgen wird erhöht, da diese Aufträge naturgemäss auf einen längeren Zeitraum ausgerichtet sind.*

Eindringen in Computersysteme im Ausland*: Das Eindringen in Computersysteme und -netzwerke im Ausland zur Informationsbeschaffung muss bei Dringlichkeit sofort erfolgen können, weshalb dafür ein Dringlichkeitsverfahren geschaffen wird.*

Politische Steuerung durch den Bundesrat*: Die Verpflichtung des Bundesrates zur jährlichen Publikation einer Beurteilung der Bedrohungslage wird mit Blick auf die künftige Vierjahreskadenz der sicherheitspolitischen Berichte gestrichen.*

Die Kompetenz des Bundesrates zum Abschluss von völkerrechtlichen Verträgen im Bereich des Nachrichtendienstes wird ergänzt. Die Kontrolle und Aufsicht über diese Verträge sind durch die GPDel und die AB-ND weiterhin gewährleistet.

Durchsetzung von Verfügungen*: Neu wird eine verwaltungsstrafrechtliche Strafbestimmung zur Durchsetzung von Verfügungen nach dem NDG geschaffen.*

Weiteres*: Die Arbeitsbereiche Cyber und das integrale Lagebild über die sicherheitsrelevanten Vorgänge im In- und Ausland werden besser verankert.*

Anpassungen im präventiv-polizeilichen Bereich: *Neu wird eingeführt, dass das Bundesamt für Polizei Ausreisebeschränkungen gegen Personen verfügen kann, die sich an Gewaltakten im Zusammenhang mit Demonstrationen oder Kundgebungen im Ausland beteiligen. Die Voraussetzungen für Ausreisebeschränkungen bei Gewalttätigkeiten an Sportveranstaltungen werden überarbeitet. Zudem wird die Möglichkeit zur Anordnung der Vorbereitungshaft während der Durchführung eines Ausweisungsverfahrens wegen Gefährdung der inneren oder äusseren Sicherheit auf Personen ausgedehnt, die über eine Kurzaufenthalts-, Aufenthalts- oder Niederlassungsbewilligung verfügen.*

Inhaltsverzeichnis

Botschaft

1 Ausgangslage

1.1 Handlungsbedarf und Ziele

Das Nachrichtendienstgesetz vom 25. September 2015[1] (NDG) trat am 1. September 2017 in Kraft. Schon während der parlamentarischen Beratung wurde die spätere Prüfung einzelner Bestimmungen angeregt, so namentlich die Zusammenlegung der Funktionen der Unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND) mit jenen der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung (UKI).

Deshalb beauftragte der Bundesrat mit Beschluss vom 16. August 2017 über das Inkrafttreten des NDG und der dazugehörigen Verordnungen das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), im Rahmen einer künftigen Revision des NDG, spätestens aber bis Ende 2021, eine gesetzliche Grundlage für die selbstständige Einreichung des Budgets der AB-ND im NDG und im Parlamentsgesetz vom 13. Dezember 2002[2] (ParlG) zu schaffen, um deren Unabhängigkeit zusätzlich zu erhöhen. Am 20. Februar 2019 beauftragte der Bundesrat sodann das VBS, ihm bis Ende Juni 2020 einen Vorentwurf für eine Revision des NDG zu unterbreiten. Insbesondere sollten dabei die Übertragung der Aufgaben der UKI an die AB-ND, Anpassungen im Bereich der genehmigungspflichtigen Beschaffungsmassnahmen (GEBM) sowie Anpassungen formeller Natur geprüft werden.

Ferner soll die Vorlage mehrere Verbesserungsvorschläge berücksichtigen, die vor allem durch externe Stellen wie die Geschäftsprüfungsdelegation der eidgenössischen Räte (GPDel), das Bundesverwaltungsgericht und die kantonalen Vollzugsbehörden (KND) aufgrund erster praktischer Erfahrungen beim Vollzug des NDG eingebracht wurden, und Unterschiede in den Sprachversionen des Gesetzestexts bereinigen.

Mit Beschluss vom 26. August 2020 beauftragte der Bundesrat das VBS, die Regelung der Informationssysteme des Nachrichtendienstes des Bundes (NDB) sowie das Auskunftsrecht einer Neukonzeption zu unterziehen, basierend auf den im Jahresbericht 2019 vom 28. Januar 2020[3] der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation der eidgenössischen Räte von der GPDel formulierten Vorschlägen zum Umgang mit nachrichtendienstlichen Daten. Ausserdem sah die GPDel Bedarf für gewisse Klärungen betreffend die Tätigkeiten der AB-ND und deren Empfehlungen, insbesondere gegenüber den KND.

Als Folge verschiedener parlamentarischer Vorstösse regelt die Vorlage zudem die Ausweitung des Anwendungsbereichs der GEBM auf den gewalttätigen Extremismus sowie auf das Einholen von Daten bei Finanzintermediären. Durch eine Änderung des

1 SR **121**
2 SR **171.10**
3 BBl **2020** 2971 S. 3054–3055

Bundesgesetzes vom 21. März 1997[4] über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) wird eingeführt, dass das Bundesamt für Polizei (fedpol) Ausreisebeschränkungen gegen Personen verfügen kann, die sich an Gewaltakten im Zusammenhang mit Demonstrationen oder Kundgebungen im Ausland beteiligen.

1.2 Geprüfte Alternativen und gewählte Lösung

Bei nachrichtendienstlichen Tätigkeiten handelt es sich per se um Tätigkeiten, die nur durch Behörden ausgeführt werden dürfen. Die Revision des NDG ist daher alternativlos. Im Rahmen der Arbeiten an der Revision wurde stets sorgfältig abgewogen, um das Gleichgewicht zwischen möglichen Grundrechtseingriffen und der Sicherheit der Schweiz zu wahren.

1.3 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die Vorlage ist in der Botschaft vom 24. Januar 2024[5] zur Legislaturplanung 2023–2027 und im Bundesbeschluss vom 6. Juni 2024[6] über die Legislaturplanung angekündigt.

Die Vorlage ist im Voranschlag 2025 mit integriertem Aufgaben- und Finanzplan 2026–2028 der Verwaltungseinheit VBS[7] als Geschäft zu den Zielen des Bundesrates 2025 erwähnt.

Der NDB trägt mit der frühzeitigen Erkennung, Verhinderung, Zuordnung und Abwehr von Cyberangriffen wesentlich zum Schutz der Schweiz vor Cyberrisiken bei. Die in Artikel 6 Absatz 1 Buchstabe b vorgesehene Ausweitung des Auftrags des NDB auf sicherheitspolitisch bedeutsame Vorgänge im Cyberraum unterstützt die Nationale Cyberstrategie (NCS) vom 5. April 2023[8].

Um die nachrichtendienstliche Frühwarnung zum Schutz kritischer Infrastrukturen gewährleisten zu können, muss der NDB Kontakte zu den Betreiberinnen kritischer Infrastrukturen etablieren und pflegen können, weswegen diese Kompetenz ausdrücklich in Artikel 6 Absatz 5 aufgenommen wird. Dies stimmt mit der nationalen Strategie des Bundesrates vom 16. Juni 2023[9] zum Schutz kritischer Infrastrukturen überein.

4 SR **120**
5 BBl **2024** 525
6 BBl **2024** 1440
7 Voranschlag 2025 mit IAFP 2026–2028 der Verwaltungseinheit VBS, abrufbar unter: www.efv.admin.ch > Finanzberichte > Finanzberichte Bund > Voranschlag mit integriertem Aufgaben- und Finanzplan.
8 Nationale Cyberstrategie (NCS), April 2023, abrufbar unter: www.ncsc.admin.ch > NCS Strategie > Nationale Cyberstrategie NCS.
9 BBl **2023** 1659

Ansonsten hat die Vorlage keine wesentlichen Schnittstellen mit Strategien des Bundesrates.

1.4 Erledigung parlamentarischer Vorstösse

Motion Rieder vom 28. September 2017 (17.3862 «Ausreisesperren für potenzielle Gewaltextremisten»):

Das Anliegen dieser Motion wurde in die vorliegende Änderung des NDG integriert, da diese unter anderem Mittel zur besseren Bekämpfung des Gewaltextremismus vorsieht. Aus diesem Grund ist es sinnvoll, die Vorschläge zur Umsetzung der Motion im Zusammenhang mit den für den im NDG vorgesehenen Massnahmen gegen Gewaltextremismus zu diskutieren.

Zur Umsetzung der Motion wird vorgeschlagen, dass das fedpol Ausreisebeschränkungen gegen Gewaltextremistinnen und Gewaltextremisten verfügen kann (siehe dazu die Ausführungen zur Änderung des BWIS unter Ziff. 5).

2 Vorverfahren, insbesondere Vernehmlassungsverfahren

Vorverfahren

An der Vorbereitung der Revisionsvorlage waren Vertreterinnen und Vertreter der AB-ND und der UKI, des VBS (Generalsekretariat [GS-VBS], Bundesamt für Bevölkerungsschutz [BABS], militärischer Nachrichtendienst, Dienst für Cyber- und elektromagnetische Aktionen [CEA]), des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA; Generalsekretariat), des Eidgenössischen Justiz- und Polizeidepartements (EJPD; Generalsekretariat, Bundesamt für Justiz [BJ], fedpol, Dienst Überwachung Post- und Fernmeldeverkehr [Dienst ÜPF]), der Bundesanwaltschaft (BA), der Bundeskanzlei (BK und Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter [EDÖB]) sowie der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) und der Konferenz der kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) beteiligt.

Unter der Leitung des NDB erarbeiteten interdepartementale Arbeitsgruppen die Vorlage themenbezogen. Die Revisionsvorschläge zur Aufsicht (Art. 77–78*d*) erarbeiteten die AB-ND und die UKI selbstständig. Ihre Entwürfe wurden danach in das Projekt aufgenommen. Wegen der Risikosituation und den Massnahmen zur Eindämmung der Corona-Pandemie fanden die meisten Arbeiten und Konsultationen auf dem Korrespondenzweg statt.

Das Bundesverwaltungsgericht nahm auf eigenen Wunsch nicht an Arbeitsgruppen teil. Der NDB informierte es aber laufend über den Stand der Arbeiten und das Bundesverwaltungsgericht hatte die Gelegenheit, sich in einer Vorkonsultation schriftlich

zu äussern. Es wurde auch während der Ämterkonsultation schriftlich konsultiert und nahm an der Vernehmlassung teil.

Da sich die Änderungen des Gesetzes primär an Behörden richten, eine geringe Anzahl an Unternehmen betroffen ist, und die Auswirkungen auf den Bund, insbesondere im Personalbereich, geringfügig sind, konnte auf eine Regulierungsfolgeabschätzung verzichtet werden.

Vernehmlassungsverfahren

Am 18. Mai 2022 verabschiedete der Bundesrat den Vorentwurf zur Änderung des NDG und beauftragte das VBS mit der Durchführung des Vernehmlassungsverfahrens. Dieses dauerte vom 18. Mai bis zum 9. September 2022. Zur Teilnahme eingeladen wurden 80 Vernehmlassungsadressatinnen und -adressaten, insgesamt 88 Stellungnahmen gingen beim NDB ein (Kantone: 26; Parteien: 6; Bundesgerichte: 1, gesamtschweizerische Dachverbände der Wirtschaft: 3; weitere interessierte Kreise: 14, nicht eingeladene Teilnehmende: 38, davon 6 Privatpersonen).

Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens

Mit einer Ausnahme (Graubünden) wurde die vorgesehene Revision des NDG seitens der Kantone sowie der KKPKS und der KKJPD im Allgemeinen begrüsst. Drei politische Parteien (FDP.Die Liberalen, die Mitte, Schweizerische Volkspartei), die in der Bundesversammlung repräsentiert sind, unterstützen die Revision ebenfalls. Das Schweizerische Sanitätskorps, Economiesuisse, die Schweizerische Offiziersgesellschaft und Chance CH bewerten den Vorentwurf ebenfalls positiv. Hingegen äussern sich die Grünliberalen, Libero, die Digitale Gesellschaft und Amnesty International skeptisch zum Vorentwurf. Die Grünen lehnen die ganze Revision ab und schliesslich findet die Sozialdemokratische Partei der Schweiz die Revision zu wenig ambitioniert.

Die Mehrheit der Vernehmlassungsteilnehmenden begrüsst die Einführung des Begriffs Cyberraum in Artikel 6 Absatz 1 Buchstabe b, wünscht sich aber eine präzisere Definition.

Die Mehrheit der Kantone und die KKPKS befürwortet den genehmigungsfreien Einsatz von Ortungsgeräten als unterstützende Massnahme bei einer Observation. Schwyz, Graubünden sowie das Bundesverwaltungsgericht und einige NGOs äussern sich dazu hingegen kritisch.

Praktisch alle Kantone, die KKPKS, die KKJPD sowie weitere Vernehmlassungsteilnehmende befürworten die Möglichkeit der Anwendung von GEBM im Zusammenhang mit gewalttätig-extremistischen Tätigkeiten sowie die neue Möglichkeit der Informationsbeschaffung bei Finanzintermediären.

In mehreren Stellungnahmen wird die Streichung von Artikel 28 Absatz 2 (gegen Drittpersonen, die dem Berufsgeheimnis unterstehen, sowie gegen Medienschaffende dürfen keine GEBM angeordnet werden) stark bemängelt, da nach Meinung der Verfassenden das Berufsgeheimnis gewahrt bleiben müsse. Dies gilt insbesondere für die

Medien (Impressum, Investigativ.ch, Reporter ohne Grenzen, Schweizer Presserat, SRG-SSR, Telesuisse, Stampa Svizzera, Syndicom, Verband Schweizer Privatfernsehen, Verband Schweizerischer Patent- und Markenanwälte, Verband Medien mit Zukunft), die medizinischen Berufe (FMH Verbindung der Schweizer Ärztinnen und Ärzte, Schweizerische Zahnarzt-Gesellschaft, Schweizerische Gesellschaft für Psychiatrie und Psychotherapie, Föderation der Schweizer Psychologinnen), den Schweizerischen Anwaltsverband, die Schweizerische Staatsanwaltschaftskonferenz, die Schweizer Bischofskonferenz sowie die evangelisch-reformierte Kirche der Schweiz.

Die wichtigsten Entscheide nach durchgeführtem Vernehmlassungsverfahren betreffen:

– den Einsatz von GEBM zum Einholen von Auskünften von Finanzintermediären: Die SP fordert, dass der NDB jährlich veröffentlicht, welche Art von Finanzintermediären in Anwendung der neuen Regelung überwacht wurden. Das VBS wird dieser Forderung, wenn praktisch umsetzbar, im Rahmen der Änderung des Verordnungsrechts entgegenkommen.

– die Aufhebung von Artikel 28 Absatz 2: Auf diese Aufhebung wird verzichtet. Die Relevanz in der Praxis ist für den NDB heute sehr gering.

Die Details zu den Ergebnissen der Vernehmlassung finden sich im Ergebnisbericht.[10]

3 Rechtsvergleich, insbesondere mit dem europäischen Recht

Nachfolgend werden die Regelungen ausgewählter europäischer Nachrichtendienste in Bezug auf drei gewichtige Revisionsthemen analysiert und mit den in dieser Vorlage vorgesehenen Neuerungen verglichen. Bei Deutschland (Bundesamt für Verfassungsschutz [BfV]) und Italien (Agenzia Informazioni e Sicurezza Interna [AISI] und Agenzia Informazioni e Sicurezza Esterna [AISE]) handelt es sich um zwei bedeutende Nachbarstaaten der Schweiz mit ähnlicher Rechtstradition, während die beiden Staaten Belgien (Service Général du Renseignement et de la Sécurité [SGRS]) und Estland (Kaitsepolitseiamet [KAPO]) zusätzlich aufgrund ihrer Grösse mit der Schweiz vergleichbar sind.

Informationsbeschaffung bei Finanzintermediären

Eine Ergänzung von Artikel 26 Absatz 1 mit einer neuen GEBM soll es dem NDB ermöglichen, Informationen über die Finanzierung von sicherheitsrelevanten Personen oder Gruppierungen zu erhalten. Zu diesem Zweck soll er Auskünfte über Beziehungen zwischen einer natürlichen oder juristischen Person und Händlerinnen und Händlern oder Finanzintermediären nach dem Geldwäschereigesetz vom 19. Oktober 1997[11] (GwG) einholen können.

10 Abrufbar unter: www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2022 > VBS > Vernehmlassung 2022/15 > Ergebnisbericht.
11 SR **955.0**

- Die italienischen Agenturen AISI und AISE verfügen grundsätzlich über keine solchen Befugnisse. Sie haben aber gestützt auf ihre rechtliche Grundlage die Möglichkeit, mit Behörden und Organisationen, welchen die Erfüllung öffentlicher Aufgaben übertragen wurde, für die Zusammenarbeit erforderliche Vereinbarungen abzuschliessen. Ebenfalls haben sie Zugang zu Computerarchiven dieser Stellen. In diesem Rahmen können AISI und AISE Informationen finanzieller Art erhalten, jedoch nicht über die Bewegungen einzelner Bankkonten. Die Modalitäten und Bedingungen eines solchen Informationsaustauschs, insbesondere über die Sicherstellung der technischen Nachvollziehbarkeit der Datenzugriffe, werden mit den betreffenden Behörden oder Organisationen vereinbart.
- Das BfV kann unter gewissen Bedingungen (z. B. dem Vorliegen von schwerwiegenden Gefahren für gesetzlich festgelegte Schutzgüter) von Unternehmen des Finanzsektors Informationen anfordern, einschliesslich Informationen über Kontoinhaber und Transaktionen. Voraussetzung für solche Auskunftsersuchen ist eine Anordnung des Bundesministeriums des Innern sowie die Genehmigung durch einen unabhängigen Aufsichtsausschuss (G10-Kommission).
- Der SGRS muss für die Informationsbeschaffung mit aussergewöhnlichen Methoden, worunter teilweise auch Auskunftsersuchen an Finanzinstitute fallen, einen Genehmigungsantrag an eine Kommission stellen. Zusätzlich muss jeweils die Aufsichtsbehörde über den SGRS informiert werden. Dies betrifft alle Informationen über Finanzprodukte und Transaktionen sowie deren Überwachung. Ordentliche Informationsbeschaffungen im Finanzsektor wie die Beschaffung von Informationen über einen Kontoinhaber benötigen hingegen lediglich die Genehmigung der Leitung des SGRS.
- Das KAPO kann entsprechende Informationen einholen. In Estland müssen dem Bankgeheimnis unterstehende Informationen (alle Daten, die einem Kreditinstitut bekannt sind und einen Kunden des Kreditinstituts oder eines anderen Kreditinstituts betreffen) im Zusammenhang mit Untersuchungen unter anderem Sicherheitsbehörden offengelegt werden – unter gewissen Voraussetzungen und wenn es für die Erfüllung von deren Aufgaben notwendig ist. Zudem gehört es zu den Rechten und Pflichten von Kreditinstituten, in gesetzlich definierten Fällen in Zusammenhang mit Geldwäscherei, Terrorismusfinanzierung und internationalen Sanktionen dem Bankgeheimnis unterstehende Informationen offenzulegen.

Einsatz von elektronischen Ortungsgeräten im Rahmen von Observationen

Mit dieser Revision wird für den NDB eine Grundlage geschaffen für den genehmigungsfreien Einsatz von elektronischen Ortungsgeräten als Unterstützungsmassnahme von rechtlich zulässigen Observationen.

- Die geographische Lokalisierung von Personen durch die Verwendung von elektronischen Ortungsgeräten wie einem GPS-Tracker wird in den für die

AISI und die AISE geltenden Rechtsgrundlagen mit elektronischer Verfolgung gleichgesetzt. Für diese gibt es keine Rechtsvorschriften, die eine Genehmigung durch eine zuständige Justiz- oder politische Behörde vorschreiben.

– Für den BfV fallen Geo-Tracking-Geräte, die zur taktischen Unterstützung von Überwachungsmassnahmen eingesetzt werden, zu den klassischen heimlichen Beschaffungsmassnahmen, die keine spezielle Genehmigung erfordern. Aufgrund eines aktuellen deutschen Gerichtsurteils soll die Anwendung dieser Geräte aber zukünftig angepasst werden (erhöhte Eingriffsintensität, sofern ein Bewegungsprofil angefertigt werden kann).
– Die für den SGRS geltenden rechtlichen Grundlagen enthalten keine expliziten Regelungen zum Einsatz von Geo-Tracking-Geräten. Vielmehr fällt ein solcher Einsatz unter die Verwendung technischer Mittel. Eine Genehmigung durch die Leitung des SGRS oder durch eine Kommission ist nur in Fällen mit einer gesteigerten Eingriffsintensität nötig.
– Der Einsatz von Geo-Trackern fällt für das KAPO unter die verdeckte Überwachung und erfordert einen Beschluss der Leitung einer Sicherheitsbehörde oder einer Beamtin oder eines Beamten mit einer entsprechenden Ermächtigung.

Sicherheitsüberprüfungen und -kontrollen beim eigenen Personal und im Rahmen von Bewerbungsprozessen

Zum Schutz seiner Mitarbeiterinnen und Mitarbeiter, seiner Einrichtungen und der von ihm bearbeiteten Daten kann der NDB verschiedene Massnahmen treffen. Mit punktuellen Ergänzungen von Artikel 7 und dem neuen Artikel 7*a* soll der bereits bestehende Massnahmenkatalog erweitert werden.

– In Italien führen die AISI und der AISE Sicherheitsüberprüfungen bei ihren eigenen Mitarbeiterinnen und Mitarbeitern sowie Bewerberinnen und Bewerbern durch. Diese Überprüfungen sind gesetzlich vorgeschrieben.
– Der BfV hat die Berechtigung auf Zugang zu Büros, inkl. Durchsuchung persönlicher Sachen, und zu Kontrollen dienstlicher und privater elektronischer Geräte. Er kann zudem Hintergrundkontrollen mit Open Source Intelligence oder aufgrund von Abfragen von offiziellen Datenbanken und Informationen anderer nationaler Behörden vornehmen. Weitere Befugnisse zum Zweck des Eigenschutzes erlauben dem BfV ausserdem auch die Vornahme von verdeckten Abklärungen bei Stellenbewerberinnen und Stellenbewerbern.
– Die SGRS ist gesetzlich berechtigt, persönliche Gegenstände sowie dienstliche und private elektronische Geräte zu durchsuchen. Stellenbewerberinnen und Stellenbewerber werden einer offiziellen Sicherheitsüberprüfung unterzogen.

– Das KAPO kann bei seinen Mitarbeiterinnen und Mitarbeitern Sicherheitskontrollen durchführen. Diese unterstehen ebenfalls einer Sicherheitsüberprüfung. Das KAPO kann dazu die gleichen Mittel anwenden, die ihm auch für sonstige Ermittlungen gesetzlich zustehen.

4 Grundzüge der Vorlage

4.1 Die beantragte Neuregelung

Die neue Konzeption der Regelung der Informationssysteme sowie das datenschutzrechtliche Auskunftsrecht betreffend Daten des NDB basierten auf den von der GPDel im Jahresbericht 2019[12] formulierten Vorschlägen zum Umgang mit nachrichtendienstlichen Daten. Mit dem Inkrafttreten des revidierten Datenschutzgesetzes vom 25. September 2020[13] (DSG) sowie neuen technologischen Entwicklungen im Umgang mit Daten änderten sich weitere Rahmenbedingungen der Datenbearbeitung, was den Bundesrat veranlasst, die nachrichtendienstlichen Datenhaltungsregeln konzeptionell neu anzugehen. Angestrebt wird eine technologieneutrale und einfach zu verstehende und zu handhabende Regelung (vgl. dazu die einleitenden Erläuterungen vor Art. 44 ff.). Diese Anpassungen stellen umfangmässig den Hauptteil der heutigen Vorlage dar.

Weitere Themen dieser Revision sind:

– Zusätzliche Massnahmen zur Früherkennung und Verhinderung von gewalttätigem Extremismus, basierend auf verschiedenen parlamentarischen Vorstössen nach negativen Entwicklungen der Sicherheitslage (siehe Erläuterungen zu Art. 27).

– Eine neue Regelung zur Aufklärung der Finanzierung von schweren Bedrohungen der Sicherheit der Schweiz als Antwort auf die verschärfte Sicherheitslage in verschiedenen Bereichen der inneren oder äusseren Sicherheit, namentlich des Terrorismus, der Spionage und des gewalttätigen Extremismus. Wegen der Schwere des Grundrechtseingriffs ist dies als GEBM ausgestaltet (siehe Erläuterungen zu Art. 26).

– Verbesserungsvorschläge für die praktische Umsetzung des NDG, die vor allem durch externe Stellen aufgrund erster Erfahrungen beim Vollzug des NDG eingebracht wurden.

– Sprachliche Anpassungen zur Vereinheitlichung der Terminologie in den drei Amtssprachen.

12 BBl **2020** 2971 S. 3053–3055
13 SR **235.1**

4.2 Abstimmung von Aufgaben und Finanzen

Die Revision an sich hat nur in geringem Rahmen Auswirkungen auf die finanziellen und personellen Ressourcen der Behörden des Bundes und der Kantone, die mit Aufgaben nach dem NDG betraut sind. Der Mehraufwand an personellen Ressourcen beim NDB und beim fedpol ist unter Ziffer 6.1 ausgewiesen. Mit der geplanten Personalzunahme im einstelligen Prozentbereich und dem Nichtbestehen von weiteren finanziellen und personellen Konsequenzen stehen die Bedeutung der (neuen) gesetzlichen Aufgaben und der entsprechende Aufwand in einem vertretbaren Verhältnis.

4.3 Umsetzungsfragen

Dieser Entwurf bezweckt hauptsächlich, bereits bestehende Prozesse und Tätigkeiten des NDB bzw. der KND zu optimieren oder klarer zu regeln. Deshalb kann vollumfänglich auf die bereits bestehenden eidgenössischen und kantonalen Strukturen aufgebaut werden.

Mit dem neuen Artikel 14 Absatz 3 soll der Einsatz von Ortungsgeräten als Unterstützungsmassnahme von rechtlich zulässigen Observationen möglich sein. Dies wird von den meisten Kantonen grundsätzlich unterstützt, gleichzeitig nehmen sie die Formulierung im Entwurf aber als zu restriktiv wahr. Aus Sicht der meisten Kantone sollte es möglich sein, eine Standortbestimmung durch ein Ortungsgerät weiterlaufen zu lassen, um nach einem Unterbruch der Observation diese anhand der gesendeten Standortdaten wieder aufnehmen zu können. Damit würden nicht unnötig Personalressourcen verschwendet und die Observationskräfte könnten das Entdeckungsrisiko minimieren oder vermeiden.

Mehrere Kantone (BE, UR, SZ, SO, GR, AG) sowie die KKPKS verlangen in ihrer Stellungnahme zur Vernehmlassung, dass die KND die Identifikation und Befragung von Personen als genehmigungsfreie Beschaffungsmassnahme selbstständig durchführen können sollen (Art. 24 i. V. m. Art. 85 Abs. 1).

Von einigen KND (ZH, UR, OW, JU) und der KKJPD wurde gefordert, dass die KND einen gegenseitigen Zugriff auf ihre nachrichtendienstlichen Daten erhalten sollen. Dies, um mit wenig Aufwand herauszufinden, ob der KND eines Nachbarkantons zu einer Person oder Organisation bereits Daten bearbeitet. Da nicht alle KND mit dieser Zugriffsvergabe einverstanden sind, wird diese nur als «Kann-Vorschrift» eingeführt.

5 Erläuterungen zu einzelnen Artikeln

Für eine bessere Lesbarkeit der Erläuterungen werden alle sprachlichen Anpassungen, die keine inhaltlichen Änderungen bewirken und nur eine Sprache betreffen, am Anfang aufgelistet:

Betrifft nur den französischen Text:

Artikel 5 Absatz 5

Es handelt sich um eine rein sprachliche Anpassung an den deutschen und den italienischen Text.

Artikel 15, 18 und 35

Heute wird im Rahmen der nachrichtendienstlichen Aktivitäten von «source humaine» gesprochen. Deswegen wird der Begriff «informateur» im ganzen Gesetz durch «source humaine» ersetzt.

Artikel 23 Absatz 2

Der Begriff «audition» wird durch den auch in Artikel 24 verwendeten Begriff «interrogatoire» ersetzt.

Artikel 26 Absatz 1 Buchstaben a und a^{bis}

Es handelt sich um eine rein sprachliche Vereinheitlichung.

Artikel 27 Absatz 1 Einleitungssatz und Buchstabe b

Es handelt sich um rein sprachliche Anpassungen.

Artikel 33 Absatz 2 Buchstaben a und b

Es handelt sich um eine rein sprachliche Anpassung an den deutschen und den italienischen Text.

Artikel 35 Absatz 2 und Absatz 3 Buchstaben a und b

Es handelt sich um rein sprachliche Anpassungen.

Artikel 38 Absatz 6

Der Begriff «travail» wird durch den Begriff «activité» ersetzt. Die Verwendung des Begriffs wird dadurch einheitlicher.

Artikel 39, 41 und 42

Der Ausdruck «du réseau câblé» wird gestrichen. Die Präzisierung, um welche Aufklärung es sich handelt, ist nicht nötig, da sich dies aus der Thematik des 7. Abschnitts zur Kabelaufklärung ergibt.

«Réseau filaire» wird durch «réseau câblé» ersetzt; somit wird die Terminologie im ganzen Gesetzestext vereinheitlicht (Art. 39 Abs. 1 und Art. 41 Abs. 1 Bst. d).

Der Ausdruck «mot-clés» wird durch «critère de recherche» ersetzt. Dies entspricht der Realität, da nicht nur nach Wörtern sondern bspw. auch nach Telefonnummern oder IP-Adressen aufgeklärt wird.

Betrifft nur den deutschen Text:

Im ganzen Erlass wird «orientiert» *ersetzt durch* «informiert».

Artikel 19 Absatz 3 und 20 Absatz 2

Diese Anpassung bezweckt die einheitliche Verwendung der Formulierung «geheim halten» im ganzen Gesetz.

Artikel 32

Sachüberschrift

Mit der Ergänzung der Überschrift wird sofort ersichtlich, dass die Beendigung der Beschaffungsmassnahme gemeint ist.

Absatz 1 Buchstabe c

Es handelt sich um eine rein sprachliche Anpassung an die ansonsten verwendete Bezeichnung «Vorsteherin oder Vorsteher des VBS» nach Artikel 37 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[14] (RVOG).

Betrifft nur den italienischen Text:

Artikel 39 Absatz 4 Buchstabe c

Der Ausdruck «die segnali via cavo» wird gestrichen. Die Präzisierung, um welche Aufklärung es sich handelt, ist nicht nötig, da sich dies aus der Thematik des 7. Abschnitts zur Kabelaufklärung ergibt.

5.1 Allgemeine Erläuterungen

Alle Grundsatznormen, in denen der NDB genannt wird, gelten auch für die KND. Die KND werden nur dann ausdrücklich genannt, wenn eine Regelung spezifisch nur sie betrifft oder eine gewisse Hervorhebung ihrer Rechte und Pflichten notwendig ist, weil sonst nicht klar wäre, ob die KND zu einer bestimmten Handlung befugt sind.

14 SR **172.010**

Im ganzen Erlass wird «unabhängige Aufsichtsbehörde» ersetzt durch «AB-ND», mit den nötigen grammatikalischen Anpassungen.

5.2 Die Bestimmungen im Einzelnen

Artikel 1

Buchstabe a

Die heutige Formulierung lässt den Eindruck entstehen, dass der NDB ausschliesslich Aufgaben nach dem NDG erfüllt. Das trifft aber nicht zu. Der NDB erfüllt, wie jede andere Amtsstelle, auch reine Verwaltungsaufgaben in Anwendung des RVOG. Er ist beispielsweise an Ämterkonsultationen im Rahmen von Rechtsetzungsverfahren, an der Bearbeitung parlamentarischer Vorstösse oder an der Beantwortung von Medienanfragen beteiligt. Ebenfalls rekrutiert, führt und betreut der NDB sein Personal, betreibt die Informatik, beschafft Güter und Dienstleistungen nach dem Beschaffungswesen und führt seine Finanzen. Die ausdrückliche Erwähnung der nachrichtendienstlichen Tätigkeiten in Artikel 1 stellt klar, dass die übrigen Verwaltungstätigkeiten des NDB nicht im NDG geregelt sind, sondern sich nach den allgemein anwendbaren Bestimmungen für die Bundesverwaltung richten.

Buchstabe d

Der NDB bearbeitet nicht nur nachrichtendienstliche Daten. Das NDG regelt die Unterscheidung von nachrichtendienstlichen und administrativen Daten und enthält gewisse Grundsätze für die Bearbeitung administrativer Daten. Entsprechend wird neu in Artikel 1 auch die Datenbearbeitung des NDB als Regelungsgegenstand des NDG genannt. Wo das NDG nichts Abweichendes regelt, finden die Bestimmungen des DSG Anwendung.

Artikel 5

Wie bereits eingangs erwähnt, gelten Artikel, in denen der NDB genannt wird, auch für die KND. Die KND werden nur dann ausdrücklich genannt, wenn eine Regelung spezifisch nur sie betrifft oder eine gewisse Hervorhebung ihrer Rechte und Pflichten notwendig ist, weil sonst nicht klar wäre, ob die KND zu einer bestimmten Handlung befugt sind.

Absatz 6

Die geltende nachrichtendienstliche Datenbearbeitungsschranke zugunsten der politischen Betätigung und der Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit soll weiterhin unangetastet bleiben (vgl. Abs. 5). Die notwendigen Ausnahmen beschreibt Absatz 6 jedoch präziser als bisher. Es handelt sich dabei durchwegs um Fallkonstellationen, bei denen der NDB auch heute schon Daten nach Absatz 5 zwingend bearbeiten muss, um seinen in Artikel 6 umschriebenen Auftrag oder seine administrativen Pflichten erfüllen zu können (bspw. muss der NDB eine Meldung bei der Prüfung nach Art. 46 Abs. 1 lesen, auch wenn sie Inhalte aufweist, die unter die Datenbearbeitungsschranke fallen).

Buchstabe a

Es kann vorkommen, dass zum Zeitpunkt des Eingangs von Daten aufgrund der Quelle, des Inhalts oder des Kontexts ein Aufgabenbezug durchaus wahrscheinlich erscheint, aber noch nicht gesichert vorliegt. Um herauszufinden, ob ein Aufgabenbezug gegeben ist, sind deshalb in solchen Fällen weitere Abklärungen nötig. So ist es bspw. möglich, dass ein ausländischer Nachrichtendienst dem NDB eine Erkenntnisanfrage zu einer Person zukommen lässt, die in dessen Land rechtsradikales Gedankengut verbreitet, was bereits eine Zuständigkeit der ausländischen Behörde begründet. Weil sich diese Person zu einem Treffen in die Schweiz begeben hat, möchte der Partnerdienst nun wissen, ob der NDB über entsprechende Erkenntnisse verfügt. Der NDB erteilt in der Folge dem KND, in dessen Kanton sich die betreffende Person aufgehalten hat, einen Abklärungsauftrag. Erst das Ergebnis dieser Abklärung wird aufzeigen, ob es sich um ein Treffen gewalttätig-extremistischer Personen handelt, ob damit der Aufgabenbezug gegeben ist und ob eine weitere Datenbearbeitung zulässig ist. Selbstverständlich kann dies auch bei Daten vorkommen, die bei den KND eingehen. Das Vorgehen zur Abklärung des vermuteten Aufgabenbezugs wird nun aus Gründen der Transparenz ausdrücklich festgehalten (vgl. dazu auch die Ausführungen zu Art. 45 Abs. 4).

Buchstabe b

Zurzeit ist der Anwendungsbereich der in Absatz 6 geregelten Ausnahmen auf Terrorismus, Spionage und gewalttätigen Extremismus beschränkt. Dies ging noch auf das BWIS zurück, welches das Thema Cyber noch nicht enthielt und davon ausging, dass Proliferationstätigkeiten nicht unter den Missbrauch der genannten Grundrechte fallen könnten. Es gibt jedoch keinen Grund, weshalb der Missbrauch der in Artikel 5 Absatz 5 genannten Grundrechte im Bereich Nonproliferation und bei Angriffen auf kritische Infrastrukturen geschützt werden sollte. Deshalb wird der Anwendungsbereich dieser Bestimmung auf alle Tätigkeiten nach Artikel 6 Absatz 1 Buchstabe a ausgedehnt. Somit wird klargestellt, dass sich der NDB beispielsweise mit Absichtserklärungen zu Cyberangriffen gegen kritische Infrastrukturen oder Informationen zu vorbereitenden Treffen dazu befassen kann. Im Proliferationsbereich werden aber auch mit der Neuregelung bspw. parlamentarische Freundschaftsgruppen mit relevanten Ländern nicht zum Beobachtungsobjekt des Nachrichtendienstes.

Buchstabe c

Aus nachrichtendienstlicher Sicht ist es wichtig zu wissen, gegen wen sich eine Bedrohung richtet. Nur so kann der NDB sachgerecht berichten und können die zuständigen Behörden geeignete Massnahmen ergreifen, um die bedrohten Personen und Organisationen zu warnen und zu schützen. Machen diese potenziellen Opfer keinen Gebrauch von den in Artikel 5 Absatz 5 aufgezählten Grundrechten, ist dies unproblematisch. Wenn der NDB bspw. Kenntnis davon erhält, dass ein Anschlag auf den Hauptsitz eines Grosskonzerns geplant ist, kann er diesen und die zuständige Kantonspolizei darüber informieren und entsprechend Daten bearbeiten. In seltenen Fällen kann es aber auch vorkommen, dass Personen oder Organisationen in Situationen geschützt werden müssen, die mit den genannten besonders geschützten Grundrechten zusammenhängen. Wenn bspw. der NDB Kenntnis davon erhält, dass ein Politiker während eines öffentlichen Auftritts tätlich angegriffen werden soll, so muss er zu

dessen Schutz ausnahmsweise Daten zu dessen politischer Arbeit bearbeiten dürfen. Weitere Beispiele sind geplante Cyber-Spionage-Angriffe, die sich direkt gegen Parlamentsmitglieder richten, oder geplante gewalttätig-extremistisch motivierte Sachbeschädigungen gegen ein für das Gesundheitswesen verantwortliches Regierungsmitglied. Diese Ausnahme der Datenbearbeitung kommt aber primär nur zum Schutz erheblicher Interessen in Frage (namentlich Leib und Leben, aber auch Schutz der Privatsphäre). Die Zulässigkeit der nachrichtendienstlichen Datenbearbeitung in Ausnahmefällen wird explizit auch auf Personen und Organisationen ausgedehnt, die von den in Artikel 6 Absatz 1 Buchstabe a genannten Tätigkeiten bedroht werden könnten. So gelangen z. B. immer wieder Ausländervereinigungen in der Schweiz in den Fokus von ausländischen Behörden, was zu Cyber-Angriffen, zu politisch motivierter Bespitzelung oder auch zu tätlichen Angriffen führen kann. Es versteht sich von selbst, dass der NDB auch in diesem Bereich nur präventiv tätig werden und Massnahmen zur frühzeitigen Erkennung und Verhinderung solcher Bedrohungen ergreifen kann. Sobald sich eine Bedrohung realisiert und ein Straftatbestand erfüllt ist, fällt dies in die Kompetenz der Strafverfolgungsbehörden.

Buchstabe d

Ebenfalls ist es für die Beurteilung einer Information (bspw. für die Prüfung ihrer Richtigkeit) wichtig zu wissen, was deren Herkunft ist. Nur wenn der NDB weiss, woher eine Information stammt, kann er diese auch richtig einschätzen und beurteilen, ob diese zuverlässig ist. Es ist bspw. ein Unterschied, ob ein Passant seine Meinung zur Terrorbekämpfung in den Medien äussert oder ob dies eine ausgewiesene Fachexpertin tut. Der NDB hat nicht an der Person des Passanten oder an jener der Fachexpertin ein originäres nachrichtendienstliches Interesse, sondern an der Information über das Ereignis. Um diese bewerten zu können, ist es wichtig zu wissen, von wem diese stammt.

Bei der Steuerung menschlicher Quellen (vgl. Art. 15) verhält es sich ähnlich: die Quelle selbst ist nicht das Ziel der nachrichtendienstlichen Tätigkeit des NDB, sondern nur das Mittel dazu. Dennoch muss der NDB die Personalien der Quelle kennen und in diesem Sinne Daten über sie bearbeiten, auch in den eher seltenen Fällen, in denen die Tätigkeit der Quelle mit ihrer politischen Tätigkeit oder der Ausübung ihrer Meinungs-, Versammlungs- oder Vereinigungsfreiheit zusammenhängt.

Buchstabe e

Der NDB hat die Aufgabe, Dienststellen von Bund und Kantonen laufend über allfällige Bedrohungen zu orientieren und diese nötigenfalls auch zu alarmieren (vgl. Art. 6 Abs. 2). Er hat weiter die Aufgabe, Dienststellen von Bund und Kantonen über Vorgänge und Erkenntnisse zu informieren, welche die gesetzlichen Aufgaben dieser Stellen bei der Wahrung der inneren oder äusseren Sicherheit betreffen (vgl. Art. 6 Abs. 3). Dies tut der NDB im Rahmen des sogenannten Nachrichtenverbunds, bei dem sich die mit Sicherheitsfragen befassten Behörden von Bund und Kantonen lagerelevante Informationen zur Wahrung der inneren oder äusseren Sicherheit gegenseitig

zugänglich machen. Unter Einbezug aller Partner erstellt der NDB dann ein umfassendes Lagebild und aktualisiert dieses laufend.[15]

Die GPDel kam in ihrem Jahresbericht 2019 zum Schluss, dass solche nachrichtendienstlichen Risikobeurteilungen für die Planung von sicherheitspolizeilichen Massnahmen unter anderem auf Daten basieren können, die unter die Schranken von Artikel 5 Absatz 5 fallen. Sie erachtete dies als zulässig, wenn zu diesem Zweck Daten für weniger als ein Jahr bearbeitet werden. Diese präzisierende Vorgabe wird mit dem neuen Buchstaben e umgesetzt. Sie gilt für die Daten, die der NDB zur Führung des Nachrichtenverbunds nach Artikel 58*b* Absatz 1 E-NDG bearbeitet und die er zur Erstellung der elektronischen Lagedarstellung benötigt. So muss bspw. eine politische Partei genannt werden, wenn zur Störung von deren Jahresversammlung aufgerufen wird, damit die zuständigen Behörden den Anlass schützen können. Die sicherheitspolizeilichen Massnahmen ergreift nicht der NDB selber, sondern die dafür zuständigen Behörden des Bundes und der Kantone. Ferner geht es auch um Daten zu Personen, die Auslöser für die sicherheitspolitische Bedeutung des Ereignisses sind, selbst wenn sich die relevante Bedrohung nicht direkt gegen sie richtet (bspw. Aufruf zu gewalttätigen Protesten gegen eine öffentliche Rede eines Politikers oder den Besuch einer ausländischen Staatschefin).

Buchstabe f

Neu wird klargestellt, dass der NDB auch Daten nach Absatz 5 bearbeiten darf, wenn dies für die Erfüllung seiner administrativen Aufgaben notwendig ist. Wenn der NDB beispielsweise in Erfüllung seiner Verwaltungsaufgaben ihm zugewiesene Parlamentsgeschäfte bearbeitet, betreffen diese die politische Betätigung. Dabei fallen auch Personendaten an, ohne dass diese für die nachrichtendienstliche Aufgabenerfüllung von Bedeutung wären. Die Namen der Initiantinnen und Initianten und Mitunterzeichnenden von parlamentarischen Vorstössen, welche die innere oder äussere Sicherheit betreffen, sind entsprechend beim NDB auffindbar.

Absatz 7

Die Begriffe «personenbezogen erschlossene Daten» und «Erschliessung von Daten» werden durch Personendaten ersetzt. Da in Absatz 6 neu auch der Aufgabenbezug und Bedrohungen geregelt werden, wird auch dieser Absatz umformuliert. Daneben wird klargestellt, dass Daten auch anonymisiert statt gelöscht werden können (bspw. dann, wenn in der gleichen Meldung auch NDG-relevante Inhalte enthalten sind). Inhaltlich gibt es aber keine Änderungen.

Absatz 8

Der im aktuellen NDG verwendete Begriff «Exponent/-in» führte in der Vergangenheit verschiedentlich zu Diskussionen, weil er nicht definiert war. Neu wird klargestellt, dass es sich um Personen handelt, die sich an einer Organisation oder Gruppierung auf der Beobachtungsliste (Art. 72) beteiligen, sie personell oder materiell unterstützen, für ihre Ziele Propagandaaktionen organisieren, für sie anwerben oder

15 Vgl. Bericht des Bundesrates zur Sicherheitspolitik der Schweiz, BBl **2016** 7876, Fn. 80, sowie Botschaft vom 19. Febr. 2014 zum Nachrichtendienstgesetz, BBl **2014** 2105 S. 2144.

ihre Tätigkeiten nach Artikel 6 Absatz 1 Buchstabe a auf andere Weise fördern. Am Regelungsgehalt ändert sich dadurch nichts.

Artikel 6

Absatz 1 Buchstabe b

Der geltende Begriff des Angriffs auf kritische Infrastrukturen im NDG hat sich als zu eng erwiesen, um alle sicherheitspolitisch relevanten Vorgänge im Cyberraum abzudecken. Cyberangriffe, nicht nur gegen kritische Infrastrukturen, haben zunehmend eine sicherheitspolitische Relevanz. Sie werden nicht nur von einzelnen Hackerinnen oder Hackern oder kriminellen Gruppen durchgeführt, sondern zunehmend von staatlich unterstützten Akteuren, Streitkräften und Nachrichtendiensten. Nachrichtendienstliche Früherkennung und Prävention müssen dieser Entwicklung, welche die innere oder äussere Sicherheit der Schweiz bedroht, Rechnung tragen. Der NDB muss mit der nachrichtendienstlichen Aufklärung eine umfassende sicherheitspolitische Einschätzung solcher Cyberangriffe vornehmen und damit Grundlagen für die Beurteilung allfälliger Gegenmassnahmen schaffen. Bereits heute ist der NDB für die Darstellung der gesamtheitlichen Cyberbedrohungslage auf Bundesebene zuständig, wie zum Beispiel im Rahmen der Kerngruppe Sicherheit und im Rahmen der nachrichtendienstlichen Gesamtlage. Es ist nicht sinnvoll, wenn sich der Auftrag des NDB auf Cyberangriffe gegen kritische Infrastrukturen beschränkt. Beispielsweise können Cyberangriffe auf in der Schweiz ansässige internationale Organisationen oder NGOs sowie der Missbrauch von IKT-Infrastrukturen in der Schweiz für Cyber-Angriffe sicherheitspolitisch von erheblicher Bedeutung sein, insbesondere wenn sie direkt oder indirekt von ausländischen staatlichen Stellen ausgehen. Der NDB muss auch solche Cybervorfälle nachrichtendienstlich identifizieren, verhindern und analysieren können.

Damit begründet sich die Ausweitung des Auftrags des NDB auf den gesamten Cyberraum, wobei stets eine sicherheitspolitische Bedeutung vorliegen muss. Eine solche liegt vor, wenn Ereignisse und Entwicklungen im Cyberraum dazu geeignet sind, die Selbstbestimmung der Schweiz, ihre demokratische und rechtsstaatliche Ordnung, den Wirtschafts- und Forschungsstandort Schweiz und den Standort internationaler Organisationen zu gefährden, der Schweiz schweren sicherheitspolitischen Schaden zuzufügen oder die Handlungsfähigkeit ihrer Behörden und der kritischen Infrastrukturen der Schweiz zu beeinträchtigen. Hier trägt der NDB mit der frühzeitigen Erkennung, Verhinderung, Abwehr und Attribution von Cyberangriffen wesentlich zum Schutz der Schweiz vor Cyberrisiken bei, wie dies in den einschlägigen Strategien des Bundes festgehalten ist.

Die Ausweitung des Auftrags des NDB auf sicherheitspolitisch bedeutsame Vorgänge im Cyberraum wurde in der Vernehmlassung als zeitgemäss und notwendig erachtet. Verschiedentlich wurde angeregt, den Begriff Cyberraum im Gesetz zu definieren.

Eine besondere Definition im NDG ist nicht nötig, da sich der Begriff Cyberraum auf die Erläuterungen stützt, die in der Nationalen Strategie zum Schutz der Schweiz vor

Cyberrisiken (NCS) 2018–2022 zu finden sind, die der Bundesrat am 18. April 2018[16] verabschiedet hat. Der Cyberraum ist die Gesamtheit der Informations- und Kommunikationsinfrastrukturen (Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln, und der dadurch ermöglichten Interaktionen zwischen Personen, Organisationen und Staaten. Dies geht weiter als das Internet. Diese Definition des Cyberraums gilt auch in der aktuellen NCS von 2023.

Absatz 2bis

Der Nachrichtenverbund ist eine besondere Organisationsform zur Bündelung von lagerelevanten Informationen, die dem NDB von verschiedenen Partnern, die Teil des Lageverbunds Schweiz sind, oder von ausländischen Partnerdiensten geliefert werden. Dies können z. B. Hinweise zu Reisebewegungen von gewaltbereiten Personen sein, Aufrufe zu Gewalt oder Erkenntnisse zu Bedrohungen. Die elektronische Lagedarstellung (vgl. dazu Art. 58*b* Abs. 1 E-NDG und die Erläuterungen dazu) soll alle Informationen enthalten, die die zuständigen Schweizer Behörden für das Ergreifen von Sicherheitsmassnahmen benötigen. Dazu gehören auch Daten, die der NDB in Erfüllung seiner Aufgaben nach Absatz 1 nicht bearbeiten würde. Die Bearbeitung in der elektronischen Lagedarstellung beschränkt sich allerdings auf dieses Instrument und den hier genannten Zweck (vgl. dazu Art. 5 Abs. 6 Bst. e und die Erläuterungen dazu).

Absatz 5

Um die nachrichtendienstliche Frühwarnung zum Schutz kritischer Infrastrukturen gewährleisten zu können, muss der NDB Kontakte zu den Betreiberinnen kritischer Infrastrukturen etablieren und pflegen können. Zudem stellt das BABS die übergeordnete Koordination beim Schutz kritischer Infrastrukturen sicher. Deswegen ist eine enge und regelmässige Absprache zwischen dem NDB und dem BABS für die Kontaktaufnahme und -gestaltung mit den Betreiberinnen kritischer Infrastrukturen notwendig. Diese Absprache wird in der Nachrichtendienstverordnung vom 16. August 2017[17] (NDV) näher geregelt werden. Mit der Ergänzung dieses Absatzes wird einem Bedürfnis der Betreiberinnen kritischer Infrastrukturen entsprochen. Dies stimmt ebenfalls mit der nationalen Strategie des Bundesrates vom 16. Juni 2023 zum Schutz kritischer Infrastrukturen überein.

Artikel 7

Absatz 1 Buchstabe e

Artikel 7 gibt dem NDB die Möglichkeit, zum Schutz und zur Sicherheit seiner Mitarbeiterinnen und Mitarbeiter, seiner Einrichtungen und seiner Daten Massnahmen zu treffen. Dabei geht es insbesondere um Personen-, Objekt- und Informationsschutz

16 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, abrufbar unter: www.ncsc.admin.ch > NCS Strategie > Strategie NCS 2012–2022 - Archiv.

17 SR **121.1**

sowie um die Durchsetzung von Vorschriften, welche die Sicherheit und Glaubwürdigkeit des NDB beim Umgang mit klassifizierten Daten steigern. Der bestehende Massnahmenkatalog soll mit dieser Revision sinnvoll ergänzt werden.

Buchstabe e hält fest, dass der NDB die Nutzung seiner eigenen Daten bzw. die Nutzung der Geräte, die er seinen Mitarbeiterinnen und Mitarbeitern oder jenen der KND zur Verfügung stellt, auswerten kann. Liegen konkrete Anhaltspunkte auf eine akute Bedrohung der Sicherheit des NDB oder auf Verstösse gegen Dienstvorschriften vor, so kann der NDB dies auch ohne Kenntnis der betroffenen Person tun.

Hinweise auf eine akute Bedrohung der Sicherheit des NDB oder auf Verstösse gegen dienstliche Vorschriften können auf verschiedene Art und Weise entstehen und auf verschiedenen Kanälen eingehen. So können beispielsweise Mitarbeiterinnen und Mitarbeiter des NDB bzw. der KND oder aber auch ein Partnerdienst eine Sicherheitsmeldung erstatten, die eine Sachverhaltsabklärung nach sich zieht. Ebenfalls können Anhaltspunkte wie die Mitnahme von privaten Mobiltelefonen oder anderen Aufzeichnungsgeräten in sensible Bereiche des Arbeitsortes oder problematische Kontakte im privaten oder dienstlichen Umfeld vorliegen. Gibt es z. B. Hinweise darauf, dass Mitarbeiterinnen oder Mitarbeiter des NDB für einen Nachrichtendienst eines anderen Staates tätig sind bzw. durch einen solchen rekrutiert werden, muss der NDB in der Lage sein, diesen Hinweisen nachzugehen, ohne die betreffenden Mitarbeiterinnen und Mitarbeiter unmittelbar über die notwendigen Abklärungen zu informieren. Andernfalls bestünde das Risiko, dass Hinweise vernichtet oder Verhaltensweisen geändert würden. Eine personenbezogene Auswertung ist in jedem Fall nur möglich, wenn die Direktorin oder der Direktor des NDB die Genehmigung dazu erteilt (siehe dazu auch die Erläuterungen zu Abs. 1^{bis}).

Absatz 1^{bis}

Die personenbezogene Auswertung von Daten oder Gerätenutzungen nach Absatz 1 Buchstabe e setzt die schriftliche Genehmigung der Direktorin oder des Direktors des NDB oder der vorgesetzten Stelle des KND voraus und kann teilweise nur unter Mitwirkung technischer Bereiche des NDB vollzogen werden. Somit ist in jedem Fall mindestens das Vieraugenprinzip gewährleistet. Stellt der NDB mutmasslich strafbares Verhalten fest, so erstattet er bei den zuständigen Strafverfolgungsbehörden Anzeige.

Absatz 1^{ter}

Zum Schutz seiner Mitarbeiterinnen und Mitarbeiter vor ausländischen Nachrichtendiensten führt der NDB eine Liste mit Ländern, deren Bereisung mit erhöhten Risiken verbunden ist (vor allem das Risiko einer Verhaftung oder der Ausübung von Druck aufgrund der nachrichtendienstlichen Funktion der betroffenen Person). Gewisse Länder versuchen, ausländische nachrichtendienstliche Mitarbeiterinnen und Mitarbeiter zu überwachen, wenn sie in das Land reisen. Dies kann bereits mit vertieften Kontrollen an der Grenze beginnen. Diese Länder versuchen zu ermitteln, mit wem die nachrichtendienstlichen Mitarbeiterinnen und Mitarbeiter Kontakte haben. Auch bekannt ist eine Überwachung des Mobiltelefons, in deren Rahmen der Datenaustauch sowie die Bewegungen im Zielland übermittelt werden oder so in das Gerät eingedrungen wird, dass dies auch bei einer Rückkehr in die Schweiz weiterhin möglich bleibt. Die

fraglichen Länder differenzieren dabei nicht, ob die Reise private oder dienstliche Zwecke hat.

Möchten Mitarbeiterinnen und Mitarbeiter des NDB in ihrer Freizeit solche Länder bereisen, müssen sie deshalb neu bei der für Schutz- und Sicherheitsmassnahmen zuständigen Stelle des NDB eine Bewilligung einholen. Im informellen internationalen Verbund westlicher Nachrichtendienste wird derzeit darüber diskutiert, ob solche Massnahmen Standard sein müssen, um weiterhin auf internationaler Ebene zusammenarbeiten zu können. Die Bewilligungspflicht für private Reisen stellt einen gewissen Eingriff in die Grundrechte der Mitarbeiterinnen und Mitarbeiter dar, weshalb es dafür eine gesetzliche Grundlage braucht.

Die Verbindung von Mitarbeiterinnen und Mitarbeitern der KND (die in der Regel Polizeiangestellte sind) zum NDB ist normalerweise weit weniger ersichtlich, als jene der Mitarbeiterinnen und Mitarbeiter des NDB selber. Dementsprechend sind die Mitarbeiterinnen und Mitarbeiter der KND bezüglich der oben genannten Risiken weniger exponiert. Zudem stehen sie nicht in einem Arbeitsverhältnis mit dem NDB. Folglich gilt für diese die hier geregelte Bewilligungspflicht nicht. Es bleibt aber jederzeit möglich, sich beim NDB über Risikoländer zu erkundigen und sich beraten zu lassen.

Absatz 2

Da es in diesem Gesetz keine Regelungen über einzelne Informationssysteme mehr gibt, wird der Begriff «Informationssysteme» durch «Daten» ersetzt. Dies führt zu keinen inhaltlichen Änderungen.

Artikel 7a *Beschaffung und Bearbeitung sicherheitsrelevanter Daten über Mitarbeiterinnen und Mitarbeiter, Stellenbewerberinnen und Stellenbewerber und Beauftragte*

Absatz 1

Der NDB kann auch bei bereits angestellten Mitarbeiterinnen und Mitarbeitern, die über eine gültige Personensicherheitsprüfung (PSP) nach dem Informationssicherheitsgesetz vom 18. Dezember 2020[18] (ISG) verfügen, im Falle eines Ereignisses, das Sicherheitsfragen aufwirft, Abklärungen durchführen. Je nach Ergebnis leitet er anschliessend eine Wiederholung der PSP ein. Anders als die Massnahmen nach Artikel 7 Absatz 1 Buchstabe e, müssen diese Abklärungen mit einer Information der betroffenen Person einhergehen (siehe auch die Erläuterungen zu Abs. 4) und sind zeitlich auf höchstens drei Monate zu befristen. Dies verhindert, dass Mitarbeiterinnen und Mitarbeiter des NDB jederzeit mit solchen Kontrollen zu ihrer Person rechnen müssen.

Absatz 2 und 3

Der NDB hat sich zu vergewissern, dass Personen, die in der engsten Auswahl für eine Anstellung beim NDB stehen, sowie Personen und Unternehmen, die sich für Aufträge des NDB bewerben oder solche ausführen, kein Risiko für die Sicherheit

[18] SR **128**

seiner Mitarbeiterinnen und Mitarbeiter, seiner Einrichtungen sowie der von ihm bearbeiteten Daten darstellen. Dafür müssen die mit Schutz- und Sicherheitsmassnahmen betrauten Mitarbeiterinnen und Mitarbeiter des NDB Abklärungen über diese Personen und Unternehmen durchführen können. Die betroffenen Personen bzw. Unternehmen müssen über diese Abklärungen informiert werden.

Die Abklärungen erfolgen durch die Abfrage der dem NDB zur Verfügung stehenden internen und externen Daten, das Einholen von mündlichen und schriftlichen Auskünften, namentlich auch bei den betroffenen Personen und Unternehmen, und das Konsultieren von öffentlich zugänglichen Informationsquellen. Die vorgesehenen Abklärungen begründen keine Pflicht externer Stellen, Daten speziell zu diesem Zweck zu erheben oder aufzubewahren. Es handelt sich um das Abfragen resp. Einholen ohnehin vorhandener Daten. Mit der vorliegenden Bestimmung wird auch keine neue Kompetenz des NDB zur Informationsbeschaffung geschaffen, die über das Abfragen und Einholen von Informationen nach diesem Absatz hinausgeht.

Diese frühzeitig geführten Abklärungen ersetzen nicht die Personensicherheitsprüfungen und Betriebssicherheitsverfahren nach dem ISG. Diese können jedoch nicht immer rechtzeitig vor der Anstellung erfolgen. Der NDB leitet sie nach Artikel 33 ISG ein, bevor die Person ihre Funktion beginnt. Ein Abschluss vor der Funktionsübernahme ist der Fachstelle PSP aus organisatorischen Gründen jedoch in den wenigsten Fällen möglich. Die angestellten Personen haben schon vor dem Ergebnis der PSP Zugang zu den Räumlichkeiten des NDB und Zugriff auf klassifizierte Dokumente. Ein sinnvoller praktischer Arbeitseinsatz ist nur möglich, wenn die Personen in ausreichendem Mass Zugriff auf die allgemeinen nachrichtendienstlichen Daten des NDB haben.

Absatz 4

Im Gegensatz zu den Massnahmen nach Artikel 7 Absatz 1 Buchstabe e hat der NDB die betroffene Person oder die betroffene Unternehmung in jedem Fall vorgängig über die Beschaffung oder Bearbeitung von Daten zu ihr zu informieren.

Absatz 5

Mehrere Kantone wollten im Rahmen der Vernehmlassung wissen, wie weit Artikel 7*a* E-NDG auch auf die Mitarbeiterinnen und Mitarbeiter der KND angewendet werden kann. Da die KND Daten des NDB bearbeiten, sollen die Schutz- und Sicherheitsmassnahmen nach den Absätzen 1–3 auch gegenüber Mitarbeiterinnen und Mitarbeitern der KND zum Einsatz kommen können.

Absatz 6

Das Beschaffen und Bearbeiten der Auskünfte und Daten nach Absatz 1 setzt die schriftliche Genehmigung der Direktorin oder des Direktors des NDB oder der vorgesetzten Stelle des KND voraus. Somit ist in jedem Fall mindestens das Vieraugenprinzip gewährleistet.

Artikel 8

Absatz 1

Im Sinn einer einheitlichen Terminologie wird der Ausdruck «Gefährdung» durch «Bedrohung» ersetzt.

Artikel 9

Absatz 3

Die KND haben die Pflicht, sämtlichen Hinweisen auf Tätigkeiten nach Artikel 6 Absatz 1 Buchstabe a nachzugehen und diese abzuklären. Dabei ist es möglich, dass die Abklärungen ergeben, dass es sich nicht um eine vom Aufgabengebiet des NDG abgedeckte Tätigkeit handelt, womit der Aufgabenbezug nicht gegeben ist (bspw. wendet sich ein besorgter Lehrer an einen KND, weil sich einer seiner Schüler islamischen Glaubens auffällig verhält und er eine Radikalisierung befürchtet; die Abklärungen des KND können diese Annahme aber nicht bestätigen). In einem solchen Fall dürfen die KND die bearbeiteten Daten zum Zweck der Nachvollziehbarkeit während fünf Jahren aufbewahren (vgl. Art. 58*a* E-NDG), erstatten dem NDB aber keinen Bericht. Bestätigt sich jedoch eine Bedrohung der inneren oder äusseren Sicherheit im Sinne des NDG, erstatten die KND dem NDB umgehend Bericht. Da der heutige Artikel 85 Absatz 2 den gleichen Regelungsinhalt aufweist, kann er aufgehoben werden (vgl. dazu die Ausführungen zu diesem Artikel).

Absatz 4

Neu wird klargestellt, dass der NDB der Verantwortliche im Sinne von Artikel 5 Buchstabe j DSG für die Datenbearbeitung der KND ist, soweit sich deren Datenbearbeitung auf das NDG stützt. Dabei ist unerheblich, ob die KND unaufgefordert oder gestützt auf einen konkreten Auftrag des NDB tätig werden. Dadurch entstehen dem NDB aber keine neuen Risiken, da er diese Verantwortung schon heute wahrnimmt und im Rahmen der Selbstkontrolle (vgl. Art. 75) die daraus resultierenden Risiken minimiert. Auskunftsgesuche, die bei den KND eingehen, bearbeitet der NDB gestützt auf die Artikel 63 ff.

Artikel 14

Absatz 3

Nach heutigem Recht (Art. 14) kann der NDB im Rahmen einer genehmigungsfreien Massnahme Vorgänge und Einrichtungen an öffentlichen und allgemein zugänglichen Orten beobachten und in Bild und Ton festhalten. Dazu gehört auch die begleitende Observation, d. h. das Verfolgen und Beobachten einer – in der Regel – Person oder eines Fahrzeugs über eine gewisse Dauer durch ein Observationsteam.

Die mit solchen Observationen beauftragten Mitarbeiterinnen und Mitarbeiter sind an die geltende Rechtsordnung gebunden. Entsprechend einfach ist es bisweilen für eine Zielperson, sich einer Observation zu entziehen und umso schwieriger für die observierende Person, den Kontakt zum Beobachtungsobjekt nicht unbeabsichtigt zu verlieren. So kann beispielsweise das Überfahren eines Rotlichts, das Überschreiten der zulässigen Höchstgeschwindigkeit oder etwa das Abbiegen im dichten Stadtverkehr ausreichen, damit das Observationsteam den Kontakt verliert. Dieses Gesetz soll des-

halb mit einer Bestimmung ergänzt werden, die es erlaubt, während genehmigungsfreien Observationen Ortungsgeräte (GPS-Sender) einzusetzen, um die Zielpersonen oder -objekte rasch wieder aufzufinden, falls der Sichtkontakt vorübergehend verloren gehen sollte. Zu diesem Zweck soll der bestehende Artikel 14 mit einem entsprechenden Absatz ergänzt werden. Zudem wird in Artikel 26 Absatz 1 Buchstabe b ein Vorbehalt eingefügt.

Der damit vorgeschlagene Einsatz eines Ortungsgeräts beschränkt sich auf die Übermittlung der aktuellen Koordinaten des Beobachtungsobjekts während der laufenden Observation, mit dem einzigen Zweck, die Kontinuität der Beobachtung zu gewährleisten. Geht der Kontakt zum Beobachtungsobjekt dauerhaft verloren, so ist die Übermittlung der Ortungsdaten zu beenden. Die Zeitdauer, bis der Kontakt als dauerhaft verloren gilt, ist dabei kurz bzw. verhältnismässig anzusetzen. Die observierenden Personen sollen verpflichtet werden, die Übermittlung nach spätestens einer Stunde zu beenden. Der Einsatz eines Ortungsgeräts während einer Observation ist somit einzig ein Hilfsmittel. Die Daten dürfen nicht für eine spätere Analyse oder andere Zwecke gespeichert werden. Ist die Speicherung der Daten für das Funktionieren des Ortungsgeräts aus technischen Gründen unverzichtbar, sind sie nach Beendigung der Observation umgehend zu vernichten. Sofern sich das Beobachtungsobjekt an einen nicht öffentlichen und nicht allgemein zugänglichen Ort begibt, ist die Datenübertragung des Ortungsgeräts zu beenden. Das Gleiche gilt, wenn das Observationsteam die Observation beendet. Will das Observationsteam zu einem späteren Zeitpunkt die Observation weiterführen, muss es das Beobachtungsobjekt mit den üblichen Mitteln auffinden. Erst wenn das Beobachtungsobjekt für das Observationsteam wieder sichtbar ist, darf die Übermittlung der Ortungsdaten wieder eingeschaltet werden. Solch detaillierte Regelungen gehören nach Ansicht des Bundesrates ins Verordnungsrecht, das anschliessend revidiert wird.

Die Frage, ob die Regelung von Artikel 14 Absatz 3 E-NDG in Verbindung mit Artikel 26 Absatz 1 Buchstabe b E-NDG angesichts des grundrechtlichen Privatsphärenschutzes nach Artikel 13 der Bundesverfassung (BV)[19] verfassungsmässig ist, wird unterschiedlich beurteilt. Gemäss diesen Bestimmungen ist der unterstützende Einsatz von Ortungsgeräten nicht genehmigungspflichtig, wenn er für die Kontinuität einer Observation erforderlich ist. Dies gilt selbst dann, wenn eine solche Massnahme wochen- oder sogar monatelang andauert. Auch eine nachträgliche Information der betroffenen Person und ein Rechtsmittelverfahren sind nicht vorgesehen.

Gemäss der bisherigen Beurteilung des Bundesrates bedeutet das Orten von Personen oder Sachen mittels GPS-Geräten einen starken Eingriff in das Recht auf Privatsphäre (Art. 13 BV).[20] Das Bundesgericht hat das in Bezug auf eine kantonale Rechtsgrundlage bestätigt. Einem jüngeren Leiturteil zufolge ist die präventiv-polizeiliche Überwachung mittels GPS-Gerät ohne vorgängige richterliche Genehmigung verfassungswidrig. Selbst eine nachträgliche Genehmigung allein reicht nicht aus, um die Grundrechte der Betroffenen zu wahren.[21] Dies liegt darin begründet, dass präventive

19 SR **101**
20 Botschaft vom 19. Februar 2014 zum Nachrichtendienstgesetz, BBl **2014** 2105 S. 2169.
21 BGE **147** I 103 E. 17.5.2

Überwachungsmassnahmen besonders hohe Risiken für die freiheitliche und demokratische Ordnung bergen, zumal Aufgaben- und Kompetenznormen im Polizei- und Nachrichtendienstrecht oftmals eine rechtsstaatlich heikle Offenheit aufweisen. Angemessene und wirksame verfahrensrechtliche Garantien gegen Missbräuche sind in diesem Bereich deshalb von zentraler Bedeutung.[22]

Dass die Anforderungen an den Einsatz von Ortungsgeräten anders zu beurteilen wären, wenn diese ausschliesslich vorübergehend zur Unterstützung einer Observation verwendet würden, ergibt sich aus diesem Leiturteil nicht. Dagegen spricht, dass die Intensität des Grundrechtseingriffs, die sich aus der unmittelbaren Beobachtung kombiniert mit der Ortungsmöglichkeit ergibt, nicht generell geringer, sondern potenziell sogar grösser ist als bei der ausschliesslichen Überwachung mittels Ortungsgeräten nach Artikel 26 Absatz 1 Buchstabe b E-NDG, da sich aus der Beobachtung gegenüber der blossen Ortung umfassendere Informationen ergeben. Diese Bewertung hat bislang auch der Bundesgesetzgeber vorgenommen, der in Kenntnis der Anwendungsszenarien[23] auch den unterstützenden Einsatz von Ortungsgeräten nach dem NDG der Genehmigungspflicht unterstellt hat. Ebenso erfordert der Einsatz von Ortungsgeräten nach der Strafprozessordnung (StPO)[24], selbst wenn er nur öffentliche Orte betrifft, sowohl eine vorgängige Genehmigung durch das Zwangsmassnahmengericht als auch die nachträgliche Information der betroffenen Person.[25] Letztere darf nur unter engen Voraussetzungen und vorbehaltlich der Zustimmung des Zwangsmassnahmengerichts aufgeschoben oder unterlassen werden. Namentlich muss der dringende Verdacht bestehen, die betroffene Person habe eine Straftat von erheblicher Schwere begangen. Das Bundesgericht orientierte sich bei der Bestimmung des verfassungsrechtlich zulässigen Rahmens des Einsatzes von Ortungsgeräten an diesen strafprozessualen Schranken sowie an der geltenden Regelung im NDG.[26] Dies spricht gegen die Verfassungsmässigkeit von Artikel 14 Absatz 3 E-NDG.

Der Bundesrat vertritt indes die Auffassung, dass sich das Bundesgericht im zitierten Leiturteil nicht im Speziellen zum Einsatz von Ortungsgeräten als Unterstützungsmassnahme von rechtlich zulässigen Observationen im nachrichtendienstlichen Bereich unter einschränkenden Bedingungen äussert. Er ist der Meinung, dass der in diesem Artikel vorgesehene Einsatz eines Ortungsgeräts von einem Einsatz nach Artikel 280 Buchstabe c StPO und nach Artikel 26 Absatz 1 Buchstabe b E-NDG zu unterscheiden ist. Diese beiden Artikel streben primär die dauernde Standortfeststellung und das Erfassen von Bewegungen über einen definierten Zeitraum an.

Beim vorliegend geplanten Einsatz eines Ortungsgeräts nach Artikel 14 Absatz 3 E-NDG handelt es sich hingegen um eine taktisch und zeitlich klar begrenzte Unterstützung. Es werden keine Daten beschafft, die nicht auch bei einem Einsatz auf Sicht beschafft würden. Der Eingriff in die Privatsphäre ist damit tendenziell nicht grösser als bei der Observation selbst. Dagegen ist eine Observation, wie bereits oben darge-

22 BGE **147** I 103 E. 16 und 17.5.1
23 BBl **2014** 2105 S. 2164
24 SR **312.0**
25 Art. 269–279 StPO i. V. m. Art. 281 Abs. 4 StPO
26 BGE **147** I 103 E. 17.4 und 17.5.2

legt, ohne Lokalisierung eines Zielobjekts heute äusserst schwierig und ohne Gefährdung von anderen Verkehrsteilnehmenden kaum mehr möglich. Die Unterstützung der Observation durch den Einsatz von Ortungsgeräten ohne richterliche Genehmigung erscheint deshalb als verhältnismässig. Ohnehin bleibt der NDB an die Grundsätze der Datenbeschaffung gebunden, die die Verhältnismässigkeit bei der Wahl der Beschaffungsmassnahme vorschreiben (Art. 5 Abs. 3).

Der Einsatz eines Ortungsgeräts nach diesem Artikel wird die ständige Überwachung mit Ortungsgeräten nach Artikel 26 Absatz 1 Buchstabe b E-NDG in Fällen von schweren Bedrohungen der Sicherheit der Schweiz nicht ersetzen.

Die meisten Kantone befürworteten anlässlich der Vernehmlassung diese neue Unterstützungsmöglichkeit für Observationen. Einige verlangten sogar eine offenere Formulierung, die es erlauben würde, die Standortbestimmung fortzusetzen, um nach einem Unterbruch der Observation diese anhand der gesendeten Standortdaten wieder aufnehmen zu können. Der Bundesrat hingegen vertritt den Standpunkt, dass die Bestimmung eng zu definieren ist, um den Unterschied zum Einsatz eines Ortungsgeräts nach Artikel 26 Absatz 1 Buchstabe b E-NDG hervorzuheben und um der Rechtsprechung des Bundesgerichts Rechnung zu tragen.

Artikel 17

Absatz 2

Die Direktorin oder der Direktor des NDB kann bereits heute bewilligen, dass Mitarbeiterinnen und Mitarbeiter eines KND mit einer Legende ausgestattet werden. Die Bestimmung wird sprachlich an den neuen Absatz 2^{bis} angepasst, inhaltlich ändert sich nichts.

Absatz 2^{bis}

Wenn der NDB bei der Informationsbeschaffung mit inländischen Amtsstellen zusammenarbeitet, kann es notwendig sein, deren Mitarbeiterinnen und Mitarbeiter genauso zu schützen, wie solche des NDB oder der KND. Somit sollen u. a. auch die Instrumente der Legendierung (Art. 17) oder Tarnidentität (vgl. Erläuterungen zu Art. 18) zum Einsatz kommen können. Artikel 17 wird deshalb entsprechend durch einen Absatz 2^{bis} ergänzt. Im Vordergrund stehen dabei die vom NDB mit Beschaffungen im Cyberraum beauftragten Dienststellen des VBS (Computer Network Operations [CNO] des CEA des Kommandos Cyber). Es ist auch nicht ausgeschlossen, dass zum Beispiel Mitarbeitende der Armee im Rahmen einer besonderen Operation durch den NDB beauftragt werden (subsidiärer Sicherungseinsatz) und zu diesem Zweck mit einer Legende ausgestattet werden.

Der Anwendungsbereich der Bestimmung erfasst auch Mitarbeiterinnen und Mitarbeiter kantonaler Amtsstellen, die im Auftrag des NDB tätig sind. So kann z. B. die Ausstattung mit einer Legende notwendig sein, wenn Angehörige einer Kantonspolizei dem NDB logistischen Support leisten oder einen KND bei einem grösseren Einsatz operativ unterstützen. Bewilligungen zur Ausstattung mit einer Legende sollen

aber auf kantonaler Stufe nur sehr zurückhaltend erteilt werden, auch weil eine Legendierung jeweils eine gezielte Ausbildung und Begleitung erfordert und daher mit einem beträchtlichem Aufwand verbunden ist.

Artikel 18

Absatz 1 Buchstaben b und b^{bis}

Wenn der NDB bei der Informationsbeschaffung mit inländischen Amtsstellen zusammenarbeitet, kann es notwendig sein, deren Mitarbeiterinnen und Mitarbeiter genauso zu schützen, wie solche des NDB oder der KND. Im Vordergrund stehen dabei die vom NDB mit Beschaffungen im Cyberraum beauftragten Dienststellen des VBS (CNO). Artikel 18 Absatz 1 wird deshalb entsprechend durch einen Buchstaben b^{bis} ergänzt. Betreffend den Anwendungsbereich kann auf die Ausführungen zu Artikel 17 Absatz 2bis E-NDG verwiesen werden. Die Anpassung in Buchstabe b ist hingegen rein sprachlicher Natur, es handelt sich um eine Angleichung an die Formulierung in Buchstabe b^{bis}.

Absatz 2 Buchstabe a

In diesem Gesetz wird durchgehend der Ausdruck «kantonale Vollzugsbehörde» verwendet. Absatz 2 Buchstabe a wird entsprechend angepasst.

Artikel 19

Absatz 2 Buchstabe f

Die Sicherheit im Cyberraum gewinnt zunehmend an Bedeutung. Deswegen wird analog zur neuen Formulierung in Artikel 6 Absatz 1 Buchstabe b auch der Katalog der möglichen Bedrohungsquellen im Zusammenhang mit dem Auskunftsrecht bei konkreten Bedrohungen um die sicherheitspolitisch bedeutsamen Vorgänge im Ausland und im Cyberraum ergänzt.

Artikel 20

Absatz 1 Buchstabe b

Diese Anpassung ist aufgrund der neuen Bezeichnung infolge der Reorganisation der Eidgenössischen Zollverwaltung nötig und beinhaltet keine Änderung materieller Natur. Tritt die Totalrevision des Zollgesetzes (BAZG-Vollzugsaufgabengesetz vom 20. Juni 2025[27] [BAZG-VG]) vor dieser Vorlage in Kraft, so ist diese Anpassung hinfällig.

Absatz 1 Buchstabe i

Behörden, die für den Betrieb von Informatiksystemen zuständig sind oder andere darin unterstützen, sollen dem NDB Auskünfte bezüglich sicherheitspolitisch relevanter Cyberangriffe erteilen, damit der NDB eine umfassende Lagedarstellung im Cy-

27 BBl **2025** 2035

berbereich vornehmen und gegebenenfalls Massnahmen zur Erkennung und Verhinderung von Cyberangriffen ergreifen kann. Diese Bestimmung ersetzt keinesfalls die gesetzlichen Vorgaben zum Schutz des Fernmeldegeheimnisses, die bei spezifischen Überwachungsmassnahmen jeweils einzuhalten sind.

Absatz 1 Buchstabe j

In Einklang mit den gesetzestechnischen Richtlinien wird hier einzig die Abkürzung des GwG eingefügt und eine sprachliche Angleichung an das GwG vorgenommen.

Artikel 23

Absatz 2

Hier handelt es sich lediglich um eine Vereinheitlichung der in diesem Gesetz verwendeten Terminologie.

Artikel 25

Absatz 1 Buchstabe a

Die Auskunftspflicht Privater wird auf die gewerbsmässigen Betreiberinnen von Beherbergungsbetrieben ausgedehnt. Diese verfügen wie die schon bisher verpflichteten Transportunternehmungen oft über Informationen und Daten, die für das frühzeitige Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit erforderlich sind. Somit könnte der NDB temporäre Aufenthaltsorte von Zielpersonen ermitteln und je nach Situation auch Kontaktpersonen einer Zielperson, wenn z. B. die Zielperson für mehrere Hotelzimmer zahlt oder ihr Zimmer von Dritten bezahlt wird. Es könnte auch ermittelt werden, welche Organisation Räume mietet, um ein Treffen zu organisieren.

Der Begriff «Beherbergungsbetrieb» umfasst sämtliche Betreiberinnen, die (meist gegen Entgelt) Personen eine Übernachtungsmöglichkeit zur Verfügung stellen. Die Daten über den gewerblich organisierten Austausch von Wohnungen und Häusern fallen auch darunter.

Die Auskunftspflicht Privater wird ebenfalls auf die gewerbsmässigen Betreiberinnen von Transportinfrastrukturen ausgedehnt. Der Bundesrat teilt die anlässlich der Vernehmlassung von verschiedenen Kantonen geäusserte Meinung, dass Betreiberinnen von Flughäfen, Bahnhöfen, Häfen usw. auch in die Aufzählung der Privaten mit besonderen Auskunftspflichten aufgenommen werden müssen. Der Begriff «Infrastrukturanlagen für den Transport» beschränkt sich nicht auf den Luftverkehr, sondern entspricht auch Infrastrukturen für Schiff- und Bahntransport.

Die grundsätzlichen Regelungen über die Datenspeicherung oder Meldepflichten der Betreiberinnen von Beherbergungsbetrieben und Infrastrukturanlagen richten sich weiterhin nach kantonalem Recht. Dieses Gesetz führt weder neue Pflichten zur Datenerhebung noch zur Datenaufbewahrung ein, sondern nur den Zugriff auf bereits vorhandene Daten auf Anfrage des NDB oder der KND. Wie bis anhin werden die Auskünfte nur in Einzelfällen verlangt. Hierbei ist zu betonen, dass sich «Einzelfall» nicht auf eine einzelne Person beziehen muss, sondern bspw. auch eine bestimmte,

mit Risiken verbundene Veranstaltung betreffen kann wie das World Economic Forum oder eine internationale Konferenz wie die Ukraine Recovery Conference, die im Juli 2022 in Lugano stattfand.

Als Verband für Hotellerie und Restauration in der Schweiz begrüsste GastroSuisse anlässlich der Vernehmlassung explizit, dass die besondere Auskunftspflicht Privater nur in Einzelfällen und auf Verlangen hin besteht, und dass die Änderung dieses Gesetzes zu keinen neuen Pflichten bei der Datenerhebung oder der Datenaufbewahrung führen wird. Unabhängig von der Änderung des NDG spricht sich GastroSuisse betreffend die Meldepflicht nach Artikel 16 des Bundesgesetzes vom 16. Dezember 2005[28] über die Ausländerinnen und Ausländer und über die Integration (AIG) für eine digitale nationale Lösung aus und geht davon aus, dass bei Eintritt einer solchen auch die Auskunftsersuchen des NDB oder der KND über diese digitale Lösung abgewickelt werden könnten. So könnte der durch die Auskunftspflicht erhöhte Aufwand auf Seiten der Beherbergungsbetriebe – und auch der Behörden – besser abgefedert werden.

Der Bundesrat verzichtet darauf, besondere Auskunftsplichten für Gesundheitsfachleute in diese Bestimmung aufzunehmen, wie mitunter in der Vernehmlassung vorgeschlagen wurde. Es wäre ein schwerer Eingriff in das Berufsgeheimnis, der sich nicht rechtfertigen lässt. Eine Gesundheitsfachperson kann sich von ihrem Berufsgeheimnis entbinden lassen und eine Meldung an den NDB bzw. einen KND machen, wenn sie überzeugt ist, dass ihr Patient eine Gefährdung für die Sicherheit der Schweiz darstellt. Diese Entbindung vom Berufsgeheimnis ist kantonalrechtlich geregelt.

Absatz 3

Gleich wie die Behörden nach den Artikeln 19 und 20 sollen auch Private neu verpflichtet werden, gegenüber Dritten ein allfälliges Auskunftsersuchen des NDB geheim zu halten. Dies entspricht dem Grundsatz der Informationsbeschaffung nach Artikel 5 Absatz 4.

4. Abschnitt:

Die heutigen Bestimmungen über die GEBM sollen aufgrund der ersten Erfahrungen in der Anwendung sowie aufgrund des anlässlich verschiedener parlamentarischer Vorstösse[29] erkannten Handlungsbedarfs angepasst werden. Erstens soll eine neue GEBM eine Lücke in der Datenbeschaffung schliessen. Der NDB hat heute keine Möglichkeiten, Informationen von Finanzintermediären über die Finanzierung von sicherheitsrelevanten Personen und Gruppierungen zu erhalten. Mit dieser neuen GEBM, die die Überwachung der über Banken und ähnliche Institutionen abgewickelten Finanzbeziehungen bestimmter Personen ermöglicht, wird eine Lücke in der Datenbeschaffung geschlossen (siehe Erläuterungen zu Art. 26 Abs. 1 Bst. f und g) und dem NDB die Möglichkeit eröffnet, wertvolle Informationen zu beschaffen. Hingegen wird die Anzahl durchgeführter GEBM dadurch nicht viel höher sein als heute (siehe Erläuterungen zu Art. 27 Abs. 1 Bst. a Ziff. 1).

28 SR **142.20**
29 Z. B. Po 17.3831 und Mo 20.4568.

Weiter soll der Anwendungsbereich der GEBM auf den gewalttätigen Extremismus ausgedehnt werden (siehe Erläuterungen zu Art. 27 Abs. 1 Bst. a). Wie bisher sind auch beim Einsatz der neuen Finanzauskunft oder beim Einsatz zur Aufklärung des gewalttätigen Extremismus die strengen Voraussetzungen nach Artikel 27 einzuhalten.

Der heutige Artikel 29 wird neu in mehrere Artikel unterteilt. Diese neue Struktur der Regelung des Genehmigungsverfahrens bringt eine bessere Trennung der Inhalte mit sich.

Artikel 26

Absatz 1

Im Sinne einer Klarstellung wird im Einleitungssatz zu Absatz 1 ergänzt, dass die im Folgenden aufgeführten Beschaffungsmassnahmen nur dann genehmigungspflichtig sind, wenn sie auf Schweizer Staatsgebiet durchgeführt werden. Für Massnahmen im Ausland ist hingegen keine Genehmigung durch das Bundesverwaltungsgericht möglich. Begibt sich eine Zielperson einer in Vollzug stehenden Massnahme ins Ausland, so gelten die Bestimmungen des 6. und 7. Abschnitts. Über das Eindringen in Computersysteme und Computernetzwerke im Ausland nach Artikel 37 entscheidet entweder der Bundesrat (Art. 37 Abs. 1) oder die Vorsteherin oder der Vorsteher des VBS nach vorheriger Konsultation der Vorsteherinnen oder Vorsteher des EDA und des EJPD (Art. 37 Abs. 2).

Buchstabe b

Hier soll der Hinweis eingefügt werden, dass Ortungsgeräte im Rahmen laufender Beobachtungsmassnahmen («Observation») genehmigungsfrei verwendet werden können. Es kann auf die vorstehenden Erläuterungen zu Artikel 14 Absatz 3 E-NDG verwiesen werden.

Buchstaben f und g

Diese neuen GEBM orientieren sich an den Artikeln 284 und 285 StPO und ermöglichen die Überwachung der Beziehungen zwischen einer Zielperson des NDB und Institutionen, die dem GwG unterstellt sind. Sie unterliegen den gleichen strengen Voraussetzungen (Art. 27 Abs. 1) wie die heute bereits möglichen GEBM. Gleich wie die erwähnten Bestimmungen der StPO bilden sie eine gesetzliche Grundlage für Eingriffe in das Bankgeheimnis und entsprechen somit den Bestimmungen, die unter den Vorbehalt von Artikel 47 Absatz 5 des Bankengesetzes vom 8. November 1934[30] betreffend die Verletzung des Berufsgeheimnisses fallen. Sie stipulieren eine Auskunftspflicht der Institutionen, die dem GwG unterstellt sind, gegenüber den Behörden.

Hierzu ist festzuhalten, dass mit diesen neuen Kompetenzen keine parallelen Zuständigkeiten des NDB und der Strafverfolgungsbehörden geschaffen werden. Der Fokus des NDB ist auf die Früherkennung von Bedrohungen gerichtet, er erfüllt eine eigenständige, sicherheitspolitische Aufgabe, nicht eine strafrechtliche. Zudem hat auch der NDB ein Interesse an einem möglichst effizienten und ressourcenschonenden Einsatz

30 SR **952.0**

behördlicher Mittel und damit an der Vermeidung entsprechender Doppelspurigkeiten. Nicht zuletzt soll auch der in Artikel 29*a* E-NDG statuierte Mechanismus im Rahmen eines Antrags auf GEBM genau dies verhindern.

Weil die Auskünfte, die verlangt werden können, von Fall zu Fall variieren können, ist es nach Meinung des Bundesrates nicht sinnvoll, diese im Gesetzestext zu konkretisieren, wie es teilweise von den Vernehmlassungsteilnehmenden gewünscht wurde. Deswegen wird im Antrag nach Artikel 29 fallweise explizit beschrieben werden müssen, welche Aufzeichnungen und Dokumente zu liefern sind. Zu denken ist bspw. an Kontoauszüge, Zahlungsverkehr oder Vollmachten. Die Bestimmung übernimmt zwar nicht Wort für Wort diejenige in der StPO, soll aber vom Umfang her nicht über diese hinausgehen. Mit dem Verweis auf Artikel 2 GwG entspricht der Kreis der betroffenen Personen und Institutionen, die unter der neuen GEBM auskunftspflichtig werden, jenem des Geltungsbereichs des GwG.

Namentlich für die Finanzierung des Terrorismus werden nicht nur die grossen institutionalisierten Banken genutzt, sondern auch Dienste von kleineren Unternehmen, die Dienstleistungen im internationalen Geldtransfer anbieten, oder auch von Personen, die Bargeld tauschen. Deswegen übernimmt das NDG vom GwG die Definition des Kreises potenziell betroffener Personen, bei denen das Einholen von Auskünften über Transaktionen und Geschäftsbeziehungen möglich ist. Die Transparenz über diese Geldflüsse, die dank der Überwachung der Beziehungen möglich wird, dient dem NDB zur Erfüllung aller seiner Aufgaben nach Artikel 6.

Von Interesse für den NDB sind die Hintergründe der Finanzierung von Organisationen und Gruppierungen, die bereits aufgrund anderer Informationen in seinen Fokus geraten sind. Durch eine gezielte Überwachung kann die Bedrohung der inneren oder äusseren Sicherheit der Schweiz durch eine Organisation oder Gruppierung besser eingeschätzt werden. Zu denken ist beispielsweise an kommerzielle Unternehmen, ideelle Organisationen oder religiöse Einrichtungen, zu denen begründete Anhaltspunkte vorliegen, dass sie an terroristischen, nachrichtendienstlichen, proliferationsrelevanten oder gewalttätig-extremistischen (siehe Erläuterungen zu Art. 27 Abs. 1 Bst. a.) Umtrieben beteiligt sind, namentlich an deren Finanzierung. Informationen über die Herkunft der Finanzierung können dem NDB zusätzliche schlüssige Elemente liefern, um eine Bedrohung der inneren oder äusseren Sicherheit der Schweiz frühzeitig erkennen und verhindern zu können.

Heute hat der NDB nur sehr begrenzt Möglichkeiten, an Informationen betreffend die Finanzierung einer Einrichtung zu gelangen. So kann er unter bestimmten Voraussetzungen im Einzelfall Informationen von der Meldestelle für Geldwäscherei (MROS) erhalten (Art. 29 Abs. 2^{bis}-2^{ter} i. V. m. Art. 30 und 31 GwG sowie Art. 20 Abs. 1 Bst. j NDG).

Die MROS ist als schweizerische «Financial Intelligence Unit» (FIU) die nationale Zentralstelle, die nach dem GwG Verdachtsmeldungen bezüglich Geldwäscherei, Terrorismusfinanzierung, Geldern aus Vortaten zur Geldwäscherei oder krimineller Organisationen von den dem GwG unterstellten Instituten entgegennimmt, analysiert (Art. 23 Abs. 2 GwG), Informationen auf nationaler und internationaler Ebene austauscht (Art. 29 und 30 GwG) und bei einem begründeten Verdacht Anzeige an die zuständige Strafverfolgungsbehörde erstattet (Art. 23 Abs. 4 GwG).

Diese Auflistung der Aufgaben der Meldestelle kann prima vista zur Schlussfolgerung verleiten, dass der bestehende Informationsaustausch zwischen ihr und dem NDB das Ziel der Neuregelung bereits erfüllt. Das ist allerdings nicht der Fall: Die Meldungen von Finanzintermediären an die MROS setzen den begründeten Verdacht beispielsweise auf Terrorismusfinanzierung voraus (Art. 9 GwG). Die Tatsache allein, dass eine ideelle Organisation beispielsweise ihre Mitglieder zu Gewalttätigkeiten aufruft, berechtigt die Finanzintermediäre jedoch noch nicht zu einer Meldung an die Meldestelle. Dazu kommt, dass ein Finanzintermediär nur dann eine Meldung erstattet, wenn er die Zwecke der Terrorismusfinanzierung auch erkennt. Schliesslich hat die MROS auch bei einer Bekanntgabe von Informationen das für FIU international geltende und streng einzuhaltende Spezialitätsprinzip zu gewährleisten. Nach diesem wichtigen Grundsatz der internationalen Zusammenarbeit dürfen zwischen FIU ausgetauschte Informationen nur zu den Zwecken verwendet werden, für die sie verlangt und erteilt wurden, siehe dazu das in Ziffer 3 der Interpretativnote zu Empfehlung 40 der «Groupe d'action financière» (GAFI) erläuterte Spezialitätsprinzip[31]. Die Meldestelle als Behörde, die die Informationen erhält, muss die Auflagen der Behörde einhalten, von der die Information stammt. Dies gilt auch, wenn von einer ausländischen Stelle erhaltene Informationen mit deren Zustimmung an eine nationale Behörde bekannt gegeben werden (vgl. dazu Art. 29 Abs. 2ter GwG).

Die Aufgabe des NDB ist eine andere als die der MROS: Der NDB ist im präventiven Bereich der Informationsbeschaffung tätig und selbst für die Informationsbeschaffung zwecks Wahrung der inneren oder äusseren Sicherheit zuständig. Wenn er konkrete Anhaltspunkte hat, dass beispielsweise eine religiöse Einrichtung Personen rekrutiert, um die innere oder äussere Sicherheit der Schweiz schwerwiegend zu bedrohen, dann soll er die Möglichkeit erhalten, zwecks Vervollständigung seiner Bedrohungseinschätzung Informationen zur Finanzierung und damit auch zur Vernetzung dieser Einrichtung verlangen zu können. Diese Informationen können im Einzelfall eine wichtige Grundlage liefern, um weitere Massnahmen zu treffen, wie beispielsweise ein Tätigkeitsverbot nach Artikel 73. Die Neuregelung soll somit eine wichtige Lücke im Instrumentarium der Datenbeschaffung des NDB schliessen.

Die wirtschaftlichen Verhältnisse einer Person gehören zu deren Privatsphäre und bilden daher einen Teilgehalt des Grundrechts auf Schutz der Privatsphäre nach Artikel 13 BV und Artikel 8 der Konvention 4. November 1950[32] zum Schutze der Menschenrechte und Grundfreiheiten (EMRK). Die vorgesehene Massnahme bringt also einen Eingriff in die Privatsphäre betroffener Personen mit sich und verpflichtet zudem die dem GwG unterstellten Institutionen entgegen dem Bankgeheimnis zur Auskunftserteilung, weshalb sie als GEBM nach diesem Gesetz ausgestaltet werden soll. GEBM sind an sehr strenge Voraussetzungen gebunden und benötigen sowohl eine Genehmigung durch das Bundesverwaltungsgericht als auch eine Freigabe durch die Vorsteherin oder den Vorsteher des VBS.

31 Recommandations du GAFI - Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération (2012–2025) S. 32 und S. 132. Abrufbar unter: www.fatf-gafi.org > Sujets > Recommandations du GAFI.

32 SR **0.101**

Diese neue Massnahme der Datenbeschaffung ist folglich zum bereits existierenden Informationsaustausch zwischen dem NDB und der MROS komplementär (vgl. Art. 29 Abs. 2bis und 2ter GwG i. V. m. Art. 30 und 31 GwG sowie Art. 20 Abs. 1 Bst. j NDG). Es ist wichtig, dass mit dieser neuen Massnahme das Informationsverbot nach Artikel 10*a* GwG nicht verletzt wird. Dieses setzt das Verbot der Datenbekanntgabe an die betroffene Person gemäss den Standards der GAFI um. Die Kundin oder der Kunde des Finanzinstituts darf nicht merken, dass gegen sie oder ihn eine Verdachtsmeldung vorliegt. Dies könnte die Strafverfolgung und insbesondere die Beweiserhebung gefährden.

Diese zusätzliche GEBM benötigt der NDB nicht nur zur Aufgabenerfüllung im Bereich des Terrorismus. Auch für das frühzeitige Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit, die von verbotenem Nachrichtendienst ausgehen, können Erkenntnisse aus Finanzdaten wichtig sein. So können beispielsweise Informationen über die Finanzierung von als Tarnung dienenden Infrastrukturen wie Unterkünfte oder über Abonnemente von Fernmeldeanschlüssen, die dem Kontakt mit Quellen dienen, von hohem Interesse sein. Auch möglich sind die Entdeckung bzw. die Bestätigung der Existenz einer Scheinfirma, wenn einzig Personen, die der NDB als verdeckte Agentinnen oder Agenten identifizieren kann, Konten dieser Firma benutzen. Je nach Lage ist es somit möglich, Personen zu identifizieren, die in der Schweiz für einen anderen Staat tätig sind.

Im Bereich des gewalttätigen Extremismus (siehe Erläuterungen zu Art. 27 Abs. 1 Bst. a.) können Auskünfte über Finanztransaktionen Erkenntnisse dazu liefern, welche Immobilien von Personen, die als gewalttätige Extremisten identifiziert wurden, erworben wurden oder unterhalten werden, welche Güter diese Personen erwerben und welche Personen und Organisationen sie finanziell unterstützen oder von ihnen unterstützt werden. Ebenfalls können Informationen über die Finanzierung von Grossanlässen gewalttätig-extremistischer Gruppierungen für die Netzwerkaufklärung benötigte Erkenntnisse liefern.

In ihrer Stellungnahme im Rahmen der Vernehmlassung fordert die SP eine öffentlich zugängliche Auflistung der auf Finanzintermediäre bezogenen GEBM. Ohne Rückschlüsse auf Individuen oder einzelne Institutionen zuzulassen, soll öffentlich ersichtlich gemacht werden, welche Arten von Institutionen durch die neue Regelung überwacht wurden. Bereits heute erstellt die Präsidentin oder der Präsident der zuständigen Abteilung des Bundesverwaltungsgerichts jedes Jahr einen Tätigkeitsbericht zuhanden der Geschäftsprüfungsdelegation (Art. 29 Abs. 8 NDG bzw. Art. 29*c* E-NDG). Dieser Bericht wird mit den neuen Beschaffungsmassnahmen ergänzt werden, sofern diese zur Anwendung gekommen sind. Der Bundesrat wird im Rahmen der anschliessenden Revision des Verordnungsrechts prüfen, ob eine Veröffentlichung wie die geforderte notwendig ist, falls eine solche denn ohne Rückschlüsse auf Institutionen überhaupt möglich ist. Im Übrigen veröffentlicht bereits heute der Dienst ÜPF Statistiken zu Überwachungsmassnahmen nach dem Bundesgesetz vom 18. März 2016[33] betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF).

[33] SR **780.1**

Artikel 27

Absatz 1 Buchstabe a

Zur besseren Lesbarkeit wird dieser Buchstabe in Ziffern unterteilt.

Ziffer 1

Seit dem Inkrafttreten des NDG haben sich die Tätigkeiten der gewalttätigen rechts- und linksextremistischen Szenen intensiviert. Die Aggressivität gegenüber Sicherheitskräften und das allgemeine Gewaltpotenzial dieser Gruppen haben zugenommen. Die aktuelle Gewaltanwendung seitens Rechtsextremistinnen und Rechtsextremisten ist zwar noch relativ tief, diese besuchen aber Kampfsportausbildungen und bewaffnen sich zunehmend. Damit steigt die Risikobereitschaft, Auseinandersetzungen mit Andersdenkenden zu suchen. Besonders im Fokus stehen Fälle von Minderjährigen und jungen Erwachsenen, die sich online radikalisieren und gewalttätige extremistische Absichten entwickeln. Eine wichtige Bedeutung kommt dabei vor allem abgeschirmten Diskussionsgruppen aus dem Bereich des Akzelerationismus zu, in denen drastische Gewaltdarstellungen und Absichten zur Gewaltanwendung geteilt werden. Dementsprechend sind seit 2020 Vorfälle mit gewalttätigen Elementen im Bereich Rechtsextremismus wahrscheinlicher geworden. Gewalttätige Linksextremistinnen und Linksextremisten sind international stark vernetzt und ihre Gewaltausübung gegen Behörden und ideologisch entgegengesetzte Gruppen intensiviert sich zunehmend. In den letzten Jahren hat sich die Quantität der Gewalt gewalttätiger linksextremistischer Gruppen zwar nicht erhöht, wohl aber deren Qualität und Intensität. Diese Zunahme der Qualität und Intensität der Gewalt bzw. des Gewaltpotenzials erfolgt jedoch nicht linear, sondern verläuft vielmehr in einer Art Wellenbewegung (siehe auch den Bericht des Bundesrates vom 13. Januar 2021[34] in Erfüllung des Postulats 17.3831 Glanzmann-Hunkeler: Griffige Instrumentarien gegen Gewaltextremismus).

Zudem ist mit der Covid-19-Pandemie ein neues Gewaltpotenzial entstanden. Einzelne radikalisierte Personen wenden sich seither neuen Themenfeldern zu, um weiterhin gewalttätig aktiv sein zu können. Mit der Fragmentierung und Polarisierung der Gesellschaft ist das Risiko von politischer Radikalisierung und gewalttätigem Extremismus verbunden (siehe Bericht des Bundesrates vom 9. November 2022[35] an die eidgenössischen Räte und die Öffentlichkeit, Jährliche Beurteilung der Bedrohungslage). Möglich ist auch die Gewaltanwendung durch weitere Bewegungen (z. B. zu den Themen Tierrecht, Klima, Staatsverweigerung), um ihre politischen Forderungen durchzusetzen. Solche neuen Bewegungen, die teilweise Gewalt ausüben, unterteilen sich nicht in klassischen Links- oder Rechtsextremismus. Sie laufen unter der Bezeichnung «monothematischer Extremismus». In den öffentlich zugänglichen sozialen Medien stellt der NDB fest, dass seit 2020 immer mehr Propagandavideos und Fotografien von einschlägigen Ereignissen gepostet werden.

34 Abrufbar unter: www.parlament.ch > 17.3831 > Bericht in Erfüllung des parlamentarischen Vorstosses.
35 BBl **2022** 2754

Bei gewalttätigem Extremismus handelt es sich um Organisationen und Personen, welche die demokratischen und rechtsstaatlichen Grundlagen ablehnen und zum Erreichen ihrer Ziele Gewalttaten verüben, fördern oder befürworten (vgl. Art. 19 Abs. 2 Bst. e). Zwar wurden beim Erlass des NDG GEBM zur Aufklärung von gewalttätig-extremistischen Tätigkeiten noch ausgenommen, doch hat sich bei Ereignissen im Ausland gezeigt, dass solche Tätigkeiten auch Ausmasse annehmen können, die die innere oder äussere Sicherheit schwer bedrohen. Nach neueren Lageentwicklungen nehmen die Radikalisierung und Gewaltbereitschaft von den Behörden als gewalttätig-extremistisch bekannten Personen auch in der Schweiz deutlich zu.

Hinweise auf Waffen-, Munitions- und Sprengstoffbeschaffungen und entsprechende Ausbildungen sind für sich allein noch kein Grund zur Annahme, dass eine gewalttätig-extremistische Person die Schwelle zum Terrorismus überschreiten wird. Ob es sich im Einzelfall um eine gewalttätig-extremistische oder terroristische Aktivität handelt, hängt von der Zielsetzung, Intensität und Schwere der Handlung sowie deren Zusammenhang ab. All dies lässt sich oft erst nach der Tat erkennen.

Ohne den Einsatz von GEBM sind entsprechende Entwicklungen kaum zu erkennen. Die gewalttätig-extremistischen Szenen benutzen zunehmend verdeckte Vorgehensweisen, die der NDB mit den heute zulässigen genehmigungsfreien Informationsbeschaffungsmassnahmen nur unzureichend aufklären kann. Deshalb soll bei gravierenden Formen von gewalttätig-extremistischen Tätigkeiten mit potenziellen Schäden auch an Leib und Leben ebenfalls der Einsatz von GEBM ermöglicht werden. Zu denken ist an Fälle, in welchen Erkenntnisse bestehen, dass gewalttätig-extremistische Personen sich bewaffnen, ausbilden und sich gleichzeitig einerseits stärker von der Aussenwelt abkapseln und sich andererseits zunehmend – namentlich in sozialen Medien – mit bereits erfolgten terroristischen Anschlägen befassen und sich dazu äussern. Die Schwelle zu strafbaren Vorbereitungshandlungen ist in solchen Fällen meist noch nicht gegeben und die Personen haben keine Bezüge zu bekannten terroristischen Gruppierungen. Meistens ist zudem noch nicht bekannt, an welchem Ort, zu welcher Zeit oder auf welche Weise die gewalttätige Handlung erfolgen wird. Bedrohungsbeurteilungen sind mit prognostischen Unsicherheiten verbunden. Vorhandene Informationen können aber auf eine schwere Bedrohung der Sicherheit hinweisen, die vertieft aufgeklärt werden sollte (siehe Bericht des Bundesrates in Erfüllung des Postulats 17.3831 Glanzmann-Hunkeler: Griffige Instrumentarien gegen Gewaltextremisten).

Sind die präventiven Mittel in der Schweiz lückenhaft, besteht die erhebliche Gefahr, dass die Schweiz zu einem Rückzugsort oder Treffpunkt für ausländische gewalttätig-extremistische Personen wird (siehe Stellungnahme des Bundesrates vom 13. Mai 2020[36] auf das Postulat Jositsch vom 12. März 2020: 20.3100 «Überprüfung der Wirksamkeit des neuen Nachrichtendienstgesetzes»). Deshalb werden heute sowohl auf kantonaler wie auch auf Bundesebene (siehe z. B. Postulat Glanzmann-Hunkeler vom 28. September 2017: 17.3831 «Griffige Instrumentarien gegen Gewaltextremismus») GEBM auch für die Früherkennung und Verhinderung von gewalttätig-extremistischen Tätigkeiten gefordert, die die Sicherheit schwerwiegend bedrohen. Die

36 Abrufbar unter: www.parlament.ch> 20.3100.

bisherigen Erfahrungen mit den GEBM zeigen, dass deren Einsatz geeignet ist, zielgerichtete und punktgenaue Einzelfallabklärungen in schweren Fällen vorzunehmen. Der NDB setzt diese Mittel zurückhaltend und nur in Fällen von schweren Bedrohungen ein. Die Massnahmen müssen zudem vom Bundesverwaltungsgericht auf Notwendigkeit und Verhältnismässigkeit geprüft und genehmigt werden. 2017 kamen in 4 Operationen GEBM zur Anwendung, 2018 in 8 Operationen, 2019 in 5 Operationen, 2020 in 4 Operationen, 2021 in 2 Operationen, 2022 in 4 Operationen, 2023 in 2 Operationen, und 2024 in 6 Operationen. Diese Zahlen zeigen, dass der NDB diese Massnahmen zurückhaltend und nur in den vom Gesetz vorgesehenen Fällen von schweren Bedrohungen einsetzt.

Die Sicherheit im Cyberraum gewinnt zunehmend an Bedeutung und Cyberangriffe haben vermehrt eine sicherheitspolitische Relevanz. Der geltende Begriff des Angriffs auf kritische Infrastrukturen im NDG hat sich in diesem Zusammenhang als zu eng erwiesen, um alle sicherheitspolitisch relevanten Vorgänge im Cyberraum abzudecken. Nähere Ausführungen dazu finden sich in den Erläuterungen zu Artikel 6 Absatz 1 Buchstabe b. Ergänzend zur neuen Formulierung in Artikel 6 Absatz 1 Buchstabe b und der Ergänzung des Katalogs der möglichen Bedrohungsquellen in Artikel 19 Absatz 2 soll dieser Entwicklung Rechnung getragen werden, indem künftig GEBM auch bei Vorliegen einer konkreten Bedrohung ausgehend von sicherheitspolitisch bedeutsamen Vorgängen im Ausland oder im Cyberraum eingesetzt werden können. Die Praxis der Aufklärungstätigkeit des NDB hat gezeigt, dass sicherheitspolitisch bedeutsame Bedrohungen aus dem Ausland durchaus auch Schweizer Komponenten haben können, die der NDB in der Schweiz aufklären können muss, z. B. Aufenthalte von Akteuren in der Schweiz oder die Nutzung von Schweizer Kommunikationsmitteln durch solche Akteure. Bei entsprechend schweren Bedrohungen ist es deshalb angezeigt, diese auch fallweise mittels GEBM in der Schweiz aufklären zu können. Bei Bedrohungen mit Cybermitteln lässt sich andererseits oft erst mit der Aufklärung des Datenverkehrs oder des Inhalts der beteiligten Computersysteme in der Schweiz erkennen, wo sich die Verursacher dieser Bedrohungen befinden. Es ist deshalb notwendig, den Cyberraum auch rechtlich als das zu behandeln, was er ist (siehe dazu die Definition unter den Erläuterungen zu Art. 6 Abs. 1 Bst. b).

Mit der Streichung der Einschränkung der GEBM auf die Buchstaben a–d in Artikel 19 Absatz 2 wird nun deren Anwendungsbereich auch auf den gewalttätigen Extremismus und auf sicherheitspolitisch bedeutsame Vorgänge im Ausland und im Cyberraum ausgedehnt. Die strengen Voraussetzungen für den Einsatz von GEBM nach Artikel 27 Absatz 1 bleiben aber unverändert und gelten für alle Beschaffungsmassnahmen, die gegen schwere Bedrohungen gerichtet sind. Aufgrund der Berücksichtigung der Schwere der Bedrohung wird die Verhältnismässigkeit des Einsatzes der Beschaffungsmassnahme im Einzelfall sichergestellt.

Ziffer 2

In der praktischen Anwendung der GEBM zur Aufklärung von terroristischen Umtrieben hat sich gezeigt, dass das Bundesverwaltungsgericht Massnahmen im Bereich des Fernmeldewesens, die auf Grund technischer Umstände ausschliesslich in der Schweiz durchführbar sind, nicht genehmigen kann, wenn die Sicherheit der Schweiz nicht selbst (unmittelbar) konkret im Sinne von Artikel 19 Absatz 2 bedroht ist. Das

gilt auch für Fälle im Zusammenhang mit sowohl national als auch international geächteten Terrororganisationen wie der Al-Qaïda oder dem «Islamischen Staat». Deren Führungskräfte im Ausland nutzen teilweise Schweizer Fernmeldedienstleistungen, die nur mit GEBM in der Schweiz aufgeklärt werden können. Das Bundesverwaltungsgericht musste in der Vergangenheit einen Antrag des NDB ablehnen, weil die Schwere der (unmittelbaren) Bedrohung der Sicherheit der Schweiz nicht genug konkret gegeben war. Es verwies darauf, dass es am Gesetzgeber liege, für solche Fälle eine gesetzliche Grundlage für die Anwendung von GEBM zu schaffen.

Der Bundesrat schlägt deshalb vor, in Anlehnung an Artikel 2 Buchstabe d auch die schwere Bedrohung wichtiger internationaler Sicherheitsinteressen als Kriterium für die Anordnung von GEBM in der Schweiz einzuführen. Die Bedrohung wichtiger internationaler Sicherheitsinteressen kann eine abstrakte dauerhafte Bedrohung für die Schweiz darstellen; tritt das Ereignis ein, kann jedoch grosser Schaden entstehen. Gewisse Abklärungen, namentlich über Kommunikationsvorgänge zwischen Personen, die die internationale Sicherheit schwer bedrohen, sind aus technischen Gründen nur in der Schweiz möglich. Benutzt eine solche Person, zum Beispiel ein hohes Führungsmitglied einer internationalen Terrororganisation, einen über die Schweiz abgewickelten Kommunikationsdienst oder führen ausländische Akteure schwere Cyberangriffe gegen andere Länder über Schweizer Infrastrukturen aus, soll der NDB die Möglichkeit haben, Abklärungen mit GEBM auch im Interesse der internationalen Sicherheit vorzunehmen, und dies nicht nur bei einer unmittelbaren Bedrohung der Schweiz. Ähnliches gilt bei Tätigkeiten von nachrichtendienstlichen Agentinnen und Agenten anderer Länder, die in der Schweiz präsent sind, zu denen jedoch keine Anhaltspunkte vorliegen, dass sie gegen Schweizer oder ausländische militärische Interessen spionieren, bzw. bei denen klar ist, dass sie (zumindest derzeit) lediglich gegen ausländische politische oder wirtschaftliche Interessen agieren. Hier sollte der NDB als Abwehrbehörde deren Tätigkeit umfassend frühzeitig aufklären und verhindern können, um den politischen und wirtschaftlichen Standort Schweiz schützen zu können. Damit würde auch dem Risiko Rechnung getragen, dass solche Personen unerkannt gegen Schweizer Interessen tätig werden, wenn sich die Gelegenheit dazu bietet.

Wie für den Schutz von Schweizer Sicherheitsinteressen sollen auch die internationalen Sicherheitsinteressen auf die Themengebiete von Artikel 6 Absatz 1 Buchstaben a und b beschränkt sein, d. h. die Abwehr von Terrorismus, Spionage, Proliferation, Cyberangriffen und gewalttätigem Extremismus sowie sicherheitspolitisch bedeutsame Vorgänge im Ausland und im Cyberraum. Eine solche Kooperationsfähigkeit der Schweiz kann in einem umgekehrten Fall auch die internationale Kooperationsbereitschaft zugunsten der Sicherheit der Schweiz fördern.

Der Bundesrat spricht sich bei der Anwendung dieser neuen Möglichkeiten zur Früherkennung und Bekämpfung von schweren Bedrohungen durch gewalttätigen Extremismus und von schweren Bedrohungen von internationalen Sicherheitsinteressen für eine ebenso restriktive Praxis wie bisher aus und erwartet keine wesentliche Erhöhung der Anzahl Fälle, in denen solche Massnahmen zur Anwendung kommen. Die gesetzlichen Voraussetzungen für ihre Anwendung bleiben gleich streng und werden vom Bundesverwaltungsgericht unabhängig überprüft. Die erforderliche Freigabe der

Massnahmen auf politischer Ebene ermöglicht eine aktive Steuerung auch nach staatspolitischen Gesichtspunkten. Insgesamt dürfte es sich bei gleichbleibender Bedrohungslage um rund 5 bis 10 zusätzliche Fälle pro Jahr handeln, in welchen künftig GEBM zur Aufklärung von schweren Bedrohungen durch gewalttätigen Extremismus oder Bedrohungen wichtiger internationaler Sicherheitsinteressen eingesetzt würden.

Artikel 28

Absatz 1

In diesem Artikel erfolgt eine Klarstellung, dass darunter auch Fälle gehören, in denen eine Zielperson zwar keinen eigenen Zugriff auf die zu überwachende Infrastruktur (Telefon, Fahrzeug, Postadresse usw.) der Drittperson hat, aber diese benutzt, um Informationen weiterzuleiten, namentlich auch an die Drittpersonen. Als konkretes Beispiel kann ein im Ausland befindlicher Schweizer Dschihadkämpfer genannt werden, von dem bekannt ist, dass er regelmässig mit einer Drittperson, z. B. einem Freund oder einem Familienangehörigen, in der Schweiz kommuniziert. Eine Überwachung seines Fernmeldeanschlusses im Ausland ist technisch nicht möglich, jedoch kann der Anschluss der Drittperson in der Schweiz überwacht werden. Damit können für die Sicherheit der Schweiz wichtige Erkenntnisse zur Abwehr von terroristischen Bedrohungen gewonnen werden. Die Ergänzung «von da aus oder dorthin» soll verdeutlichen, dass die Anordnung von GEBM gegenüber einer Drittperson auch möglich ist, wenn diese lediglich Empfängerin von Informationen der zu überwachenden Person ist. Es gelten im Übrigen auch in solchen Konstellationen die üblichen strengen Voraussetzungen betreffend die Schwere der Bedrohung und die Verhältnismässigkeit der Massnahme.

Artikel 29 Genehmigungsverfahren: Antrag

Im Vergleich mit dem heutigen Absatz 1 werden einzig Buchstabe c ergänzt und Buchstabe c^{bis} neu eingefügt. Ansonsten bleibt der Absatz inhaltlich unverändert. Die weiteren Absätze des Artikels werden inhaltlich in die neuen Artikel 29*a*–29*c* überführt und deswegen hier aufgehoben.

Absatz 1 Buchstabe c

GEBM können in der Praxis bisweilen nicht ohne weitere Begleitmassnahmen umgesetzt werden. Soll beispielsweise ein Ortungsgerät an einem Fahrzeug angebracht werden und liegen die richterliche Genehmigung und die politische Freigabe dafür vor, so kann das Fahrzeug auf öffentlichem oder auf frei zugänglichem privatem Grund, in einer privaten Tiefgarage mit beschränktem Zugang, in einer abschliessbaren Einzelgarage oder auf einem privaten Abstellplatz einer Drittperson usw. abgestellt sein. Für das Anbringen (und das spätere Entfernen) des Ortungsgeräts ist somit das Betreten entsprechender Räumlichkeiten und Örtlichkeiten notwendig, wobei die jeweiligen Eigentumsverhältnisse nicht immer auf Anhieb klar erkennbar sind. In Anlehnung an Artikel 269ter Absatz 2 StPO soll deshalb auch im vorliegenden Gesetz die Möglichkeit geschaffen werden, gleichzeitig mit der Befugnis in der Hauptsache (z. B. Anbringen eines Ortungsgeräts) auch die Befugnis für die Umsetzung der notwendigen Begleitmassnahmen zu erteilen. Artikel 269ter StPO regelt den Einsatz von

besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs sowie von dazu möglicherweise notwendigen Begleitmassnahmen, die aufgrund der Eingriffsintensität von der Grundbewilligung nicht mehr abgedeckt werden. Da der NDB auch andere GEBM anwenden kann, muss die entsprechende Regelung in diesem Gesetz über die in Artikel 269ter StPO geregelten Begleitmassnahmen hinausgehen. Entsprechend sind die notwendigen Begleitmassnahmen von Fall zu Fall zu definieren. Beispielsweise kann der Einsatz eines IMSI-Catchers nicht nur im öffentlichen Raum, sondern auch in Privaträumen notwendig sein.

Die allenfalls mit dem Einsatz einer GEBM verbundenen notwendigen Begleitmassnahmen hängen vom Einzelfall ab und können im Gesetz nicht abschliessend aufgezählt werden. Der NDB muss sie deshalb in den Dokumenten für das Genehmigungs- und das Freigabeverfahren detailliert beschreiben und beantragen. Bei der Genehmigung folgt das Bundesverwaltungsgericht in der Beurteilung der Zulässigkeit den vergleichbaren Anforderungen bezüglich Eignung, Erforderlichkeit und Subsidiarität wie bei der Hauptmassnahme.

Absatz 1 Buchstabe c^{bis}

Als Folge der Anpassung in Artikel 29*a* Absatz 3 (siehe unten) betreffend die über Massnahmen von Strafverfolgungsbehörden bzw. vom Dienst ÜPF zu erteilenden Informationen, werden neu die Angaben über Strafverfahren gegen die von der Beschaffungsmassnahme betroffene Person und allfällige in diesem Zusammenhang angeordnete Zwangsmassnahmen Teil des Antrags.

Artikel 29a Genehmigungsverfahren: Entscheid

Absatz 1

Dieser Absatz entspricht dem heutigen Artikel 29 Absatz 2. Als Folge der Anpassung in Artikel 29 Absatz 1 Buchstabe c wird in diesem Absatz in Anlehnung an Artikel 274 Absatz 4 StPO ausdrücklich festgelegt, dass das Bundesverwaltungsgericht sich in seinem Entscheid über die allfälligen Begleitmassnahmen zu äussern hat.

Absatz 2

Dieser Absatz entspricht weitgehend dem heutigen Artikel 29 Absatz 3 erster Satz. Gemäss heutigem Gesetzestext versagt das Bundesverwaltungsgericht einer beantragten GEBM die Genehmigung, wenn eine *solche* Massnahme bereits aufgrund eines Strafverfahrens gegen die betroffene Person hängig ist. Dabei ist nicht hinreichend klar, ob mit einer *solchen* Massnahme eine identische Massnahme (also ebenfalls z. B. eine Fernmeldeüberwachung) gemeint ist oder lediglich eine andere Zwangsmassnahme (beispielsweise eine strafprozessuale technische Überwachung, während der NDB eine Fernmeldeüberwachung beantragt). Es ist deshalb notwendig zu präzisieren, was als *solche* Massnahme gilt.

Gleich wie bisher beabsichtigt, sollen einerseits verschiedene Massnahmen von Strafverfolgungsbehörden und Nachrichtendienst gleichzeitig möglich sein und sich andererseits Massnahmen gegenseitig ausschliessen, die dasselbe bewirken. Dies wird im Gesetzeswortlaut neu durch den Wortlaut *identisch* verdeutlicht. Läuft also beispielsweise auf dem Festnetz eine Telefonüberwachung auf Anordnung der BA, soll der

Nachrichtendienst parallel dazu in ein der Zielperson zurechenbares Mobiltelefon eindringen und diese Kommunikation aufklären dürfen, weil es sich zwar um ähnliche, aber nicht um identische Massnahmen handelt (die überdies zu unterschiedlichen Zwecken erfolgen). Nicht genehmigt würde hingegen die zeitgleiche Überwachung derselben Festnetznummer durch BA und NDB, da die Massnahmen identisch sind.

Den vom Bundesverwaltungsgericht im Rahmen einer Konsultation geäusserten Bedenken, dass es zu einer Vermischung der strafprozessualen und der nachrichtendienstlichen Überwachung führen könnte, welche unterschiedlichen Zwecken dienen und an andere Bedingungen geknüpft sind (Prävention vs. Repression), wenn eine GEBM nur bei identischen strafprozessualen Zwangsmassnahmen auszuschliessen sei, kann nach Auffassung des Bundesrates im Rahmen des Genehmigungsverfahrens hinreichend Rechnung getragen werden. Der NDB muss in seinen Anträgen auf bestehende strafprozessuale Zwangsmassnahmen hinweisen und begründen, weshalb die beantragten GEBM nicht mit diesen kollidieren. Bei einer Weitergabe von mit GEBM beschafften Informationen an die Strafverfolgungsbehörden muss der NDB sodann auf die Herkunft der Informationen hinweisen, womit die Strafverfolgungsbehörde darauf achten kann, dass strafprozessuale Schutzbestimmungen für die beschuldigte Person nicht ausgehebelt, respektive umgangen werden. Es liegt sowohl im Interesse der Strafverfolgungsbehörden als auch des NDB, dass nicht mehrere Verfahren geführt werden, die dasselbe bezwecken.

Das Bundesverwaltungsgericht gab zudem zu bedenken, dass der heutige Artikel 29 Absatz 3 lediglich die Umstände zum Zeitpunkt der Genehmigung betreffe und insofern keine explizite Regelung für den Fall enthalte, dass eine identische strafprozessuale Zwangsmassnahme erst während einer laufenden GEBM angeordnet würde. Aus den zugrundeliegenden Bestimmungen gehe nicht genügend klar hervor, ob das Nichtvorliegen einer identischen strafprozessualen Massnahme zu den Voraussetzungen für die Anordnung einer GEBM gehöre, bei deren Wegfall die GEBM unverzüglich zu beenden sei. Der Bundesrat teilt diese Bedenken nicht und ist der Auffassung, dass die Beendigung einer GEBM aufgrund der Anordnung einer identischen strafprozessualen Zwangsmassnahme durchaus gestützt auf Artikel 32 Absatz 1 Buchstabe b erfolgen kann.

Absatz 3

Dieser Absatz entspricht inhaltlich weitgehend dem heutigen Artikel 29 Absatz 3 zweiter Satz und wird an die heutige Praxis angeglichen, nach der der NDB sich vor der Antragstellung an das Bundesverwaltungsgericht über allfällige Massnahmen von Strafverfolgungsbehörden bzw. beim Dienst ÜPF direkt informiert und das Ergebnis im Antrag an das Bundesverwaltungsgericht ausführt. Nach Anregung der schweizerischen Staatsanwaltschaftskonferenz und des Kantons Freiburg sollen die zuständigen Staatsanwaltschaften als Strafverfolgungsbehörden anstelle der Zwangsmassnahmengerichte die erforderlichen Auskünfte über Strafverfahren und allfällige Zwangsmassnahmen erteilen. Dies ist sinnvoller, da nicht im Rahmen aller Strafverfahren auch Zwangsmassnahmen durchgeführt werden, der NDB aber im Genehmigungsantrag für die Durchführung einer GEBM nicht nur Angaben über angeordnete Zwangsmassnahmen, sondern ebenso Angaben über laufende Strafverfahren machen muss (Art. 29 Abs. 1 Bst. c^{bis}).

Absatz 4

Dieser Absatz entspricht inhaltlich weitgehend dem heutigen Artikel 29 Absätze 4 und 5.

Zudem wird explizit erwähnt, dass das Bundesverwaltungsgericht die Genehmigung sowohl unter bestimmten Bedingungen als auch mit Auflagen erteilen kann. Dies entspricht der derzeitigen gerichtlichen Praxis. Somit wird eine Differenz zwischen dem französischen und dem deutschen und italienischen Wortlaut beseitigt.

Artikel 29b Dauer der Genehmigung und Verlängerung

Absatz 1

Nach dem geltenden Gesetzestext läuft die Dreimonatsfrist für eine Genehmigung ab dem Zeitpunkt von deren Erteilung, unabhängig davon, wie lange das anschliessende politische Freigabeverfahren dauert, oder ob der NDB die genehmigte und freigegebene Beschaffungsmassnahme tatsächlich umsetzen konnte. Dies kann die effektive Laufzeit einer Massnahme einschränken und den Zeitraum bis zur Eingabe von Verlängerungsanträgen verkürzen. Neu soll der Beginn des maximal dreimonatigen Fristenlaufs einer gerichtlich genehmigten besonderen Informationsbeschaffungsmassnahme nicht automatisch mit dem Tag der gerichtlichen Genehmigung einsetzen, sondern das Gericht soll den Beginn der Frist auch auf einen späteren Zeitpunkt festsetzen können. Zu denken ist nicht nur an den Zeitpunkt der politischen Freigabe, sondern auch an einen aus operativen Gründen in der Zukunft angesetzten Zeitpunkt wie die Einreise einer bestimmten Person oder der Eintritt eines Ereignisses wie der Beginn einer die Sicherheit bedrohenden Veranstaltung. Die GEBM sollen zeitlich präziser gehandhabt werden können, ohne Veränderungen an der gesetzlichen Dauer (3 Monate) oder dem rechtsstaatlichen Verfahren vornehmen zu müssen.

Absatz 2

Bei Verzögerungen im Genehmigungs- und Freigabeverfahren eines an sich rechtzeitig eingereichten Antrags auf Verlängerung von GEBM besteht das Risiko, dass der NDB die Massnahme bis zur rechtskräftigen Freigabe der Verlängerung sistieren muss. Deshalb soll neu geregelt werden, dass die Frist während des Verlängerungsverfahrens gleichsam stillsteht und der NDB die Massnahme also fortsetzen darf. Somit wird verhindert, dass eine Beschaffungsmassnahme aufgrund einer Verzögerung im Verfahren unterbrochen wird. Selbstverständlich muss der NDB die Massnahme sofort einstellen, wenn das Bundesverwaltungsgericht die Verlängerung nicht genehmigt. Ein Freigabeverfahren findet danach nicht mehr statt. Die rechtzeitige Einreichung des Verlängerungsantrags berücksichtigt die fünf Arbeitstage nach Artikel 29*a* Absatz 1 für den Entscheid durch das Bundesverwaltungsgericht und die durchschnittliche Anzahl Tage des Freigabeverfahrens, das an keine Frist gebunden ist.

Absatz 3

Wie im Verfahren bei Dringlichkeit vernichtet der NDB die beschafften Daten umgehend, wenn das Gericht die Genehmigung oder die Vorsteherin oder der Vorsteher des VBS die Freigabe nicht erteilt. Die Gruppe der Gegner der erläuterten Anpassung regt an, dass die Daten aus einer GEBM nicht weitergeleitet werden sollen, bevor die

Genehmigung und die Freigabe erteilt wurden. Sie verkennt, dass der NDB bereits heute die Möglichkeit hat, unter gesetzlichen Bedingungen Daten, die er aus einer im Dringlichkeitsverfahren angeordneten GEBM beschafft hat, weiterzuleiten. Wenn er Daten aus einer solchen GEBM weitergeleitet hat und die Genehmigung oder die Freigabe nicht erteilt wird, informiert er die Stellen, die solche Daten erhalten haben.

Artikel 29c Tätigkeitsbericht über genehmigungspflichtige Beschaffungsmassnahmen

Dieser Artikel entspricht einerseits dem heutigen Artikel 29 Absatz 8. Er wurde andererseits auf Wunsch der AB-ND so ergänzt, dass diese Behörde auch den Bericht des Bundesverwaltungsgerichts inskünftig erhalten soll. Diese Zustellung war in der ursprünglichen Fassung der Verordnung vom 16. August 2017[37] über die Aufsicht über die nachrichtendienstlichen Tätigkeiten (VAND) vorgesehen. Sie wurde aber auf Anregung der GPDel per 1. Dezember 2021 aufgehoben. Zur effizienten Ausübung ihrer Aufsichtstätigkeit, insbesondere was die operationellen Tätigkeiten des NDB anbelangt, scheint es heute angebracht, dass die AB-ND eine formell-gesetzliche Grundlage für den Zugriff auf dieses wichtige Dokument erhält.

Artikel 30

Absätze 3 und 4

Die reine Verlängerung einer laufenden GEBM hat primär eine zeitliche Komponente. Die Beschaffungsmassnahme selbst bleibt aber genau gleich, weshalb vom politischen Grundsatzentscheid über die Verlängerung einer GEBM abgesehen werden kann. Daher soll neu die Vorsteherin oder der Vorsteher des VBS in eigener Verantwortung über reine Verlängerungen entscheiden können. Die Vorsteherinnen und Vorsteher von EDA und EJPD werden dadurch von einem Teil der aufgrund der heutigen Regelung anfallenden Konsultationen, die eine beträchtliche Belastung darstellen, entlastet. Die Möglichkeit, die Vorsteherin oder den Vorsteher des EDA und die Vorsteherin oder den Vorsteher des EJPD vor dem Entscheid zu konsultieren, bleibt in Fällen von besonderer Bedeutung im Ermessen der Vorsteherin oder des Vorstehers des VBS bzw. kann gemeinsam abgesprochen werden.

Bei geringfügigen Erweiterungen von bereits genehmigten und freigegebenen Massnahmen stellen sich in der Regel ebenfalls keine grundsätzlichen Fragen mehr. Das ist beispielsweise der Fall, wenn eine Zielperson ein zusätzliches Mobiltelefon mit einer neuen Telefonnummer erwirbt, die in eine bereits bestehende Überwachung ihrer Anschlüsse miteinbezogen werden soll. Bei geringfügigen Erweiterungen bleibt die Zielperson die gleiche wie im Grundantrag. Auch in solchen Fällen rechtfertigt es sich, dass die Vorsteherin oder der Vorsteher des VBS nach der Genehmigung des Bundesverwaltungsgerichts direkt über die Freigabe der Erweiterung entscheiden kann. Auch hier bleibt es der Vorsteherin oder dem Vorsteher des VBS unbenommen, die Vorsteherin oder den Vorsteher des EDA und des EJPD trotzdem vor dem Ent-

37 SR **121.3**

scheid zu konsultieren, wenn sie bzw. er es wegen der mit der Massnahme verbundenen politischen Risiken für notwendig erachtet. Auch können die Vorsteherin oder der Vorsteher des EDA und des EJPD bei der Stellungnahme zur ursprünglichen Anordnung bei besonderen Interessen verlangen, dass sie bei Verlängerungen oder Erweiterungen wieder konsultiert werden wollen. Jederzeit gilt, dass die Vorsteherin oder der Vorsteher des VBS die Vorsteherin oder den Vorsteher des EDA sowie die Vorsteherin oder den Vorsteher des EJPD über den getroffenen Entscheid informiert. Gleiches gilt auch für die geringfügige Erweiterung eines Auftrags zur Kabelaufklärung (siehe dazu die Ausführungen zu Art. 41 Abs. 4).

Artikel 33

Absätze 1, 2bis, 3 und 4

Um Unklarheiten bei der Berechnung der Monatsfrist zu vermeiden, soll die Frist für die Mitteilung von GEBM neu auf einheitlich dreissig Tage festgelegt werden.

Bei der Anwendung der Mitteilungspflicht und ihren Ausnahmen hat die Praxis gezeigt, dass die heutige Regelung teilweise zu Aufwand führt, der in keinem Verhältnis zum Schutz der Rechte der betroffenen Personen steht. Nach heutigem Recht muss der Aufschub einer Mitteilung alle drei Monate beim Gericht neu beantragt und anschliessend vom Vorsteher oder von der Vorsteherin VBS nach Konsultation der Vorsteherin oder des Vorstehers des EDA und des EJPD freigegeben werden, da das gleiche Verfahren wie für die Anordnung von GEBM gilt. Für dieses gilt eine Höchstdauer der Genehmigung von drei Monaten. Bei bisherigen Fällen des Aufschubs der Mitteilung ging es vorwiegend um Personen, gegen die ein Strafverfahren hängig war, das einen Zusammenhang mit der vorangegangenen nachrichtendienstlichen Überwachung hatte. Wenn die betroffene Person von den Strafverfolgungsbehörden aus ermittlungstaktischen Gründen noch nicht über das Verfahren informiert wurde, kann eine Mitteilung der Überwachung durch den NDB das Strafverfahren gefährden. Es erfolgt deshalb immer ein Aufschub bzw. dessen Verlängerung. Die Mitteilung erfolgt erst, wenn die Strafverfolgungsbehörde die Person informiert oder das Strafverfahren eingestellt hat.

Neu soll deshalb ein Aufschub nicht bloss für drei Monate, sondern für bis zu sechs Monate erfolgen können oder an ein bestimmtes Ereignis gebunden werden (z. B. den Fortgang eines Strafverfahrens). Der NDB hat wie bisher in seinem Antrag die Gründe für einen Aufschub und neu gegebenenfalls das Ereignis genau zu nennen, bis zu dessen Eintritt der Aufschub gelten soll. Das Bundesverwaltungsgericht entscheidet sodann begründet über die Genehmigung des Aufschubs. Da der blosse Aufschub der Mitteilung keine definitive Massnahme darstellt, soll er neu einzig dem Genehmigungsverfahren unterstellt werden. Es ist nicht zu erwarten, dass ein rechtlich gebotener Aufschub aus politischen Gründen nicht bestätigt wird. Ein Aufschub der Mitteilung aufgrund der Beziehungen der Schweiz mit dem Ausland enthält hingegen eine politische Komponente. Deswegen soll dieser Aufschub das Freigabeverfahren durchlaufen.

Der definitive Verzicht auf die Mitteilung soll hingegen wie bisher dem politischen Freigabeverfahren unterstellt bleiben. Wird der Aufschub der Mitteilung durch das

Bundesverwaltungsgericht genehmigt, kann eine Information der im Freigabeverfahren involvierten Departemente sinnvoll sein. Falls nötig wird dies in Zusammenhang mit der Anpassung des Verordnungsrechts im Anschluss an die Gesetzesrevision geregelt.

Weiterhin gilt die Mitteilungspflicht nur für tatsächlich durchgeführte Massnahmen. Bei Massnahmen, die zwar genehmigt und freigegeben wurden, die aber z. B. aus technischen Gründen nicht umgesetzt werden konnten, liegt kein Eingriff in die Grundrechte vor. Sie unterstehen deshalb nicht der Mitteilungspflicht.

Artikel 37

Absätze 3–6

Artikel 37 enthält heute keine Dringlichkeitsregelung, wie sie bei den GEBM in Artikel 31 besteht. Das Eindringen in Computersysteme und -netzwerke im Ausland zwecks Störung, Verhinderung oder Verlangsamung von deren Funktion als Massnahme gegen Angriffe auf kritische Infrastrukturen ist eine in der Regel heikle und in der Wirkung sofort erkennbare Massnahme und soll weiterhin nur auf Entscheid des Bundesrates erfolgen.

Das Eindringen zur Informationsbeschaffung erfolgt jedoch unbemerkt und muss bei Dringlichkeit sofort erfolgen können, um rechtzeitig an wichtige Informationen zu kommen. Es rechtfertigt sich deshalb, eine Dringlichkeitsregelung analog jener für die GEBM zu ergänzen. Diese hat sich bewährt und sieht vor, dass die Direktorin oder der Direktor des NDB die Massnahme direkt anordnen und vollziehen lassen kann und sie nachträglich zur Genehmigung und Freigabe nach dem üblichen Verfahren unterbreitet. Nach Anordnung der Massnahme ist unverzüglich die Vorsteherin oder der Vorsteher des VBS zu informieren.

Sollte die Vorsteherin oder der Vorsteher des VBS unmittelbar oder nach Konsultation von EDA und EJPD die Weiterführung der Massnahme ablehnen, müssten sie zusätzlich über die Verwendung der allenfalls bereits beschafften Daten entscheiden. Es ist möglich, dass zwar eine Massnahme aus Gründen der politischen Risikoabwägung nicht weitergeführt werden soll, dass der NDB aber bereits damit beschaffte und für die Beurteilung der Sicherheitslage relevante Informationen verwenden darf.

Artikel 39

Absatz 1

Als Konsequenz der Ausdehnung des Auftrags des NDB auf den gesamten Cyberraum in Artikel 6 Absatz 1 Buchstabe b wird dieser Absatz ebenfalls angepasst. Die Kabelaufklärung bleibt aber eine Massnahme, die sich gegen das Ausland richtet. Es werden keine Personen in der Schweiz überwacht (siehe auch Abs. 3). Zudem bleiben die Bedingungen für eine Kabelaufklärung gleich wie heute. Reine «Inland-Inland»-Kommunikationen werden nicht erfasst.

Absatz 3

Die Anpassung in Absatz 3 soll besser zum Ausdruck bringen, dass bei der Kabelaufklärung alle Personen in der Schweiz vor gezielter Aufklärung mit diesem Mittel geschützt sind (vgl. Art. 42 Abs. 2, der ebenfalls von Personen im Inland spricht). Damit kann der NDB mit der Kabelaufklärung keine ausländischen Personen im Inland aufklären, was bereits der heutigen Anwendung entspricht. Hingegen kann es sinnvoll und notwendig sein, Schweizer Personen im Ausland mit Kabelaufklärung zu überwachen, wenn sichergestellt ist, dass sich diese nicht in der Schweiz aufhalten. Dies entspricht der heutigen Praxis bei der Funkaufklärung, z. B. bei Schweizer Personen, die terroristisch motiviert in Dschihadgebiete reisen oder bei ausländischen Tochterfirmen von (zumeist ebenfalls ausländisch beherrschten) Firmen, die in der Schweiz im Handelsregister eingetragen sind und Verbindungen zu mutmasslichen Proliferationsaktivitäten haben. Es ist einerseits gerechtfertigt, solchen Personen im Ausland keinen höheren Schutz zukommen zu lassen als ausländischen Personen im Ausland; andererseits ist es in solchen Fällen nicht immer möglich in der Schweiz GEBM durchzuführen, weil es an den entsprechenden technischen oder physischen Zugängen fehlt.

Suchbegriffe sind weiterhin beliebige Zeichen-, Zahlen- und Buchstabenkombinationen oder eine Mischung daraus, durch die Daten nach auftragsrelevanten Verbindungsdaten und Kommunikationsinhalten gefiltert werden, um ein Resultat zu generieren (z. B. Namen von juristischen oder natürlichen Personen, Telefonnummern, E-Mail-Adressen, IP-Adressen, Merkmale schädlicher Cyberaktivitäten resp. Indicators of Compromise, Koordinaten usw.). Diese Suchbegriffe müssen sich inhaltlich den vom Bundesverwaltungsgericht genehmigten Suchbegriffskategorien zuordnen lassen. Dabei können sich Suchbegriffe auch aus technischen Kommunikationselementen (Randdaten der Telekommunikation) zusammensetzen. Ein Beispiel für einen solchen zusammengesetzten Suchbegriff könnte eine Mobiltelefonnummer (MSISDN) einer natürlichen Person aus der Suchbegriffskategorie «natürliche Personen» sein sowie die Einschränkung eines internationalen Länderpräfixes oder einer internationalen Länderkennung eines Mobilfunknetzes (MCC; Mobile Country Code). Weitere denkbare Einschränkungen wären ausserdem bestimmte Zeitfenster oder technische Merkmale wie die Identifikatoren von Mobilfunkantennen. Diese Kombination mehrerer Suchbegriffskategorien kann den Präzisierungsgrad der Suche erhöhen.

Im Rahmen der Vernehmlassung wünscht sich das Bundesverwaltungsgericht weitere Präzisierungen in Zusammenhang mit der Zulässigkeit von Suchbegriffen und von deren Kombinationen. Aus Sicht des Bundesrates ist dieses Anliegen im Rahmen der anschliessenden Verordnungsrevision zu berücksichtigen.

Artikel 41

Absatz 1 Buchstabe b

Der heutige Begriff «Notwendigkeit» soll gemäss der vom Bundesverwaltungsgericht entwickelten Praxis zu den Genehmigungsanträgen durch die für die Beurteilung der Verhältnismässigkeit massgeblichen Elemente Geeignetheit, Erforderlichkeit und Zumutbarkeit ersetzt werden. Das Element der Notwendigkeit ist dabei durch den Begriff der Erforderlichkeit immer noch abgedeckt.

Absatz 1bis

Anträge auf Kabelaufklärung sind meist komplex und zeitlich nicht dringend, weshalb sich eine Verlängerung der Entscheidfrist auf zehn Tage rechtfertigt. Dies wird vom Bundesverwaltungsgericht explizit begrüsst.

Absatz 2

Hier wurde nur der Ausdruck «weitere Verfahren» durch «übrige Verfahren» ersetzt. Damit wird insbesondere signalisiert, dass der Entscheid ebenfalls durch eine Einzelrichterin oder einen Einzelrichter gefällt wird.

Absatz 3

Die Kabelaufklärung bedarf – gleich wie eine GEBM – der richterlichen Genehmigung durch das Bundesverwaltungsgericht und daran anschliessend der politischen Freigabe durch die Vorsteherin oder den Vorsteher des VBS nach Konsultation die Vorsteherin oder des Vorstehers des EDA und des EJPD. Nach heutigem Recht erfolgt die erstmalige Genehmigung für höchstens sechs Monate und kann nach demselben Verfahren um jeweils höchstens drei Monate verlängert werden.

Die Kabelaufklärung ist aufwendig und hochkomplex. Zum heutigen Zeitpunkt ist sie nur für eine länger andauernde Informationsbeschaffung über sicherheitspolitisch bedeutsame Vorgänge im Ausland geeignet. Da auf Dauer ausgerichtet, hat sich die vom heutigen Gesetz vorgesehene Höchstdauer für eine Verlängerung als deutlich zu kurz erwiesen: Zur Sicherstellung eines unterbruchlosen Betriebes muss der NDB heute bereits für jeden Kabelaufklärungsauftrag schon nach zwei Monaten einen Verlängerungsantrag für das richterliche Genehmigungs- und das politische Freigabeverfahren einreichen. Auch gilt es zu beachten, dass Systemanpassungen oder andere Massnahmen (z. B. Leitungsausbau) sich oft nicht sofort in entsprechenden Resultaten niederschlagen, sondern dass es dazu eines längeren Zeitraums bedarf.

Mit der Erhöhung der Höchstdauer für eine Verlängerung auf sechs Monate wird nicht nur der vorwiegend strategischen Ausrichtung der Kabelaufklärung Rechnung getragen, sondern auch der Tatsache, dass es sich bei der Kabelaufklärung um einen eigentlichen Sensor des NDB und nicht um ein im Rahmen einer bestimmten zeitlich beschränkten Operation eingesetztes Beschaffungsmittel handelt. Im Bereich der Auslandaufklärung wechseln die Bedrohungslagen und damit die Nachrichtenbedürfnisse in der Regel nicht im Rhythmus von drei Monaten und die Kapazitäten des NDB und des Bundesverwaltungsgerichts können sinnvoller eingesetzt werden als zur Bearbeitung von rasch aufeinanderfolgenden Genehmigungsverfahren. Unterschiedliche Fristen für die Grundgenehmigung und die jeweilige Verlängerung rechtfertigen sich in diesem Bereich nicht.

Um weiterhin flexibel und zeitnah auf Lageänderungen und Aufklärungsbedürfnisse reagieren zu können, besteht auch bei der längeren Laufzeit von Genehmigungen die Möglichkeit einer Auftragsanpassung. Dies ist beispielsweise der Fall, wenn bei einem Kabelaufklärungsauftrag neue Fernmeldedienstanbieterinnen, thematische Anpassungen oder neue Kategorien von Suchbegriffen einbezogen werden müssen. Solche Anpassungen muss der NDB weiterhin nach dem normalen Verfahren beantragen.

Absatz 4

Wie bereits in den Erläuterungen zu Artikel 30 Absätze 3 und 4 ausgeführt, rechtfertigt es sich in Fällen von geringfügigen Erweiterungen von bereits genehmigten und freigegebenen Massnahmen, dass die Vorsteherin oder der Vorsteher des VBS nach der Genehmigung des Bundesverwaltungsgerichts ohne zwingende Konsultation der Vorsteherin oder des Vorstehers des EDA und des EJPD direkt über die Freigabe der Erweiterung entscheiden kann. Das Gleiche gilt auch für die Aufnahme weiterer Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsdienstleistungen in einen bestehenden Auftrag zur Kabelaufklärung. Bei einer solchen handelt es sich ebenfalls nur um eine geringfügige Erweiterung, da die zusätzliche Aufnahme zwar Teil der nachrichtendienstlichen Risikobeurteilung sowie der juristischen Verhältnismässigkeitsprüfung ist, nicht aber Teil der Risikobeurteilung auf politischer Stufe, die insbesondere aussenpolitische Erwägungen berücksichtigt.

Artikel 42

Absatz 3bis

Beim Erlass des NDG ging man davon aus, dass die Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsdienstleistungen – wie in Artikel 43 NDG festgelegt – in der Lage sind, hinreichende Auskünfte insbesondere über die von ihnen geführten internationalen Datenströme zu geben. In den ersten Anwendungsfällen der Kabelaufklärung hat sich aber gezeigt, dass das nur sehr bedingt zutrifft. Die Schweizer Betreiberinnen kennen oft nur die Herkunfts- und Zielpunkte der Datenströme in den benachbarten Ländern und nicht deren weiterreichende Herkunft oder Endpunkte. Wie diese Datenströme verlaufen und welche Art von Kommunikationsdaten transportiert werden, ist einem stetigen, raschen Wandel unterworfen.

Die internationalen Datenströme werden über hochdynamische Netzwerke geleitet, deren Routing sich rasch ändern und nicht langfristig vorausgesagt werden kann. Die Fernmeldedienstanbieterinnen optimieren ihre Datenflüsse permanent, sei es zugunsten einer besseren Übertragungsqualität, sei es aus wirtschaftlichen Überlegungen. Der durchführende Dienst soll deshalb neu die im Rahmen von bestehenden Aufträgen erfassten Signale und Daten technisch analysieren dürfen, um ein möglichst aktuelles und realitätsgetreues Bild der bearbeiteten Datenströme, der damit transportierten Signale und der Herkunft und Destination der Kommunikationsdaten zu erhalten. Ebenfalls gilt es, die technische Beschaffenheit der erfassten Signale zu ermitteln, weil dies einen direkten Einfluss auf die vom durchführenden Dienst zu deren Erfassung und Bearbeitung einzusetzenden technischen Mittel hat.

Diese Art von Auswertung ist technischer Natur und nicht auf den Informationsgehalt der erfassten Daten bezogen. Solche technischen Informationen speichert der durchführende Dienst CEA als Grundlagen für weitere Aufträge bei sich. Es geht darum, zu erkennen, wo welche Arten von Datenströmen transportiert werden und welche davon nachrichtendienstlich relevante Informationen enthalten können. Die dabei gewonnenen Erkenntnisse kann der durchführende Dienst mit dem NDB teilen, damit dieser die Formulierung der Kabelaufklärungsaufträge zielgerichteter vornehmen

kann (d. h. die Bezeichnung der zu überwachenden Datenströme in den Kabelaufklärungsaufträgen).

4. Kapitel: Datenbearbeitung und Qualitätssicherung

Allgemeine Bemerkungen

In ihrem Jahresbericht 2019 regte die GPDel an, im Rahmen der anstehenden Revision des NDG ein alternatives Datenbearbeitungskonzept zu prüfen, in welchem der Zweck der Informationssysteme (Art. 47–57), die Regeln für den Datentransfer zwischen den Systemen (Art. 44 Abs. 3 und 4) und die Anwendbarkeit der Schranken von Artikel 5 für einzelne Systeme in Verbindung mit spezifischen Löschfristen neu austariert würden. Gefordert wurde eine bedeutend weniger komplexe und besser nachvollziehbare Regelung. Der grundlegende Zweck der Schranken von Artikel 5 stehe dabei jedoch nicht zur Disposition.

Dieser Revisionsentwurf trägt diesen Empfehlungen Rechnung. Die neue Datenbearbeitungskonzeption zeichnet sich durch eine Fokussierung auf die Daten und deren Bearbeitung aus. Die Eingangsprüfung, die Qualitätssicherung der Daten und die Datenbekanntgabe werden einheitlich geregelt. Zentral ist dabei der Verzicht auf eine Differenzierung verschiedener Informations- und Speichersysteme (das neue DSG verzichtet ebenfalls auf den Begriff «Informationssystem»). Damit ist die Regelung technologieneutral, umfasst lückenlos alle Daten des NDB und verbessert die Qualitätssicherungsmöglichkeiten erheblich.

Die Neuregelung bedeutet keine grundsätzliche Abkehr von den Grundsätzen der aktuellen Regelung. Dies gilt insbesondere auch bezüglich der selektiven Zugriffe auf Daten. So werden die geltenden Datenkategorien beibehalten. Aus Gründen der Transparenz werden neue Unterkategorien ausgewiesen. Bei diesen handelt es sich um Kennzeichnungen bzw. Meta-Daten, nicht um Kategorien im Sinne des DSG wie z. B. besonders schützenswerte Personendaten im Sinne von Artikel 5 Buchstabe c DSG. Auch beibehalten werden die Zugriffsberechtigungen anderer Behörden mit wenigen Ausnahmen, die in den Erläuterungen zum 6. Abschnitt ausgewiesen werden.

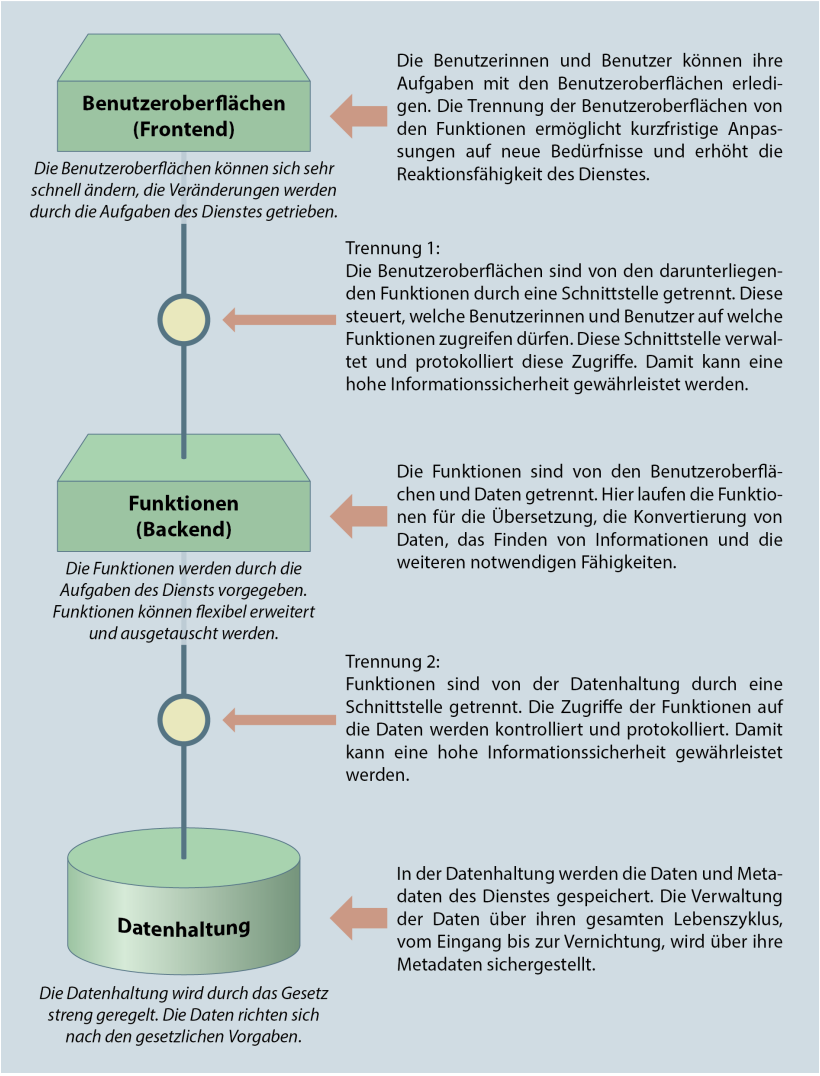
Der Verzicht auf die Nennung von Informationssystemen entspricht auch zeitgemässen IT-architektonischen Ansätzen. Das Arbeiten mit monolithischen Informationssystemen, mit einer physischen Einheit von Daten und Software, ist heute veraltet. Daten werden heute in technisch geeigneten Speicherlösungen sicher und redundant gespeichert. Diese Speicherung auf einem Datenhaltungslayer, gekoppelt mit der nur logisch erfolgenden Verbindung zu den zugreifenden Softwarelösungen, ermöglicht den Verzicht auf Kopien und eine alle Daten umfassende, einheitliche Datenbewirtschaftung (periodische Überprüfung, Korrektur, Löschung, Archivierung) über den ganzen Lebenszyklus der Daten.

Auch ohne Rückgriff auf einzelne Informationssysteme können die Zugriffe wie bisher differenziert gesteuert werden. Da die Zugriffsthematik aber neu auf übergeordneten architektonischen Ebenen (Daten-Service-Layer und App-Service-Layer) angesiedelt werden, können die Zugriffsrechte nicht nur wie heute grob auf Ebene

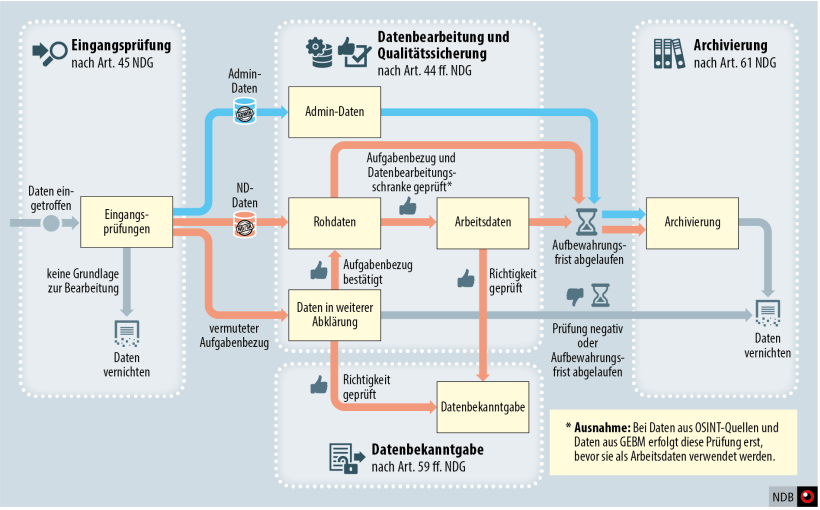
Informationssysteme definiert werden, sondern darüber hinaus feiner bis auf Stufe der Datenbearbeitung und der einzelnen Information. Ausgehend von einem Zugriffs- und Rollenkonzept können sowohl die funktionalen Berechtigungen (welche Tools stehen welcher Rolle zur Verfügung) als auch die fachlichen Berechtigungen (welche Daten stehen welchen Rollen zur Verfügung und dürfen durch sie bearbeitet werden) fein gesteuert werden. Somit können auch in Zukunft rechtliche Auflagen bezüglich der Zugriffe problemlos umgesetzt werden. Neu folgt die Regelung im Gesetz den vier Etappen im Lebenszyklus der Daten: Der Eingang der Daten, deren Verwendung, die Bekanntgabe an Stellen ausserhalb des NDB und die Löschung und Archivierung.

Die Bearbeitung von Personendaten richtet sich nach dem DSG, sofern die Bestimmungen des vorliegenden Revisionsentwurfs keine andere Regelung vorsehen.

Übersicht IT-Architektur



Übersicht Datenbearbeitung NDG



Beim Dateneingang wird geprüft, ob es sich um nachrichtendienstliche oder administrative Daten handelt (Eingangsprüfung). Administrative Daten sind insbesondere alle Daten, die der NDB gestützt auf das RVOG und die KND gestützt auf die entsprechende kantonale Gesetzgebung zu administrativen Zwecken bearbeiten, die also nicht der Aufgabenerfüllung nach Artikel 6 dienen. Dazu gehören auch Daten zu Mitarbeiterinnen und Mitarbeitern des NDB und der KND, zu Personen, die mit dem NDB z. B. für Anfragen oder Auskunftsgesuche in Kontakt treten, zu externen Dienstleistungserbringerinnen und -erbringern, zu Projekten, zum Unterhalt und zur Weiterentwicklung von Informatiklösungen (z. B. Quellcodes oder Grundlagendaten von Applikationen), zu politischen Geschäften, zu Landkarten, zur Zuordnung von Adressen zu Geokoordinaten in einem Geoinformationssystem, zum Schriftenwechsel mit Aufsichtsbehörden des NDB und dem Bundesverwaltungsgericht usw. Administrative Daten werden als solche gekennzeichnet und nach Massgabe der jeweiligen Rechtsgrundlagen weiterbearbeitet. Nachrichtendienstliche Daten betreffen alle Aufgaben, die in Artikel 6 aufgelistet sind. Es sind sämtliche Daten, die der NDB und die KND zur Erfüllung dieser Aufgaben bearbeiten, sowie die Daten, die zur Gewinnung dieser Daten erforderlich sind. Nachrichtendienstliche Daten werden sequenziell mit den folgenden Fragen geprüft: Ist der Aufgabenbezug nach Artikel 6 gegeben? Handelt es sich um Daten aus öffentlich zugänglichen Quellen oder um GEBM? Wenn nein, ist die Datenbearbeitungsschranke von Artikel 5 tangiert? Die Prüfung des Aufgabenbezugs erfolgt grundsätzlich vor der Prüfung der Datenbearbeitungsschranke. Daten aus öffentlich zugänglichen Quellen wie gedruckte oder elektronische Medien werden beim Dateneingang nur bezüglich des Aufgabenbezugs geprüft, da der NDB den Inhalt solcher Meldungen nicht steuern kann und solche Daten in hoher Zahl anfallen. Die Prüfung erfolgt aber, wenn der NDB solche Daten für das Erstellen von

nachrichtendienstlichen Produkten verwenden will (vgl. auch das analoge Vorgehen bei Daten aus GEBM).

Bei der Datenverwendung handelt es sich insbesondere um das Auswerten, Verdichten und Vernetzen von Daten sowie die Erstellung von Produkten. Administrative Daten haben keine gesetzlichen Unterkategorien und werden während ihrer Verwendung nicht weiter geprüft. Ihre weitere Bearbeitung richtet sich vor allem nach dem RVOG.

Nachrichtendienstliche Daten werden nach dem Eingang basierend auf den Ergebnissen der Eingangsprüfung als Rohdaten kategorisiert, wenn der Aufgabenbezug gegeben und (ausgenommen bei Daten aus öffentlich zugänglichen Quellen und aus GEBM) die Prüfung der Datenbearbeitungsschranke erfolgt ist. Rohdaten haben eine tendenziell mittlere Aufbewahrungsdauer und werden regelmässig von der Qualitätssicherungsstelle des NDB mittels Stichproben geprüft. Sie dürfen nicht ohne weitere Prüfung Dritten bekannt gegeben und nicht in Produkten des NDB verwendet werden. Daneben findet eine Kategorisierung in Arbeitsdaten statt. Es handelt sich hierbei um nachrichtendienstliche Rohdaten, die für eine vertiefte Weiterbearbeitung durch den NDB vorgesehen sind und als solche gekennzeichnet wurden, sowie die Produkte aus solchen Datenbearbeitungen (z. B. Analyseberichte, Lageberichte, Alarmierungen). Arbeitsdaten haben eine tendenziell längere Aufbewahrungsdauer. Die Prüfung, dass diese Daten für eine vertiefte Weiterbearbeitung vorgesehen sind, gilt als erste periodische Überprüfung. Die Arbeitsdaten werden daraufhin regelmässig von den Fachspezialisten periodisch geprüft und bewirtschaftet und von der Qualitätssicherungsstelle mittels Stichproben geprüft. Weiter werden sie bei ihrer Bekanntgabe geprüft, was ebenfalls als periodische Überprüfung gilt.

Bei der Bekanntgabe an Dritte unterliegen die Arbeitsdaten einer Bekanntgabeprüfung nach drei Kriterien: Ist die Bekanntgabe notwendig, ist sie zweckmässig und sind die rechtlichen Voraussetzungen für die Bekanntgabe an Dritte erfüllt? Anlässlich der Bekanntgabeprüfung erfolgt jeweils auch eine kritische Überprüfung, ob der NDB die betroffenen Arbeitsdaten für seine Aufgabenerfüllung weiterhin benötigt. Dabei werden nicht mehr benötigte Daten gelöscht (und nicht bekannt gegeben) und die weiterhin benötigten bestätigt (periodische Überprüfung).

Sowohl administrative als auch nachrichtendienstliche Daten bietet der NDB dem Schweizerischen Bundesarchiv (BAR) an, sobald er sie nicht mehr ständig benötigt. Das BAR entscheidet über die Notwendigkeit der Archivierung. Die vom BAR als archivwürdig bezeichneten Daten gibt der NDB dem BAR ab und vernichtet sie in seinen Beständen. Die entsprechende Nomenklatur (löschen, abgeben, vernichten) wird in diesem Gesetz konsequent angewendet.

Kapitel/Gliederungstitel

Das 4. Kapitel wurde der besseren Übersicht halber neu strukturiert (1. Datenkategorien, 2. Eingangsprüfung, 3. Arbeitsdaten, 4. Datenbearbeitung durch kantonale Vollzugsbehörden, 5. Datenbearbeitung zum Nachrichtenverbund, 6. Zugriffsberechtigungen und 7. Qualitätssicherung). Die besonderen Bestimmungen über den Datenschutz und die Archivierung wurden in einem neuen 4*a.* Kapitel festgehalten. Aus diesem Grund wurde auch der Gliederungstitel des 4. Kapitels angepasst. Die

Reihenfolge folgt somit, wie bereits erwähnt, weitgehend den Prozessschritten vom Eingang der Daten beim NDB bis zu deren Archivierung bzw. Vernichtung. In Anlehnung an das DSG wird neu einheitlich von Daten und Personendaten gesprochen.

1. Abschnitt: Datenkategorien

Artikel 44

Absatz 1

In dieser Bestimmung werden die beiden Hauptkategorien definiert, denen die eingehenden und bereits abgespeicherten Daten zugeordnet werden: die nachrichtendienstlichen Daten, die der NDB und die KND zum Zweck der Erfüllung ihrer in Artikel 6 aufgeführten Aufgaben bearbeiten, und die administrativen Daten, die sie zum Zweck der Erfüllung ihrer administrativen Aufgaben bearbeiten (vgl. zum Begriff der administrativen Aufgaben auch die beispielhafte Aufzählung in den allgemeinen Ausführungen oben).

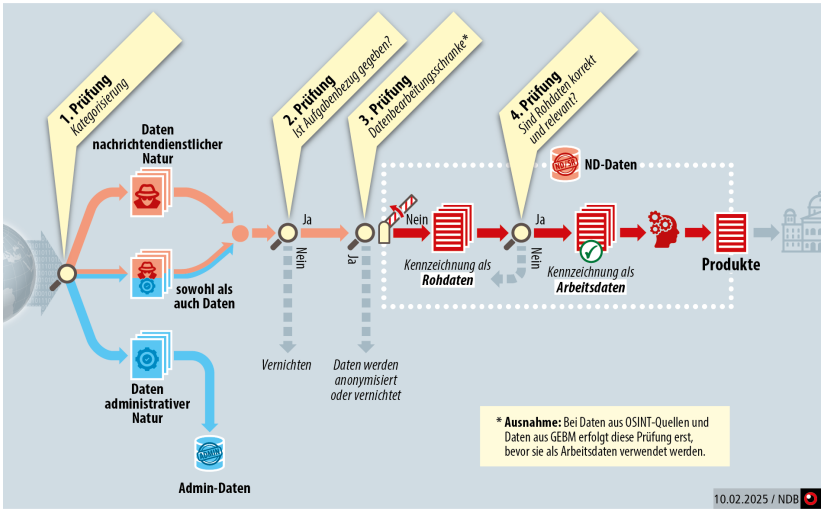
Absatz 2

Die nachrichtendienstlichen Daten werden weiter unterteilt in Rohdaten und Arbeitsdaten. Die nachrichtendienstlichen Daten werden nach der Eingangsprüfung beim NDB und den KND vorerst nur gespeichert. Rohdaten dürfen ohne die Prüfung der Richtigkeit und Relevanz nicht weiterverwendet werden. Arbeitsdaten sind Rohdaten, die auf ihre Richtigkeit hin geprüft wurden und gestützt auf ihre aktuelle Relevanz tatsächlich weiterbearbeitet werden, sowie die aus der Weiterbearbeitung resultierenden Produkte (z. B. Analyseberichte, Meldungsausgänge, Berichte, Anträge an Behörden, Stellungnahmen, Aufträge an KND, Amtsberichte, Referate, Lageeinschätzungen).

2. Abschnitt: Eingangsprüfung

Artikel 45 Prüfung des Aufgabenbezugs und Zuordnung der Datenkategorie

Übersicht Eingangsprüfung



Absatz 1

Wie bereits erwähnt, prüfen der NDB und die KND die bei ihnen eingehenden Daten in einem ersten Schritt daraufhin, ob sie nachrichtendienstlicher oder administrativer Natur sind, und kennzeichnen sie entsprechend. Diese Prüfung erfolgt bei der Abspeicherung der Daten (normalerweise innerhalb eines Arbeitstages; vgl. aber die Ausnahmen nach Art. 45 Abs. 4 und 46 Abs. 2). Der Bundesrat wird die Fristen im Ausführungsrecht regeln. Bei den Datenkategorien «nachrichtendienstlich» und «administrativ» handelt es sich nicht um Datenkategorien im Sinne des DSG.

Absatz 2

Sind die Daten sowohl nachrichtendienstlicher als auch administrativer Natur, werden sie als nachrichtendienstlich gekennzeichnet. Damit ist sichergestellt, dass im Zweifelsfall die strikteren Datenbearbeitungsvorgaben für nachrichtendienstliche Daten zur Anwendung kommen.

Absatz 3

Daten, die weder einen Bezug zum Aufgabengebiet des NDB aufweisen noch von ihm zu administrativen Zwecken verwendet werden können, sind zu vernichten oder unwiderruflich zu anonymisieren (bspw. wenn einzelne Inhalte einer Meldung keinen Aufgabenbezug aufweisen, wohl aber der Rest, sind die Inhalte ohne Aufgabenbezug

zu anonymisieren). Handelt es sich um fälschlicherweise an den NDB adressierte Informationen, kann der NDB die Absenderin oder den Absender darauf aufmerksam machen, bevor er die Daten bei sich vernichtet oder anonymisiert oder, im Fall physischer Einsendungen, an die Adressatin oder den Adressaten zurücksendet. Handelt es sich um Informationen, die der NDB von einem KND erhalten hat, informiert er diesen über die Anonymisierung oder Vernichtung, damit der KND dies auch in seinen Datenbeständen tun kann.

Absatz 4

Es kann vorkommen, dass zum Zeitpunkt des Eingangs von Daten noch unklar ist, ob ein Aufgabenbezug vorliegt. So ist es beispielsweise möglich, dass ein Partnerdienst dem NDB eine Erkenntnisanfrage zu einer Person zukommen lässt, die in dessen Land rechtsradikales und rassistisches Gedankengut verbreitet, was bereits eine Zuständigkeit der ausländischen Behörde begründet. Weil sich diese Person längere Zeit in der Schweiz aufgehalten hat, möchte der Partnerdienst nun wissen, ob der NDB über zusätzliche Erkenntnisse verfügt. Der NDB erteilt in der Folge dem KND, in dessen Kanton sich die betreffende Person aufgehalten hat, einen Abklärungsauftrag. Erst das Ergebnis dieses Abklärungsauftrages wird aufzeigen, ob es sich um eine gewalttätig-extremistische Person handelt, und damit der vermutete Aufgabenbezug gegeben und eine weitere Datenbearbeitung zulässig ist. Umgekehrt ist es auch möglich, dass erst die Erkenntnisanfrage an einen Partnerdienst den Aufgabenbezug zu einer ausländischen Person klären kann. Dabei wird der Partnerdienst auf den Zweck der Anfrage hingewiesen. Die Daten dürfen nur zu diesem Zweck verwendet werden. Möglich ist auch, dass dabei Dritte (Privatpersonen) angesprochen werden, beispielsweise ein Meldungserstatter, um Rückfragen zu klären, die Eltern eines mutmasslich gewalttätig radikalisierten Schülers oder die Ehefrau eines mutmasslichen Dschihadreisenden. Die Bekanntgabe ist somit in solchen Fällen Mittel zum Zweck der Eingangsprüfung, untersteht den Schranken der Artikel 59–62 und ist nur zulässig, soweit dies zur Abklärung des Aufgabenbezugs nötig ist. Selbstverständlich kann dies auch bei Daten vorkommen, die bei den KND eingehen. Das Vorgehen zur notwendigen Abklärung des Aufgabenbezugs wird aus Gründen der Transparenz in diesem Gesetz ausdrücklich festgehalten.

Artikel 46 Prüfung der Anwendbarkeit von Artikel 5 Absatz 5

Absatz 1

Ist der Aufgabenbezug gegeben, stellen der NDB und die KND sicher, dass die Daten keine Inhalte aufweisen, die der Datenbearbeitungsschranke von Artikel 5 Absatz 5 unterliegen, wenn nicht eine der Ausnahmen von Artikel 5 Absatz 6 oder 8 greift. Die heutige Bestimmung von Artikel 45 Absatz 1, wonach Meldungen, die mehrere Personendaten enthalten, als Ganzes beurteilt werden, wird aufgrund der Kritik der parlamentarischen Aufsichtsbehörde fallen gelassen. Neu stellen der NDB und die KND sicher, dass die eingehenden nachrichtendienstlichen Meldungen keine Personendaten enthalten, welche gegen die Datenbearbeitungsschranke von Artikel 5 Absatz 5 verstossen, auch wenn die Meldung Daten zu mehreren Personen oder Sachverhalten enthält.

Absatz 2

Da veröffentlichte Informationen (wie gedruckte oder elektronische Medien) in der Regel jederzeit von jeder Person abgerufen werden können, ist es nicht sinnvoll, sie bei ihrer reinen Speicherung der Datenbearbeitungsschranke von Artikel 5 Absatz 5 zu unterstellen oder sie auf ihre Richtigkeit hin zu beurteilen. Die Richtigkeit von Medienberichten lässt sich oft nur nach einiger Zeit beurteilen und Medienberichte entsprechen nicht den Vorgaben des NDG, wie sie die KND bei ihren Berichten einhalten müssen. So enthalten namentlich Medienberichte zu NDG-relevanten Ereignissen (z. B. Terroranschlägen und Spionagefällen) oft Statements von Politikerinnen und Politikern zu den Vorgängen. Der NDB und die KND sollen diese trotzdem speichern dürfen, ohne eine ineffiziente und aufwändige Vorzensur ausüben zu müssen. Bei Daten aus öffentlich zugänglichen Quellen, die für die Aufgabenerfüllung benötigt werden, prüfen sie daher die Datenbearbeitungsschranke weiterhin erst, bevor sie diese als Arbeitsdaten verwenden. Diese Praxis wurde vom Bundesamt für Justiz in einem Rechtsgutachten, das es im Auftrag des VBS im Februar 2020 erstellte, bereits unter dem geltenden Recht als vertretbar beurteilt.

Eine Ausnahme besteht ebenfalls für die Daten aus GEBM, bei welchen der NDB die Einhaltung der Datenbearbeitungsschranke dann prüft, wenn er diese Daten für eine vertiefte Weiterbearbeitung kennzeichnet (vgl. den Verweis von Art. 50 Abs. 1 auf Art. 46, in dem die Eingangsprüfung beschrieben wird). Dies entspricht dem heutigen Vorgehen, das die Prüfung im Rahmen der Erfassung im IASA NDB vorsieht. Daten, die durch GEBM unter Einsatz technologischer Mittel (z. B. bei einer Kommunikationsüberwachung) beschafft werden, können zum einen sehr umfangreich sein und zum anderen viele Informationen enthalten, die nichts mit dem Aufklärungsziel zu tun haben, weil sie z. B. rein privater Natur sind. Auch dem Persönlichkeitsschutz Dritter, die z. B. den Fernmeldeanschluss der überwachten Person benutzen, ist Rechnung zu tragen. Oft lässt sich nicht auf Anhieb feststellen, ob bestimmte Kommunikationen relevant sind oder nicht, weil beispielsweise das Kontaktnetz der überwachten Person erst noch identifiziert werden muss oder weil diese zum Schutz ihrer Kontakte konspirative Elemente in der Kommunikation anwendet. Informationen können deshalb nicht sofort als notwendig oder nicht notwendig identifiziert werden. Nicht zuletzt dient die gesonderte Abspeicherung auch dem Schutz der übrigen Daten des NDB, da z. B. bei der Überwachung von Internetkommunikationen oder beim Eindringen in Computersysteme auch Schadsoftware (Viren, Trojaner) auftauchen können. Diese sollten nicht in die Daten des NDB eingeschleppt werden. Je nach Grund der gesonderten Abspeicherung erfolgt diese logisch (wenn die Daten nicht mit Schadsoftware kontaminiert sein können) oder physisch (wenn die Gefahr der Kontaminierung des übrigen Datenbestands des NDB besteht).

Artikel 47 Übertragung der Prüfpflichten

Dort, wo der NDB die Absender von Daten eingehend beauftragen und schulen kann, kann er diesen die Prüfung des Aufgabenbezugs und der Datenbearbeitungsschranke übertragen und die Daten automatisiert speichern. Dazu müssen die Anforderungen an eine Bearbeitung durch Auftragsbearbeiter nach Artikel 9 Absatz 1 DSG erfüllt sein. Dies wird heute insbesondere im Bereich der Daten aus öffentlich zugänglichen

Quellen getan, indem der CEA dem NDB Agentur- und Pressemeldungen zukommen lässt, welche einen Aufgabenbezug nach Artikel 6 aufweisen. Die Mitarbeiterinnen und Mitarbeiter des CEA werden jährlich von der Qualitätssicherungsstelle des NDB geschult. Diese prüft ebenfalls jährlich stichprobenweise, ob die auf diese Weise eingegangenen Daten einen Aufgabenbezug nach Artikel 6 aufweisen.

Artikel 48 Vorbereitungs- und Sicherheitsmassnahmen

Der NDB verfügt bereits heute über die Berechtigung, sowohl Daten aus Beschaffungen im Ausland, die mit GEBM vergleichbar sind, und Daten aus GEBM (vgl. Art. 36 Abs. 5 und Art. 58 Abs. 1) als auch besonders sensitive Daten nach Artikel 7 Absatz 2 der Verordnung vom 16. August 2017[38] über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB) gesondert abzuspeichern. Ausschlaggebend für die gesonderte Abspeicherung kann der Umfang der Daten, die Geheimhaltung (namentlich Quellenschutz) oder die Sicherheit (namentlich Gefahr der Kontaminierung des Datenbestandes und der IT-Systeme) sein. Je nach Grund muss die gesonderte Abspeicherung nicht physisch erfolgen, sondern kann auch nur logisch sein. Sie darf aber nur über eine beschränkte, vom Bundesrat im Hinblick auf den Grund der gesonderten Abspeicherung zu bezeichnende Zeit andauern. Fällt der Grund für die gesonderte Abspeicherung weg, sind die Daten in die ordentliche Ablage zu überführen. Die Eingangsprüfung beginnt auch bei diesen Daten sofort nach deren (gesonderter) Abspeicherung.

Artikel 49 Kennzeichnung von nachrichtendienstlichen Daten

Absätze 1 und 2

In diesem Artikel werden die Unterkategorien nachrichtendienstlicher Daten ausgewiesen. Diese ersetzen die heutige Kennzeichnung nach Informationssystem und ermöglichen es dem NDB, die heute für die Informationssysteme geltenden unterschiedlichen Datenbearbeitungsvorschriften und dabei insbesondere den selektiven Zugriff beizubehalten. Sämtliche beim NDB eingehende Daten sind ausnahmslos mindestens einer dieser Unterkategorien zuzuweisen (vgl. dazu auch die Ausführungen zur Eingangsprüfung zu Art. 45). Dies gilt auch für die gesondert abgespeicherten Daten. Es ist aber auch möglich, dass Daten gleichzeitig in mehrere Unterkategorien fallen. Folgende Daten-Unterkategorien entsprechen Daten in den nachstehenden aktuellen Informationssystemen:

Buchstabe a:	IASA NDB, IASA-GEX NDB, Quattro P, ISCO; Technisches Labor Cyber;
Buchstabe b:	OSINT-Portal;
Buchstabe c:	Speichersysteme GEBM;
Buchstabe d:	Speichersysteme Daten aus Beschaffungen im Ausland;
Buchstabe e:	Ablage für besonders sensitive Daten (vgl. Art. 7 VIS-NDB);

[38] SR **121.2**

Buchstabe f:	Informationssystem zur elektronischen Lagedarstellung (ELD);
Buchstabe g:	IASA NDB, IASA-GEX NDB und im KND-Index nach Artikel 29 Buchstabe b VIS-NDB;
Buchstabe h:	KND-Index nach Artikel 29 Buchstabe b VIS-NDB;
Buchstabe i:	Temporäre Ablage «Ablageprüfung»;
Buchstabe j:	IASA-Index nach Artikel 29 Buchstabe a VIS-NDB.

Innerhalb der einzelnen Daten-Unterkategorien können die Daten wiederum unterschiedlich nach Thematik kategorisiert werden, um bspw. den unterschiedlichen Aufbewahrungsfristen und Zugriffsberechtigungen Rechnung zu tragen (auf diese Weise kann bspw. die unterschiedliche Handhabung der heutigen Daten von IASA NDB und IASA-GEX NDB beibehalten werden).

Artikel 50 Daten aus genehmigungspflichtigen Beschaffungsmassnahmen

Absatz 1

Dieser Absatz entspricht weitgehend dem heutigen Artikel 58 Absatz 2. Neu ist vorgesehen, dass die Eingangsprüfung bei diesen Daten spätestens dreissig Tage nach Abschluss der dazugehörigen Operation nach Artikel 46 vorgenommen werden muss. Dies ist erforderlich, weil oftmals Daten(-bestände) nicht gleich bei ihrer Abspeicherung eingangsgeprüft werden können und auch mit anderen Daten, die im Rahmen der Operation erhoben werden, in einen Kontext gestellt werden müssen. Die Daten dürfen aber erst nach erfolgter Eingangsprüfung verwendet werden (vgl. den Verweis auf Art. 46). Weisen die Daten einen Bezug zu laufenden Operationen auf, werden sie im Rahmen der Eingangsprüfung als Roh- oder Arbeitsdaten gekennzeichnet. Ist dies nicht der Fall, müssen sie vernichtet werden. Dabei ändert sich das Anknüpfungskriterium der Frist für die Vernichtung. Der Grund dafür ist der Umstand, dass eine Operation mehrere Monate oder sogar Jahre andauern kann, während einzelne Beschaffungsmassnahmen schon bereits nach wenigen Tagen beendet sein können. Im Schnitt dauert eine Operation nach der bisherigen Erfahrung des NDB sechs Monate bis zwei Jahre. Das führt dazu, dass heute Daten vernichtet werden müssen, obwohl deren Auswertung noch gar nicht abgeschlossen ist oder deren Relevanz erst im weiteren Verlauf der Operation beurteilt werden könnte.

Zur Veranschaulichung folgende Beispiele: Betreffend einen dem NDB bekannten ausländischen Nachrichtendienstoffizier in der Schweiz (Person A) führt der NDB im Zusammenhang mit der Vergiftung eines Oppositionspolitikers im Ausland eine Operation durch, um die Involvierung von Person A in die Vergiftung abzuklären. Im Rahmen dieser Operation werden GEBM gegen die Person A durchgeführt und die Randdaten seiner Kommunikationsmittel abgefragt. In diesen Randdaten entdeckt der NDB Kontakte der Person A zu verschiedenen staatlichen Stellen, anderen Nachrichtendienstoffizieren und der Person B. Person B ist dem NDB nicht bekannt und er muss die Daten zu ihr einen Monat nach Abschluss der GEBM, das heisst nach Erhalt der Randdaten, vernichten. Die Operation dauert fort und zwei Monate später wird dem NDB bekannt, dass die Person B im Verdacht stehe, Teil des Chemiewaffenpro-

gramms des betroffenen Landes zu sein. Da die Resultate aus der GEBM bereits vernichtet sind, kann der NDB keine Verbindung zwischen den Personen A und B feststellen, obschon die Operation insgesamt noch nicht beendet ist.

Vor allem bei der rückwirkenden Auswertung von Randdaten von Fernmeldeanschlüssen ist die heutige Monatsfrist sehr problematisch, weil die GEBM mit der Übergabe der Randdaten aus maximal sechs Monaten beendet ist, während die Auswertung der Daten deutlich mehr Zeit als einen Monat in Anspruch nehmen kann. Der NDB muss die Abonnentinnen und Abonnenten sowie die mutmasslichen Benutzerinnen und Benutzer der Kommunikationspartner der überwachten Person abklären und identifizieren. Danach ist es wichtig, dass die Ergebnisse der verschiedenen GEBM untereinander abgeglichen werden, um mögliche Schlüsselpersonen entdecken zu können. Die Identifizierungen und die Abklärungen bei ausländischen Partnerdiensten des NDB dauern häufig bis zum Ende einer Operation an. Ein vorgängiges Vernichten der Informationen kann damit sowohl die Ziele der Operation gefährden wie auch die Glaubwürdigkeit des NDB gegenüber den Partnern in Frage stellen.

Es ist deshalb notwendig, den Zeitpunkt für die Vernichtung auf einen Monat nach Abschluss der Operation festzulegen.

Absatz 2

Dieser Absatz entspricht dem ersten Satz des heutigen Artikels 58 Absatz 3 und enthält nur formelle Klarstellungen.

Absatz 3

Dieser Absatz entspricht dem zweiten Satz des heutigen Artikels 58 Absatz 4, enthält nur formelle Klarstellungen und wurde zur besseren Verständlichkeit von Absatz 2 getrennt.

Absatz 4

Dieser Absatz entspricht dem heutigen Artikel 58 Absatz 4 und enthält nur formelle Klarstellungen.

3. Abschnitt: Arbeitsdaten

Artikel 51 Prüfung auf Richtigkeit

Absatz 1

Die Überprüfung der Richtigkeit von Daten setzt voraus, dass diese mit weiteren Informationen in einen Kontext gestellt werden. Diese nachrichtendienstliche Auseinandersetzung mit dem Inhalt der Daten kann nicht bereits beim Abspeichern erfolgen, siehe dazu auch die Ausführungen im erläuternden Bericht zur NDV und zur VIS-NDB.[39] Sie geschieht beim Übergang der Rohdaten zu Arbeitsdaten. Das Ergebnis der Prüfung wird festgehalten. Ungeprüfte Daten (Rohdaten) dürfen grundsätzlich nicht für die nachrichtendienstliche Auswertung und Produktion verwendet werden

[39] Abrufbar unter: www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2017 > VBS > Vernehmlassung 2017/4 > Bericht.

und entfalten keinerlei Aussenwirkungen. Eine sehr begrenzte Ausnahme gilt lediglich für den blossen Zugriff der KND auf Daten aus öffentlich zugänglichen Quellen in Artikel 58*e* Absatz 2 E-NDG. Jede weitere Verwendung bedingt aber auch hier eine vorgängige Datenprüfung.

Absatz 2

Der NDB muss auch weiterhin «Desinformationen» und «Falschinformationen» nicht nur zur Beurteilung der Lage oder einer Quelle bearbeiten können, sondern auch für andere Aufgaben, die in Artikel 6 aufgezählt sind. In den letzten Jahren haben hohe Stellen ausländischer Regierungen, aber auch Private vermehrt Falschinformationen eingesetzt, um z. B. verdeckten Einfluss auf politische Entscheidprozesse oder die öffentliche Meinung zu nehmen, um von einem Ereignis abzulenken oder um eine öffentliche Debatte zu steuern und so ganze Gesellschaften anderer Länder zu destabilisieren. Dazu werden Personen direkt angegriffen und Falschinformationen über sie verbreitet. Wichtig sind in diesem Zusammenhang auch die besonders schützenswerten Informationen, da es gerade bei diesen die Möglichkeit der bewussten, manipulativen Falschinformation (z. B. über den Gesundheitszustand eines sicherheitspolitisch relevanten Staatschefs) gibt. Diese Informationen muss der NDB zur Erfüllung seiner Aufgaben nach Artikel 6 und in Abweichung vom Grundsatz der Datenrichtigkeit nach Artikel 6 Absatz 5 DSG bearbeiten können.

Absatz 3

Damit die als «Desinformation» oder «Falschinformation» beurteilten Daten klar identifiziert werden können, kennzeichnet der NDB sie als falsch.

Artikel 52 Bearbeitungszwecke

Absatz 1

In diesem Absatz werden die Zwecke aufgelistet, zu denen der NDB und die KND Daten bearbeiten dürfen. Die Bearbeitungszwecke sind heute bei den betreffenden Informations- und Speichersystemen geregelt und bleiben unverändert (vgl. dazu auch die Ausführungen oben zu Art. 49). Neu wird aus Gründen der Transparenz ausgewiesen, dass der NDB auch zur Durchführung von Schutz- und Sicherheitsmassnahmen Daten bearbeiten darf (vgl. Bst. b).

Absatz 2

Aus Gründen der Transparenz soll neu explizit geregelt werden, dass der NDB und die KND auch entlastende Personendaten bearbeiten dürfen (bspw. wenn die vom NDB bei einem KND in Auftrag gegebenen Umfeldabklärungen ergeben, dass eine von einem Partnerdienst als gewalttätig gemeldete Person – zumindest nach den Erkenntnissen des KND – als gewaltlos einzustufen ist). Dies aber nur unter der Voraussetzung, dass zur gleichen Person oder Organisation bereits belastende Personendaten bearbeitet wurden und diese nun teilweise oder ganz entkräftet werden. Je nach Bedeutung der Daten kann das dazu führen, dass sie im Anschluss vorzeitig gelöscht und archiviert oder vernichtet werden.

Artikel 53 Profilings

Im DSG wird der Begriff des Persönlichkeitsprofils nicht mehr verwendet. Dieser wird neu durch «Profiling» oder «Profiling mit hohem Risiko» ersetzt, was hier übernommen wird.

Der NDB wird in Zukunft verstärkt auf die automatisierte Auswertung seiner Daten angewiesen sein, um auf dieser Grundlage, teilweise in automatisierter Weise, die Merkmale einer Person erkennen und bewerten zu können oder zum automatisierten Vergleich eingehender oder selbst beschaffter Daten mit bestehenden nachrichtendienstlichen Daten. Dies ist denkbar für die Evaluation eines Bewegungsprofils einer Zielperson, die zeitliche Aufarbeitung von Ereignissen oder um Veränderungen im Verhalten von Personen (Radikalisierung etc.) aufzuzeigen. Der Einsatz von lernfähigen Programmen zur Suche und Kategorisierung von Informationen ist heute für die effiziente Aufgabenerfüllung des NDB unabdingbar und wird auch von Aufsichtsgremien gefordert. Schliesslich sei darauf hingewiesen, dass die im Entwurf gewählte Formulierung bspw. mit jener des Bundesgesetzes vom 20. März 1981[40] über die Unfallversicherung übereinstimmt.

Da heute die automatisierte Bearbeitung und Auswertung von Daten (d. h. in einem Computersystem und nicht auf Papier) der Regelfall ist, wird neu auf eine entsprechende Berechtigungsklausel im Gesetz verzichtet (Art. 44 Abs. 4 NDG; vgl. dazu auch Art. 7 DSG, der von der automatisierten Datenbearbeitung ausgeht).

Artikel 54 Festlegung von Kategorien ausländischer Personen

Dieser Artikel entspricht inhaltlich dem heutigen Artikel 55 Absätze 1 und 4. Auch die darin enthaltene Delegation an den Bundesrat geht nicht über die aktuelle Regelungskompetenz hinaus.

Artikel 55 Ausführungsbestimmungen

Dieser Artikel entspricht weitgehend dem heutigen Artikel 47 Absatz 2 und übernimmt ebenfalls die Rechtsetzungsdelegationen an den Bundesrat aus dem heutigen Artikel 58 Absatz 6. Gestrichen wurden die Zuständigkeiten bei der Datenbearbeitung, da sich diese aus der Regelung der Zugriffsberechtigungen ergeben. Hinzugefügt wurde der Transparenz halber in Buchstabe e die Vernichtung von Daten. Zu den einzelnen Delegationskompetenzen ist Folgendes zu bemerken:

Buchstabe a: Der Katalog der Personendaten wird heute in den Anhängen der VIS-NDB geregelt. Es ist nicht beabsichtigt, diesen zu ändern oder zu erweitern.

Buchstabe b: Die Zugriffsrechte werden heute in den Anhängen der VIS-NDB geregelt. Es ist nicht beabsichtigt, sie wesentlich zu ändern oder zu erweitern (Ausnahmen: Gruppe Verteidigung und Bundesamt für Zoll- und Grenzsicherheit [BAZG]).

40 SR **832.20**

Buchstabe c: Die Häufigkeit der Qualitätssicherung ist heute in der VIS-NDB bei jedem Informationssystem separat geregelt. Es ist nicht beabsichtigt, sie zu ändern oder zu verringern.

Buchstabe d: Die Aufbewahrungsdauer wird heute in der VIS-NDB ebenfalls bei jedem Informationssystem separat geregelt. Es ist nicht beabsichtigt, sie zu ändern oder zu verlängern.

Buchstabe e: Die Löschung und Vernichtung von Daten wird heute in Artikel 8, 9 und 70 VIS-NDB geregelt. Es ist nicht beabsichtigt, diese Vorgaben zu ändern.

Buchstabe f: Die Datensicherheit wird heute in Artikel 13 VIS-NDB geregelt. Es ist nicht beabsichtigt, diese Vorgaben zu ändern.

4. Abschnitt: Datenbearbeitung durch kantonale Vollzugsbehörden

Artikel 56 Arbeitsumgebung

Absatz 1

Der Begriff «Datensammlung» wird mit dem DSG abgeschafft. Er wird hier durch den auch inhaltlich stimmigeren Begriff «Arbeitsumgebung» ersetzt. Die KND bearbeiten die NDG-relevanten Daten in der vom NDB zur Verfügung gestellten Arbeitsumgebung. Diese befindet sich innerhalb des gesicherten Computernetzwerks des NDB (vgl. Art. 7 Abs. 2). Die KND dürfen keine eigenen Informatikmittel benutzen.

Absatz 2

Neu wird aus Gründen der Transparenz klargestellt, dass die KND dazu berechtigt sind, Daten für den Transfer in die speziell gesicherten Computernetzwerke, in dem sich die vom Bund zur Verfügung gestellte Arbeitsumgebung befindet (vgl. Art. 7 Abs. 2), für kurze Zeit in ihrer kantonalen Arbeitsumgebung zwischenzuspeichern. Es ergibt sich aus der Natur der Sache, dass die KND Daten, welche sie beschaffen (z. B. Fotos, Register- oder Internetauszüge), erst digitalisieren und zwischenspeichern müssen, bevor sie diese über eine besonders gesicherte Schnittstelle in die vom Bund zur Verfügung gestellte Arbeitsumgebung transferieren können. Eine direkte Eingabe in die vom Bund zur Verfügung gestellte Arbeitsumgebung ist derzeit aus Gründen der Informationssicherheit nicht möglich. Auf die Daten in der kantonalen Arbeitsumgebung haben nur die Leiterin oder der Leiter des KND sowie deren oder dessen Stellvertreterin oder Stellvertreter und die Person Zugriff, welche die Daten abgespeichert hat. Aus Gründen der Informationssicherheit sollten die in der kantonalen Arbeitsumgebung abgespeicherten Daten gleich nach deren Überführung in die vom Bund zur Verfügung gestellte Arbeitsumgebung vernichtet werden.

Artikel 57 Bearbeitung nach kantonalem Recht

Dieser Artikel entspricht dem heutigen Artikel 46 Absatz 2 und enthält nur formelle Klarstellungen. Insbesondere wird klargestellt, dass es sich um kantonale Daten handelt, wenn die KND in Anwendung des kantonalen Rechts (z. B. Polizeirecht) tätig werden. Diese Daten sind von den Daten, welche sie gestützt auf das NDG bearbeiten, strikt zu trennen. Hinweise auf das Vorhandensein und den Inhalt von Daten, die gestützt auf das NDG bearbeitet werden, sind nur zulässig, sofern der NDB dies ausdrücklich bewilligt (z. B. bei Amtsberichten oder anderen berechtigten Bekanntgaben).

Artikel 58 Bekanntgabe

Absatz 1

Die Artikel 33 und 33*a* NDV regeln nicht nur die Bekanntgabe von Daten, welche die KND vom NDB erhalten haben, sondern auch die Bekanntgabe von Daten, welche diese in eigener Kompetenz beschafft haben. Damit dafür eine ausreichende gesetzliche Grundlage besteht, wird die heutige Regelung in diesem Absatz entsprechend ergänzt. Mit den Ergänzungen sind keine Kompetenzerweiterungen verbunden. Der Begriff «Lagebeurteilung» wurde gestrichen, da es sich dabei auch um Daten im Sinne des DSG handelt. Auch die Rechtsetzungsdelegation an den Bundesrat bleibt inhaltlich unverändert, allerdings wird «welche Stellen» durch «wen» ersetzt und in Anlehnung an das DSG wird von «Zweck der Bekanntgabe» statt von «Umfang der Weitergabe» gesprochen. Unter diese Bestimmung zu subsumieren ist auch die Bekanntgabe von Daten zur Beauftragung der Observationseinheit einer Kantonspolizei und die Bekanntgabe von Daten um ein Auskunftsbegehren (Abklärungsauftrag).

Absatz 2

Dieser Absatz stellt klar, dass die KND für Sicherheitsfragen im Grenzgebiet auch den dafür zuständigen ausländischen Polizeibehörden Daten bekannt geben dürfen.

Absatz 3

Bei der Bekanntgabe von Daten sind die KND an die Vorgaben der Artikel 59–62 gebunden.

Artikel 58a Aufbewahrungsdauer

Die KND sollen ihre Daten auch weiterhin maximal fünf Jahre aufbewahren dürfen. Während dieser Zeit haben sie die Möglichkeit, dem NDB Bericht zu erstatten. Durch die Berichterstattung verlängert sich die Aufbewahrungsfrist der entsprechenden Informationen und der Kreis der Zugriffsberechtigten wird auf die zugriffsberechtigten Mitarbeiterinnen und Mitarbeiter des NDB und der KND erweitert. Wie oben zu Artikel 9 Absatz 3 ausgeführt, haben die KND die Pflicht, sämtlichen Hinweisen auf Tätigkeiten nach Artikel 6 Absatz 1 Buchstabe a nachzugehen und diese abzuklären. Dabei ist es möglich, dass die Abklärungen ergeben, dass es sich nicht um eine vom Aufgabengebiet dieses Gesetzes abgedeckte Tätigkeit handelt, womit der Aufgabenbezug nicht gegeben ist (vgl. dazu das Beispiel zu Art. 9 Abs. 3). Da solche Hinweise zeitlich verzögert und von verschiedenen Melderinnen und Meldern bei den KND

eingehen und es zu verhindern gilt, gleiche Abklärungen mehrmals vorzunehmen, sollen die KND solche Daten auch weiterhin zum Zweck der Nachvollziehbarkeit während fünf Jahren aufbewahren können. Dies wird neu aus Transparenzgründen klargestellt. Im Hinblick auf die kurze Aufbewahrungsdauer, wird auch weiterhin auf eine periodische Überprüfung der Daten durch die KND verzichtet.

5. Abschnitt: Datenbearbeitung zum Nachrichtenverbund

Artikel 58b

Absatz 1

Dieser Absatz entspricht inhaltlich dem heutigen Artikel 53 Absätze 1 und 3 und gibt dem NDB die Berechtigung, das nach Artikel 55 Absatz 1 der Bevölkerungsschutzverordnung vom 11. November 2020[41] vom BABS betriebene Informationssystem ELD auch weiterhin zur Führung des Nachrichtenverbunds zu nutzen. Es ist aber nicht ausgeschlossen ist, dass der NDB in Zukunft eine eigene Informatiklösung realisiert oder sich derjenigen eines Kantons anschliesst und auf dieser den Nachrichtenverbund führt. Deshalb wird im vorliegenden Artikel der Nachrichtenverbund geregelt, nicht die momentane Informatiklösung, mit welcher dieser betrieben wird.

Absätze 2 und 3

Zusätzlich zu den vom NDB selbst bearbeiteten Informationen enthält der Nachrichtenverbund schon heute auch Informationen anderer Behörden, die weniger restriktiven Datenschutzvorschriften unterstellt sind. Deswegen kann es sein, dass der Nachrichtenverbund Daten enthält, die der NDB nach diesem Gesetz selbst nicht bearbeiten dürfte. Der Nachrichtenverbund soll jedoch nicht nur die Bedürfnisse des NDB abdecken, sondern jene aller Sicherheitsbehörden der Schweiz. Dies hat auch Auswirkung auf die Qualitätssicherung der Daten im Nachrichtenverbund: Da auch hier je nach Behörde unterschiedliche Vorgaben bestehen, sieht Artikel 58*b* Absatz 3 vor, dass inskünftig jene Behörde zuständig ist, welche die Daten abgespeichert hat. Dies ist für das fedpol heute in Artikel 44 Absatz 4 VIS-NDB geregelt. Heute ist im Hinblick auf allfällige Verstösse gegen die Datenbearbeitungsschranke des NDG auch die Aufbewahrungsfrist der vom fedpol abgespeicherten Daten kürzer (vgl. Art. 45 Abs. 2 VIS-NDB). Dies soll für alle nicht vom NDB oder von den KND abgespeicherten Daten weiterhin gelten (vgl. die weiteren Ausführungen zum Nachrichtenverbund auch in den Erläuterungen zu Art. 5 Abs. 6 Bst. e).

6. Abschnitt: Zugriffsberechtigungen

Die Zugriffsberechtigung der AB-ND wird in Artikel 78*a* Absatz 4 geregelt.

Artikel 58c Zugriff auf nachrichtendienstliche Daten des NDB

Absatz 1

41 SR **520.12**

Die Zugriffsberechtigungen der Mitarbeiterinnen und Mitarbeiter des NDB werden heute bei den betreffenden Informations- und Speichersystemen geregelt. Dies erschwert es, sich eine Übersicht zu verschaffen. Neu wird die Zugriffsberechtigung deshalb zentral für alle nachrichtendienstlichen Daten des NDB im vorliegenden Absatz geregelt und zwar dahingehend, dass nur insofern auf diese zugegriffen werden darf, als dies die Erfüllung der gesetzlichen Aufgaben erfordert. Das heisst bspw., dass nicht mehr alle Mitarbeiterinnen und Mitarbeiter des NDB Zugriff auf Daten aus öffentlichen Informationsquellen (Art. 13) haben, sondern nur noch jene, die einen Zugriff benötigen, um ihre gesetzlichen Aufgaben zu erfüllen. Andererseits gibt es aber auch Mitarbeiterinnen und Mitarbeiter, die heute nicht zugriffsberechtigt sind, einen Zugriff aber für die Erfüllung ihrer gesetzlichen Aufgaben benötigen (bspw. die Qualitätssicherungsstelle und die Datenschutzberatung für die Durchführung von Kontrollen oder der Rechtsdienst für die Bearbeitung von Gesuchen). Neu wird auch derjenigen Stelle des NDB, die für die Durchführung von Schutz- und Sicherheitsmassnahmen zuständig ist, ein Zugriff auf nachrichtendienstliche Daten eingeräumt, damit diese beispielsweise bei der Anstellung neuer Mitarbeiterinnen und Mitarbeiter des NDB prüfen kann, ob über diese Daten vorliegen (vgl. zu den Aufgaben dieser Stelle auch Art. 7 und 7*a*).

Absatz 2

In der Vergangenheit kam es mehrmals vor, dass der NDB einen KND für umfangreiche Auswertungen oder die Durchführung einer Operation vorübergehend um personelle Ressourcen bat. Diese Einsätze waren aber bis anhin wenig effizient, da die Mitarbeiterinnen und Mitarbeiter des KND keine Zugriffsberechtigung auf die den Mitarbeiterinnen und Mitarbeitern des NDB zur Verfügung stehenden Daten des NDB hatten. Dies soll nun geändert werden. Solange die Mitarbeiterinnen und Mitarbeiter eines KND beim NDB eingesetzt werden, werden sie den Mitarbeiterinnen und Mitarbeitern des NDB gleichgestellt und erhalten, sofern dies notwendig ist, die gleichen Zugriffsberechtigungen.

Artikel 58d Zugriff auf nachrichtendienstliche Daten der kantonalen Vollzugsbehörden

Absatz 1

Die Zugriffsberechtigung der Mitarbeiterinnen und Mitarbeiter der KND auf ihre eigenen Daten (vgl. Art. 49 Bst. h) bleibt unverändert.

Absatz 2

Dieser Absatz entspricht dem heutigen Artikel 54 Absatz 4. Der Zugriff der KND wird aber auf die Erfüllung ihres gesetzlichen Auftrags beschränkt.

Absatz 3

Von einigen KND und der KKJPD wurde gefordert, dass die KND gegenseitig Zugriff auf ihre nachrichtendienstlichen Daten nach Artikel 49 Buchstabe h erhalten (heute haben die KND nur auf die Daten Zugriff, die sie in ihrer eigenen, vom NDB zur Verfügung gestellten NDG-Arbeitsumgebung abgespeichert haben). Dies, um mit wenig Aufwand herauszufinden, ob der KND eines Nachbarkantons zu einer Person oder

Organisation gestützt auf dieses Gesetz ebenfalls bereits Daten bearbeitet. Dies ist insbesondere bei laufenden Abklärungen sinnvoll, also zum Zeitpunkt, zu dem die betroffene Person oder Organisation noch nicht dem NDB gemeldet und dort registriert wurde und die KND nicht in der Lage sind, auf diese Weise festzustellen, ob ein anderer KND gestützt auf dieses Gesetz Daten zur betreffenden Person oder Organisation bearbeitet. Da nicht alle KND mit dieser Zugriffsvergabe einverstanden sind, wird dies hier nur als «Kann-Vorschrift» geregelt. Details der Zugriffe können somit im Verordnungsrecht geregelt werden.

Absatz 4

Die Qualitätssicherungsstelle des NDB hat die Aufgabe, die Datenbearbeitung der KND stichprobenweise zu überprüfen (vgl. Art. 58*j* Abs. 1 E-NDG). Zu diesem Zweck hat sie schon heute Zugriff auf die Daten der KND, was der Vollständigkeit halber nachgetragen wird.

Absatz 5

In der Vergangenheit kam es mehrmals vor, dass der NDB einen KND für umfangreiche Auswertungen oder die Durchführung einer Operation vorübergehend personell verstärkte. Diese Einsätze waren aber bis anhin wenig effizient, da die Mitarbeiterinnen und Mitarbeiter des NDB keine Zugriffsberechtigung auf die den Mitarbeiterinnen und Mitarbeitern des KND zur Verfügung stehenden Daten des KND hatten. Dies soll nun geändert werden. Solange die Mitarbeiterinnen und Mitarbeiter des NDB bei einem KND eingesetzt werden, werden sie den Mitarbeiterinnen und Mitarbeitern des KND gleichgestellt und erhalten, sofern dies notwendig ist, die gleichen Zugriffsberechtigungen.

Artikel 58e Zugriff von Behörden auf nachrichtendienstliche Daten des NDB

Absatz 1

Analog der heutigen Regelung von Artikel 51 erhalten die KND und Bundesbehörden nicht Zugriff auf sämtliche Daten des NDB, sondern grundsätzlich nur auf jene Daten, die zur Identifizierung einer Person, einer Organisation, einer Gruppierung, eines Gegenstands oder eines Ereignisses notwendig sind, sofern der NDB in Erfüllung seiner Aufgaben dazu Daten bearbeitet. Heute sind das die im IASA-GEX und im IASA NDB erfassten Objekte, die in den IASA INDEX gespiegelt werden. Wie heute werden diesen Behörden inskünftig somit die einer Person, Organisation usw. zugeordneten Daten selbst nicht via Abrufverfahren offengelegt, sondern es wird nur ein Treffer ausgewiesen, wenn bspw. Name, Vorname und Geburtsdatum oder die Firma übereinstimmen. Die Bekanntgabe weiterer Daten müssen die anfragenden Behörden mit Begründung auf dem Weg der Amtshilfe beim NDB beantragen (vgl. Abs. 2).

Die Zugriffsberechtigungen sowohl innerhalb des NDB, als auch bei den KND und anderen Externen, die heute bereits Zugriff haben, bleiben grundsätzlich unverändert. Es gilt weiterhin der Grundsatz der Verhältnismässigkeit, der verlangt, dass der Zugriff auf einer Need-to-know-Basis erfolgt. Der Bundesrat erhält in Artikel 55 Buchstabe b E-NDG den Auftrag, die detaillierten Zugriffsberechtigungen wie bisher zu regeln.

Buchstabe a

An der Zugriffsberechtigung der KND ändert sich nichts.

Buchstabe b

Das fedpol erhält weiterhin Zugriff, um feststellen zu können, ob der NDB zu einer Person, einer Organisation, einer Gruppierung, einem Gegenstand oder einem Ereignis nachrichtendienstliche Daten bearbeitet (vgl. den heutigen Art. 51 Abs. 4 Bst. c). Die einer Person, Organisation etc. zugeordneten Daten werden nicht im Abrufverfahren offengelegt. Die Bekanntgabe dieser Daten muss das fedpol mit Begründung beim NDB beantragen. Das fedpol benötigt die vorliegende Zugriffsberechtigung auch für die Wahrnehmung gerichtspolizeilicher Aufgaben, weshalb die Aufzählung in diesem Absatz transparenterweise entsprechend ergänzt wurde.

Buchstabe c

Heute gibt es zwei Fachstellen, die Personensicherheitsprüfungen durchführen: Eine in der BK und eine im VBS. Beide Stellen haben zu diesem Zweck Zugriff auf nachrichtendienstliche Daten des NDB. Mit einer allgemeineren aufgabenbezogenen Formulierung soll neu verhindert werden, dass bei einer erneuten Anpassung der organisatorischen Angliederung einer Fachstelle eine Gesetzesänderung notwendig wird. Zudem werden die Zugriffe für beide Fachstellen am selben Ort geregelt. Die Anpassungen sind daher rein formeller Natur. An der Zugriffsberechtigung ändert sich nichts (vgl. den heutigen Art. 51 Abs. 4 Bst. d). Die für die Personensicherheitsprüfungen zuständigen Fachstellen erhalten weiterhin Zugriff, um feststellen zu können, ob der NDB zu einer Person, einer Organisation, einer Gruppierung, einem Gegenstand oder einem Ereignis nachrichtendienstliche Daten bearbeitet. Ihnen werden die einer Person, Organisation etc. zugeordneten Daten nicht im Abrufverfahren offengelegt. Die Bekanntgabe dieser Daten müssen sie auf dem Weg der Amtshilfe mit Begründung beim NDB beantragen.

Buchstabe d

Im Rahmen der zweiten Ämterkonsultation beantragte das Staatssekretariat für Sicherheitspolitik mit Hinweis auf die Artikel 55–58 ISG für die für Betriebssicherheitsverfahren zuständige Fachstelle einen analogen Zugriff wie jener der Fachstellen, die für Personensicherheitsprüfungen zuständigen sind. Dies zur Durchführung der Beurteilung von Betrieben.

Buchstabe e Ziffer 1

Neu sollen aufgrund ihrer gesetzlichen Aufgaben auch die Mitarbeiterinnen und Mitarbeiter des BAZG, die mit der Strafverfolgung und Risikoanalyse (vgl. Bst. f) betraut sind, Zugriff erhalten. Auch sie können nur feststellen, ob der NDB zu einer Person, Organisation etc. nachrichtendienstliche Daten bearbeitet. Die Bekanntgabe weitergehender Daten müssen sie mit Begründung auf dem Weg der Amtshilfe beantragen.

Diese neuen Zugriffe werden ebenfalls durch die Revision des ZG resp. durch das BAZG-VG aufgenommen und im geltenden NDG verankert. Die Mitarbeiterinnen und Mitarbeiter des BAZG, die mit der Strafverfolgung betraut sind, benötigen den Zugriff zur Wahrnehmung von Aufgaben des BAZG im Bereich der Strafverfolgung, soweit das Bundesrecht diese vorsieht. Damit sollen auch eine Effizienzsteigerung

erreicht und das Beschleunigungsgebot im Strafverfahren unterstützt werden. Weiter erlaubt der Zugriff eine umfassendere Einschätzung von Beschuldigten und neue Ermittlungsansätze insbesondere betreffend das Umfeld von Beschuldigten. Zudem ist so auch die bessere Beurteilung hinsichtlich einer Meldung von Personen mit Gefährdungspotenzial im Zuständigkeitsbereich des NDB, die in einem Strafverfahren des BAZG auftauchen, möglich.

Buchstabe e Ziffer 2

Die Mitarbeiterinnen und Mitarbeiter des BAZG, die mit der Risikoanalyse betraut sind, benötigen den Zugriff für die Überwachung des grenzüberschreitenden Waren- und Personenverkehrs. Auch dieser Zweck für den Zugriff stimmt mit der entsprechenden Formulierung der Aufgabe des BAZG überein. Die Nutzung der Daten hilft der Risikoanalyse des BAZG, um Analyseergebnisse zielgerichtet mit dem NDB abzustimmen und mögliche Zusammenhänge verschiedener Vorgänge zu erkennen. Dies unterstützt auch die Formulierung von Kontrollanweisungen zuhanden der mit Personen-, Waren- und Transportmittelkontrollen betrauten Mitarbeiterinnen und Mitarbeiter des BAZG. Ihnen werden die einer Person, Organisation etc. zugeordneten Daten nicht im Abrufverfahren zugänglich gemacht. Die Bekanntgabe dieser Daten müssen sie auf dem Weg der Amtshilfe mit Begründung beim NDB beantragen.

Tritt diese Vorlage vor dem BAZG-VG in Kraft, muss Buchstabe e angepasst werden bzw. muss der Zugriff des BAZG vorübergehend dem geltenden Zollrecht Rechnung tragen.

Buchstabe f

Neu zugriffsberechtigt ist die Gruppe Verteidigung der Schweizer Armee zum präventiven Schutz der Armee vor Spionage, Sabotage und weiteren rechtswidrigen Handlungen im Friedensförderungs- oder Aktivdienst. Diese Zugriffsberechtigung trägt dem Umstand Rechnung, dass der Dienst für präventiven Schutz der Armee (DPSA) im Zusammenhang mit der Friedensförderung (Armeeeinsatz im Balkan) fortlaufend Personen abklären muss. 2020 richtete er über hundert schriftliche Anfragen an den NDB. Aufgrund der Aufgaben im Friedensförderungsdienst hat der DPSA Zugang zu Informationen im Zusammenhang mit Terrorismus, gewalttätigem Extremismus und Spionage. Aufgrund der Diaspora aus dem Balkan in der Schweiz stehen solche Informationen oft in Zusammenhang mit der inneren Sicherheit oder umgekehrt mit der Sicherheit der Schweizer Armee im Friedensförderungsdienst. Ein rascher und effizienter Informationsaustausch kann somit für die Sicherheit massgeblich sein. Mit dem Zugriff im Abrufverfahren kann der Aufwand (insbesondere bei den rund 50 % nicht Verzeichneten) erheblich reduziert werden. Zugriffsberechtigt sollen nur jene Mitarbeiterinnen und Mitarbeiter des DPSA sein, die im operativen Geschäft tätig sind (Funktion «Kommissär DPSA»). Auch sie können nur feststellen, ob der NDB zu einer Person, Organisation etc. nachrichtendienstliche Daten bearbeitet. Die Bekanntgabe dieser Daten müssen sie auf dem Weg der Amtshilfe mit Begründung beim NDB beantragen.

Absatz 2

Neu wird aus Gründen der Transparenz ausgewiesen, dass die KND und Bundesbehörden nach einem positiven Abfrageresultat den NDB darum ersuchen müssen, ihnen

weitere Daten bekannt zu geben. Das Gesuch muss begründet werden. Die Datenbekanntgabe unterliegt den Einschränkungen der Artikel 59 und 60.

Absatz 3

Neu soll der NDB die Möglichkeit haben, seine Produkte (Lagedarstellungen, Analysen und Berichte) den Kunden zur Beurteilung der Auswirkungen sicherheitspolitischer Bedrohungen und zur sicherheitspolitischen Führung online zur Verfügung zu stellen. Dies hat sich bei den KND bewährt, indem der NDB ihnen klassifizierte Lageberichte oder OSINT-Monitoring-Produkte auf der Informations-Plattform der vom Bund zur Verfügung gestellten Arbeitsumgebung abspeichert. Auf diese Weise kann verhindert werden, dass der NDB diese Produkte kopieren und mit einem grossen Verteilerkreis per E-Mail oder in Papier verteilen muss. Zudem ist sichergestellt, dass der NDB die Daten pflegen und nach einer bestimmten Zeit löschen kann, was bei den anderen Übermittlungsformen nicht sichergestellt werden kann. Die Bekanntgabe der Produkte erfolgt unter dem Vorbehalt der Artikel 59 und 60.

Absatz 4

Der NDB ist verpflichtet sicherzustellen, dass die den Drittbehörden gewährten Zugriffe nicht missbraucht werden. Deshalb führt er Stichproben durch und ist dazu berechtigt, sich von den betroffenen Behörden darlegen zu lassen, weshalb sie wann auf welches Produkt zugegriffen haben.

Artikel 58f Zugriff Dritter auf nachrichtendienstliche Daten des NDB

Absatz 1

Neu ist ein auftragsbezogener und zeitlich begrenzter Zugriff von externen Personen vorgesehen (vgl. Abs. 4). Dies entspricht ebenfalls der heutigen Praxis und ist bspw. notwendig für Übersetzungen oder beim Betrieb und der Weiterentwicklung der Informatiklösungen durch externe Leistungserbringer.

Absatz 2

Darüber hinaus ist neu ein Zugriff für Personen vorgesehen, die an Projekten der Früherkennung beteiligt sind. Der NDB beabsichtigt bspw. eine «Crowdsourcing»-Plattform zur Einschätzung der Eintrittswahrscheinlichkeit von sicherheitspolitisch relevanten Ereignissen zu führen. Im Vordergrund dieser Plattform stehen individuelle und aggregierte Einschätzungen von Eintrittswahrscheinlichkeiten zu sicherheitsrelevanten Fragestellungen. In einer Anfangsphase nehmen an diesem Projekt nur Mitarbeiterinnen und Mitarbeiter des NDB teil. Diese können mit ihren pseudonymisierten Benutzerkonten ihre Einschätzungen zu lagerelevanten Ereignissen sowie Begründungen und Kommentare abgeben. Danach ist geplant, den Teilnehmerkreis auf Partner des Nachrichtenverbunds, Universitäten und Think Tanks auszuweiten. Bezüglich der Zugriffsberechtigungen gilt weiterhin der Grundsatz der Verhältnis-mässigkeit, der verlangt, dass der Zugriff auf einer Need-to-know-Basis erfolgt. So werden beispielsweise auch weiterhin nur jene Mitarbeiterinnen und Mitarbeiter Zugriff auf Daten aus GEBM haben, die mit der Durchführung einer Beschaffungsmassnahme und der Auswertung der Ergebnisse beauftragt sind. Der umfassende Zugriff der AB-ND wird in Artikel 78*a* Absatz 4 E-NDG geregelt.

Daneben sollen auch Dritten, die den NDB bei der Erfüllung seiner gesetzlichen Aufgaben temporär unterstützen, zeitlich und inhaltlich begrenzt auf die Aufgabenerfüllung Zugriff auf nachrichtendienstliche Daten erteilt werden können. Es geht hierbei insb. um Spezialistinnen und Spezialisten der Eidgenössischen Technischen Hochschulen, des CEA oder des GS-VBS.

Absatz 3

Der Zugriff der Dritten nach den Absätzen 1 und 2 kann auch besonders schützenswerte Personendaten und Personendaten, die auf einem Profiling, einschliesslich eines Profilings mit hohem Risiko, beruhen, umfassen.

Absatz 4

Der Zugriff der Dritten nach den Absätzen 1 und 2 ist zeitlich zu begrenzen und nach der Erledigung des Auftrags, der Beendigung des Projekts oder der Unterstützung des NDB aufzuheben.

Artikel 58g Zugriff auf Daten des Nachrichtenverbunds

Absatz 1

Dieser Absatz entspricht weitgehend dem heutigen Artikel 53 Absatz 3. Angesichts der engen Zusammenarbeit im Sicherheitsbereich soll der Landespolizei Liechtenstein neu ein permanenter Zugriff auf die Daten des Nachrichtenverbunds erteilt werden. Bisher konnte diese nur bei besonderen Ereignissen zugreifen.

Absatz 2

Dieser Absatz entspricht dem heutigen Artikel 53 Absatz 4.

Artikel 58h Zugriff auf administrative Daten

Absätze 1 und 2

Am Zugriff auf die administrativen Daten ändert sich im Vergleich zu heute nichts (vgl. Art. 52 Abs. 3). Für die KND ist der Zugriff auf ihre in Artikel 29 Buchstabe c VIS-NDB ausgewiesene Auftragsverwaltung heute aber nicht explizit geregelt. Daneben wird aus Gründen der Transparenz ausgewiesen, dass die KND auch auf die administrativen Daten des NDB zugreifen können, soweit es zur Erfüllung ihrer administrativen Aufgaben notwendig ist (bspw. zur Verwaltung der Aufträge des NDB).

Absatz 3

Schon heute kann die Qualitätssicherungsstelle, um Stichproben durchzuführen, auf sämtliche Daten der KND zugreifen, also auch auf die administrativen Daten, was neu aus Gründen der Transparenz ausgewiesen wird.

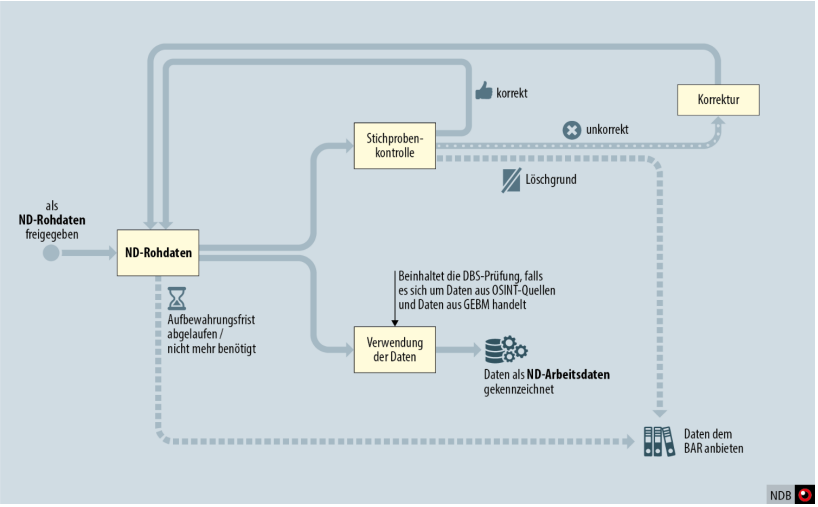
Absatz 4

Der NDB ist für die Erfüllung seiner Aufgaben auf die Zusammenarbeit mit externen Leistungserbringern angewiesen. Dies ist zum einen beim Unterhalt und der Weiterentwicklung seiner Informatikinfrastruktur der Fall. Durch die Komplexität der Software benötigt der NDB oftmals allein für das Finden der Ursachen von Problemen

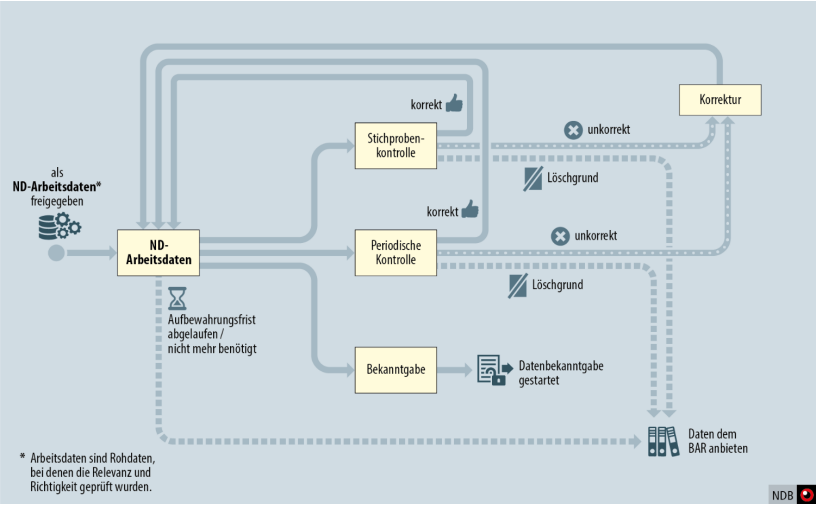
externes Knowhow. Dies gilt umso mehr für die Problembehebung. Wenn beispielsweise eine Mitarbeiterin oder ein Mitarbeiter aus Versehen ein Benutzerkonto löscht, ist nur der externe Leistungserbringer in der Lage, dieses mit allen Daten sowie den verbundenen Aufträgen und Prozessen wiederherzustellen. Die externen Leistungserbringer haben aber nur Zugriff auf die Metadaten, nicht auf die Daten selber. Es geht aber auch um Weiterentwicklungsarbeiten, bei denen externes Fachwissen zwingend notwendig ist und Daten in den betreffenden Projektdossiers bearbeitet werden müssen. Zum anderen lässt der NDB regelmässig im Mandatsverhältnis Texte durch externe Expertinnen und Experten übersetzen. Der Umstand, dass diese heute nicht auf die administrativen Daten zugreifen können, erschwert die Auftragserteilung und -erledigung und gefährdet die Informationssicherheit, indem sie die Aufträge ausserhalb der geschützten Computernetzwerke des NDB erledigen müssen.

7. Abschnitt: Qualitätssicherung

Übersicht Bearbeitung / Qualitätssicherung von Rohdaten



Übersicht Bearbeitung / Qualitätssicherung von Arbeitsdaten



Artikel 58i Nachrichtendienstliche Daten des NDB

Absatz 1

Dieser Absatz entspricht inhaltlich dem heutigen Artikel 45 Absatz 4. Da dieses Gesetz nicht mehr verschiedene Informationssysteme regelt, wird von Arbeitsdaten gesprochen. Der Begriff «strukturierte Erfassung / Erschliessung» führte in der Vergangenheit immer wieder zu Missverständnissen und Diskussionen. Mit der neuen Formulierung soll geklärt werden, worum es geht: Es geht um die Zuordnung von Daten zu Personen oder Organisationen. Daneben wird klargestellt, dass Daten auch anonymisiert statt gelöscht werden können. Gelöscht werden ganze Meldungen/Dateien, die einem Personendatensatz zugeordnet wurden. Anonymisiert wird, wo eine solche Meldung/Datei benötigt wird, weil sie noch weitere NDG-relevante Informationen enthält und bspw. einer oder mehreren weiteren Personen oder Organisationen zugeordnet ist.

Absatz 2

Dieser Absatz entspricht inhaltlich dem letzten Satz des heutigen Artikels 45 Absatz 4. Selbstverständlich werden die ausdrücklich als falsch gekennzeichneten Daten (vgl. Art. 51 Abs. 2) im Rahmen der periodischen Überprüfung nicht korrigiert. Daneben wurde der Verweis auf den Vorbehalt angepasst.

Absatz 3

Dieser Absatz entspricht weitgehend dem heutigen Artikel 45 Absatz 5.

Es entspricht bereits der heutigen Praxis, dass die Leitung der Qualitätssicherungsstelle direkt der Direktorin oder dem Direktor des NDB berichten kann, was nun ausdrücklich geregelt wird. Damit wird der Hierarchiestufe zwischen der Qualitätssicherungsstelle und der Direktorin oder dem Direktor nun ausdrücklich untersagt, es der Qualitätssicherungsstelle zu verbieten, direkt dem Direktor zu rapportieren oder auf die Rapportierung Einfluss zu nehmen.

Der heutige Buchstabe b, der eine periodische Überprüfung der Berichte der KND durch die Qualitätssicherungsstelle des NDB vorsah, wurde ersatzlos gestrichen, da es keinen Grund gibt, weshalb diese Daten speziell behandelt werden sollten. Auch diese Daten können die zuständigen Fachspezialisten periodisch prüfen, wie das der neue Artikel 58*i* Absatz 1 für alle Arbeitsdaten vorschreibt, die der NDB in Erfüllung seiner Aufgaben nach Artikel 6 Absatz 1 einer Person oder Organisation zugeordnet hat.

Heute ist es den KND untersagt, selbst Daten zu löschen (vgl. Art. 45 Abs. 5 Bst. d NDG). Auch hierfür gibt es aber keinen plausiblen Grund mehr. Vielmehr führte diese Vorschrift zu einem komplizierten Löschmechanismus, der unnötig Ressourcen seitens der KND und der Qualitätssicherungsstelle des NDB bindet. Dieser Buchstabe wird deshalb ebenfalls ersatzlos gestrichen. Die KND sollen inskünftig (wie vor dem Inkrafttreten des NDG) ihre Daten wieder selber löschen können, wenn sie diese nicht mehr benötigen oder wenn deren Aufbewahrungsfrist abgelaufen ist.

Daneben wird durch das Wort «insbesondere» klargestellt, dass diese Aufzählung nicht abschliessend ist und die Qualitätssicherungsstelle des NDB auch noch andere Aufgaben wahrnimmt.

Buchstabe a

Dieser Buchstabe entspricht inhaltlich dem heutigen Artikel 45 Absatz 5 Buchstabe a. Wie heute, sollen auch in Zukunft die Daten im Bereich des gewalttätigen Extremismus (erkenntlich durch ihre Unterkategorisierung; vgl. dazu die Ausführungen oben zu Art. 49) verstärkt und zu einem frühen Zeitpunkt überprüft werden. Heute geschieht das gleich nachdem die Daten strukturiert erfasst / erschlossen wurden. Inskünftig wird von der Zuordnung von Daten zu Personen und Organisationen gesprochen. Der Zeitpunkt der Überprüfung bleibt aber der gleiche. Der Begriff «Erheblichkeit» wird im vorliegenden Entwurf systematisch durch «Aufgabenbezug» ersetzt. Neu wird klargestellt, dass auch die Einhaltung der Datenbearbeitungsschranke geprüft wird.

Buchstabe b

Dieser Buchstabe entspricht inhaltlich dem heutigen Artikel 45 Absatz 5 Buchstabe c. Da das Gesetz neu nicht mehr verschiedene Informationssysteme regelt, bezieht sich die Stichprobentätigkeit der Qualitätssicherungsstelle nicht auf die einzelnen Informationssysteme, sondern auf sämtliche nachrichtendienstliche Daten des NDB (Rohdaten und Arbeitsdaten). Die Begriffe «Wirksamkeit» und «Zweckmässigkeit» werden im Gegensatz zum geltenden NDG nicht mehr verwendet, da sie im Datenschutzrecht nicht vorkommen. Wird statt der Wirksamkeit und Zweckmässigkeit die Verhältnismässigkeit geprüft, wird die Qualitätskontrolle ausgebaut, denn es kommen nebst der Eignung die Aspekte der Notwendigkeit und Zumutbarkeit hinzu.

Die Stichprobenkontrollen der nachrichtendienstlichen Daten der KND regelt Artikel 58*j* Absatz 1 E-NDG.

Buchstabe c

Neu wird die Datenschutzberaterin bzw. der Datenschutzberater des NDB in die Pflicht genommen, Schulungen zur Einhaltung der Vorgaben der Datenbearbeitung nach dem NDG durchzuführen. Es wird zudem klargestellt, dass auch die Mitarbeiterinnen und Mitarbeiter der KND geschult werden.

Buchstabe d

Wie bereits zu Artikel 53 E-NDG erwähnt, ist der Einsatz von lernfähigen Programmen zur Suche und Kategorisierung von Informationen heute für die effiziente Aufgabenerfüllung des NDB unabdingbar und wird auch von Aufsichtsgremien gefordert. Es handelt sich zwar nicht um künstliche Intelligenz im Sinne automatisierter Einzelentscheidungen (Art. 21 DSG). Trotzdem wird im Sinne der «Leitlinien ‹Künstliche Intelligenz› für den Bund», die der Bundesrat am 25. November 2020[42] verabschiedet hat, der Einsatz solcher KI-ähnlichen Werkzeuge transparent gemacht und eine Überwachung der Nutzung während des ganzen Lebenszyklus (vom Erwerb bis zur Deaktivierung) eingeführt.

Artikel 58j Nachrichtendienstliche Personendaten der kantonalen Vollzugsbehörden

Absatz 1

Die stichprobenweise Überprüfung der Bearbeitung der nachrichtendienstlichen Daten der KND ist nicht neu, war aber bisher nicht explizit geregelt (vgl. den heutigen Art. 45 Abs. 5 Bst. c, in dem nur von «allen Informationssystemen» gesprochen wird). Zum Begriff der Verhältnismässigkeit sei auf die Ausführungen oben zu Artikel 58*b* Absatz 3 Buchstabe b verwiesen. Die KND werden auch weiterhin ihre nachrichtendienstlichen Personendaten nicht periodisch prüfen, da diese bereits nach fünf Jahren automatisiert gelöscht werden (vgl. Art. 58*a*). Die Löschung ersetzt somit die periodische Überprüfung.

Absatz 2

Auch die Rückweisung der Berichte der KND, die ganz oder teilweise keinen Aufgabenbezug aufweisen oder die Datenbearbeitungsschranke verletzen, ist heute nicht explizit im NDG geregelt (wohl aber in Art. 3 Abs. 3 und Art. 4 Abs. 2 VIS-NDB, welche diese Pflicht schon heute vorschreiben). Aus Gründen der Transparenz und weil in diesen Fällen die Datenbearbeitung des KND korrigiert werden muss, wird dies nun explizit geregelt. Diese Vorgehensweise entspricht der heutigen Praxis.

42 Leitlinien «Künstliche Intelligenz» für den Bund vom 25. November 2020. Abrufbar unter: www.sbfi.admin.ch > BFI-Politik > BFI-Politik 2025-2028 > Transversale Themen > Digitalisierung > Künstliche Intelligenz im BFI-Bereich.

4a. Kapitel: Besondere Bestimmungen über den Datenschutz

Der heutige 4. Abschnitt des 4. Kapitels wird mit der neuen Struktur zum 4*a*. Kapitel.

1. Abschnitt: Bekanntgabe von Personendaten

Wie bereits eingangs des 4. Kapitels erwähnt, dürfen Rohdaten mit wenigen Ausnahmen nicht verwendet bzw. bekannt gegeben werden. Im vorliegenden Kapitel geht es somit grundsätzlich um Arbeitsdaten, die bereits vertieft geprüft wurden (vgl. aber die Ausnahmen von Art. 5 Abs. 6 und 46 Abs. 2). Die Bekanntgabe von Personendaten durch die KND wird in Artikel 58 geregelt.

Artikel 59 Überprüfung von Personendaten vor der Bekanntgabe

Dieser Artikel entspricht weitgehend dem heutigen Artikel 59. Inhaltlich ändert sich nichts an dieser Bestimmung. Zum besseren Verständnis wird in der Sachüberschrift ausgeführt, dass es um die Überprüfung von Personendaten geht. Da es auch bei den nachrichtendienstlichen Produkten um Personendaten geht, wurde dieser Begriff gestrichen. Zudem wird klargestellt, dass mit Personendaten auch besonders schützenswerte Personendaten und Daten, die auf einem Profiling, einschliesslich eines Profilings mit hohem Risiko, beruhen, gemeint sind. Da die Bekanntgabe allen anwendbaren rechtlichen Vorgaben, nicht nur jenen des NDG genügen muss, wurde deren explizite Erwähnung gestrichen.

Artikel 60

Dieser Artikel entspricht weitgehend dem heutigen Artikel 60. Für die KND gelten die Einschränkungen von Artikel 58 Absatz 3.

Absatz 1

Auch in diesem Absatz wird klargestellt, dass mit Personendaten auch besonders schützenswerte Personendaten und Daten, die auf einem Profiling, einschliesslich eines Profilings mit hohem Risiko, beruhen, gemeint sind. Solche Daten können auch im Rahmen der Beauftragung eines KND oder einer Observationseinheit einer Kantonspolizei bekannt gegeben werden oder um ein Auskunftsbegehren zu stellen. An der Delegation der Rechtsetzungsbefugnisse an den Bundesrat ändert sich nichts.

Absatz 3

Im Einklang mit dem ganzen Konzept der Datenhaltung wird in diesem Absatz lediglich der Begriff «Daten» durch «Personendaten» ersetzt.

Artikel 61

Absatz 1

Auch in diesem Absatz wird klargestellt, dass mit Personendaten auch besonders schützenswerte Personendaten und Daten, die auf einem Profiling, einschliesslich eines Profilings mit hohem Risiko, beruhen, gemeint sind. Da es aus datenschutzrechtlicher Sicht keinen Unterschied ausmacht, ob Personendaten auf einer Liste stehen,

wurde der Hinweis auf diese gestrichen. Wichtig ist lediglich, dass bei jedem bekannt zu gebenden Personendatum sichergestellt ist, dass die rechtlichen Voraussetzungen für die Bekanntgabe erfüllt sind.

Artikel 62

Auch in diesem Artikel wird klargestellt, dass mit Personendaten auch besonders schützenswerte Personendaten und Daten, die auf einem Profiling, einschliesslich eines Profilings mit hohem Risiko, beruhen, gemeint sind.

Buchstabe a

Der Begriff «Weitergabe» wird durch den vom DSG verwendeten Begriff «Bekanntgabe» ersetzt. Dies führt inhaltlich zu keiner Änderung.

Buchstabe b

Hier wird der Begriff «Gefährdung» durch den ansonsten in diesem Gesetz verwendeten Begriff «Bedrohungen» ersetzt (vgl. Art. 6 Abs. 1 Bst. a). Inhaltlich erfolgt keine Änderung.

Buchstabe c

Hier wird der Begriff «Auskunftsgesuch» durch «Auskunftsbegehren» ersetzt. Dies zur Verdeutlichung, dass es nicht um ein Auskunftsgesuch nach den Artikeln 63 und 63*a* E-NDG geht, sondern um ein Begehren des NDB oder eines KND um Auskunft. Unter diese Bestimmung ist auch die Informationsweitergabe an Quellen oder im Rahmen von Befragungen zu subsumieren. Inhaltlich gibt es keine Änderungen.

Buchstabe d

Hier erfolgt der Bezug auf die Bekanntgabe an Dritte im Rahmen von Artikel 45 Absatz 4 E-NDG.

2. Abschnitt: Auskunftsrecht

Die heutige Regelung des Auskunftsrechts ist kompliziert und soll auch zugunsten der Gesuchstellerinnen und Gesuchsteller vereinfacht werden.

Für administrative Daten soll nach wie vor das DSG uneingeschränkt zur Anwendung kommen. Für nachrichtendienstliche Daten gilt ebenfalls grundsätzlich das DSG. Der NDB hat aber im Vergleich zum DSG weiterhin die Möglichkeit, die Auskunft ohne Verfügung aufzuschieben. Diese Möglichkeit gilt weiterhin auch bei Nichtverzeichnung der Gesuchstellerin oder des Gesuchstellers. Allerdings wird neu klargestellt, dass hier nicht automatisch ein Aufschub erfolgen muss, sondern dass eine Einzelfallprüfung erfolgt, die im Normalfall zur Auskunft führt. Die Gesuchstellerin oder der Gesuchsteller kann wie bisher bei einem Aufschub die Prüfung durch den EDÖB verlangen.

Artikel 63 Grundsatz

In diesem Artikel wird festgehalten, dass für das Auskunftsrecht sowohl zu nachrichtendienstlichen als auch zu administrativen Daten grundsätzlich das DSG gilt. Ausnahmen davon finden sich in Artikel 63*a* Absatz 5 E-NDG (summarische Auskunft) und in den Artikeln 63*b*–65 E-NDG (Prüfung durch den EDÖB, Mitteilung des EDÖB und Prüfung durch das Bundesverwaltungsgericht). Das Auskunftsrecht betrifft nebst den administrativen Daten sämtliche nachrichtendienstlichen Daten (auch die gesondert abgespeicherten nachrichtendienstlichen Daten).

Artikel 63a Auskunftsrecht betreffend nachrichtendienstliche Personendaten

Absatz 1

Der NDB erteilt der Gesuchstellerin oder dem Gesuchsteller diejenigen Informationen, die erforderlich sind, damit diese oder dieser ihre Rechte nach dem DSG geltend machen kann. Dies geschieht grundsätzlich durch die Bekanntgabe von Personendaten «als solche», kann aber auch durch die Herausgabe von Kopien geschehen, wenn dies aus Gründen der Effizienz (bspw. bei einem Protokoll einer Ansprache der betreffenden Person durch den NDB) oder für die Gewährleistung einer transparenten Datenbearbeitung erforderlich ist.

Absatz 2

Der NDB kann die Auskunft aus den in Artikel 26 DSG vorgesehenen Gründen verweigern oder einschränken. Tut er dies, so hat er eine anfechtbare Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968[43] (VwVG) zu erlassen. Die Pflicht, eine begründete Verfügung zu erlassen, ergibt sich materiell schon aus Artikel 26 Absatz 4 DSG sowie aus dem Umkehrschluss zu Artikel 66 des Revisionsentwurfs.

Absatz 3

Der NDB hat weiterhin die Möglichkeit, eine Auskunft aufzuschieben. Nebst den in Artikel 26 DSG aufgezählten Gründen hat er nach wie vor die Möglichkeit, die Auskunft auch dann aufzuschieben, wenn er über die Gesuchstellerin oder den Gesuchsteller keine Daten bearbeitet. Im Gegensatz zu heute ist diese Bestimmung aber in der Möglichkeitsform geschrieben und soll nur in Ausnahmefällen zum Einsatz kommen. Das heisst, der NDB kann einer bei ihm nicht verzeichneten Person auch sofort Auskunft über deren Nichtverzeichnung geben und muss diese nicht drei Jahre lang im Ungewissen lassen oder er kann in unbedenklichen Fällen von sich aus die Nichtverzeichnung mitteilen und nicht erst nach der Feststellung des EDÖB, dass der Person sonst ein erheblicher, nicht wiedergutzumachender Schaden erwächst. Diese Praxis verfolgt der NDB schon heute weitgehend, weil der EDÖB in zahlreichen solchen Fällen empfahl, Auskunft zu erteilen.

Absatz 4

43 SR **172.021**

Dieser Absatz entspricht weitgehend dem heutigen Artikel 63 Absatz 4. Während der Aufschub selber nicht anfechtbar ist, erfolgt die Auskunft nach dem Wegfallen des Geheimhaltungsinteresses nach dem DSG, das heisst, in Form einer anfechtbaren Verfügung im Sinne von Artikel 5 VwVG.

Absatz 5

Heute ist nicht geregelt, was passiert, wenn die Auskunftserteilung mit unverhältnismässigem Aufwand verbunden ist. Neu ist deshalb vorgesehen, dass der NDB diesfalls bezüglich Daten, welche die Gesuchstellerin oder der Gesuchsteller selbst veröffentlicht oder dem NDB selbst eingereicht hat, summarisch Auskunft geben darf, unter Angabe des Zeitraums und Zusammenhangs, in dem die Daten bearbeitet wurden, der Zugriffsberechtigten und derjenigen Stellen, denen die Daten bekannt gegeben wurden (bspw. wenn ein Journalist wöchentlich Beiträge zur inneren oder äusseren Sicherheit publiziert, sollen ihm diese nicht in Kopie zugestellt werden müssen, sondern es soll genügen, dass der NDB ihm mitteilt, wie viele Beiträge er abgespeichert hat und aus welchem Zeitraum diese stammen). Eine summarische Auskunft kann auch in einer stichwortartigen Auflistung veröffentlichter oder dem NDB eingereichter Dokumente bestehen (bspw. Nennung der Titel der Dokumente, mit Angabe des Zeitraums etc.). Die Erfahrungen bei der Bearbeitung von Auskunftsgesuchen der letzten Jahre haben gezeigt, dass ein unverhältnismässiger Aufwand bei der Auskunftserteilung nur in ganz seltenen Ausnahmekonstellationen gegeben sein kann (bspw. wenn sich eine Person über Jahrzehnte für Belange der inneren oder äusseren Sicherheit einsetzte, in diesem Zusammenhang zahlreiche Publikationen und veröffentlichte Einschätzungen vornahm und von in- und ausländischen Medien umfangreich im Zusammenhang mit verschiedenen Ereignissen zitiert wurde oder wenn eine Person über mehrere Jahre hinweg in Ausübung ihres behördlichen Auftrags mehrmals wöchentlich Eingaben an den NDB richtete).

Absatz 6

Dieser Absatz entspricht dem heutigen Artikel 63 Absatz 5.

Artikel 63b Prüfung durch den EDÖB

Absatz 1

Dieser Absatz entspricht weitgehend dem heutigen Artikel 63 Absatz 3. Statt von Geheimhaltungsinteressen, welche den Aufschub rechtfertigen, wird neu von der Rechtfertigung des Aufschubs gesprochen.

Absatz 2

Dieser Absatz entspricht dem heutigen Artikel 64 Absatz 5. Zur Vereinheitlichung der Terminologie wird auch in diesem Absatz der Begriff «Gefährdung» durch den Begriff «Bedrohung» ersetzt. Es ist klar, dass der EDÖB die Abklärung nur machen kann, wenn ihm der Sachverhalt bekannt gegeben wird, dem die Geheimhaltung zugrunde liegt. Deshalb sind die Aufschübe des NDB gegenüber dem Beauftragten zu begründen.

Artikel 64 Mitteilung des EDÖB

Absatz 1

Der heutige Artikel 64 Absatz 1 wurde redundant (vgl. Art. 63*b* Abs. 1).

Der neue Absatz 1 entspricht dem heutigen Artikel 64 Absatz 2. Es entspricht der Konzeption des DSG, dass der EDÖB dazu befugt ist, eine Untersuchung zu eröffnen, wenn er Unregelmässigkeiten feststellt, was hier nachgetragen wird.

Absatz 2

Logischerweise wird die Gesuchstellerin oder der Gesuchsteller in Abweichung von Artikel 49 Absatz 4 DSG nicht über das Ergebnis der Untersuchung informiert. Da die Mitteilung nach Artikel 64 Absatz 1 E-NDG diejenige nach Artikel 49 Absatz 4 DSG ersetzt, beschränkt sich der Inhalt der Mitteilung des EDÖB auf das in Artikel 64 Absatz 1 Aufgeführte (der EDÖB informiert weder über die Eröffnung noch über das Ergebnis einer allfälligen Untersuchung, damit die die Gesuchstellerin oder der Gesuchsteller nicht in Erfahrung bringen kann, ob der NDB über sie Daten bearbeitet).

Absatz 3

Im Vorentwurf zu dieser Revision war noch die Prüfung durch das Bundesverwaltungsgericht enthalten, was dem damals geltenden NDG entsprach. Da im Rahmen der Totalrevision des DSG diese Prüfung im NDG aufgehoben wurde, hatte der NDB dies auch im vorliegenden Revisionsentwurf geändert.

Die externe Konsultation ergab jedoch, dass die Aufhebung der Prüfung durch das Bundesverwaltungsgericht zu einer Lücke im Rechtsschutz führte. Der NDB entschied sich deshalb, die Prüfung durch das Bundesverwaltungsgericht wieder in den Entwurf aufzunehmen.

Dieser Absatz entspricht nun wieder dem aktuellen Artikel 64 Absatz 3. Neu hat das Bundesverwaltungsgericht den Aufschub der Auskunft (früher Mitteilung genannt) und die Datenbearbeitung zu überprüfen. Da es keine Empfehlungen mehr gibt, wurde dieser Begriff gestrichen.

Absatz 4

Mit dem DSG erhält der EDÖB, wie bereits erwähnt, neu die Kompetenz, Verfügungen zu erlassen. Die heutigen Empfehlungen (vgl. den heutigen Art. 64 Abs. 2) werden abgeschafft. Der Inhalt des heutigen Absatz 4 ist damit obsolet geworden.

Artikel 65 Prüfung durch das Bundesverwaltungsgericht

Zur Wiedereinführung der Prüfung durch das Bundesverwaltungsgericht vgl. die Ausführungen oben zu Artikel 64 Absatz 3.

Absatz 1

Diese Bestimmung entspricht dem mit der Totalrevision des DSG aufgehobenen Artikel 65 Absatz 1.

Absatz 2

Dieser Absatz entspricht dem mit der Totalrevision des DSG aufgehobenen Artikel 65 Absatz 2. Da der EDÖB keine Empfehlungen mehr ausspricht, wurden die diesbezüglichen Ausführungen gestrichen.

Artikel 66

Absatz 1

Dieser Artikel entspricht mit angepassten Verweisen dem heutigen Artikel 66 Absatz 1.

Artikel 66a Besondere Bestimmungen zum Auskunftsrecht

Nach Artikel 46 Absatz 2 E-NDG erfolgt die Prüfung der Anwendung von Artikel 5 Absatz 5 bei Personendaten aus öffentlich zugänglichen Quellen und bei gesondert abgespeicherten Personendaten aus GEBM erst, wenn der NDB diese als Arbeitsdaten verwenden will. Da die Bekanntgabe von Daten an die Gesuchstellerin oder den Gesuchsteller ebenfalls unter den Begriff der Verwendung zu subsumieren ist, muss der NDB diese Prüfung durchführen, bevor er eine Auskunft an die Gesuchstellerin oder den Gesuchsteller richtet.

3. Abschnitt: Archivierung

Der heutige 5. Abschnitt des 4. Kapitels wird mit der neuen Struktur zum 3. Abschnitt.

Artikel 68

Dieser Artikel entspricht weitgehend dem heutigen Artikel 68. Die Archivierungsregeln betreffend die AB-ND sind neu in Artikel 78*e* geregelt.

Absatz 1

In diesem Gesetz und nachfolgend in den Vollzugsverordnungen wird zwischen «Löschen» und «Vernichten» unterschieden. Zur Löschung bestimmte Daten bietet der NDB dem BAR zur Archivierung an. Als nicht archivwürdig bewertete Daten und solche, die dem BAR bereits abgeliefert wurden, vernichtet er. In Absatz 1 geht es um die Archivierung von Daten, die der NDB nicht mehr ständig benötigt. Deshalb geht es in dieser Phase um die «Löschung» und nicht um die «Vernichtung» von Daten. Von den Daten sind nur die Findmittel im System des BAR abgespeichert. Die Daten selber sind auf von diesen unabhängigen Festplatten abgespeichert.

Absatz 4

Hier wird klargestellt, dass der NDB Daten, welche das BAR als nicht archivwürdig beurteilt, gleich nach deren Löschung vernichtet, auch wenn deren Aufbewahrungsfrist noch nicht abgelaufen ist. Dies entspricht dem datenschutzrechtlichen Grundsatz, wonach Daten nur so lange bearbeitet werden dürfen, wie dies zur Aufgabenerfüllung notwendig ist (auch die Aufbewahrung bereits gelöschter Daten stellt eine Datenbearbeitung dar).

Artikel 70

Absatz 1 Buchstabe c

Der Buchstabe c des heutigen Artikels 70 Absatz 1 soll gestrichen werden. Einerseits erhält der NDB nach dem revidierten Artikel 27 inskünftig die Berechtigung, auch gegen gewalttätig-extremistische Personen und Gruppierungen GEBM durchzuführen, was die durch den Bundesrat vorzunehmende Abgrenzung solcher Personen und Gruppierungen überflüssig macht. Andererseits gibt es nach der neuen Datenbearbeitungskonzeption inskünftig kein separates Informationssystem IASA-GEX mehr, in dem die Daten zu gewalttätig-extremistischen Personen und Gruppierungen getrennt von den übrigen nachrichtendienstlichen Daten bearbeitet werden.

Absatz 1 Buchstabe d

Buchstabe d des heutigen Artikels 70 Absatz 1 soll ebenfalls gestrichen werden, um Doppelspurigkeiten zu vermeiden. Eine jährliche sicherheitspolitische Lagebeurteilung ist heute nicht mehr notwendig, da der Bundesrat mit dem neu alle vier Jahre erscheinenden Sicherheitspolitischen Bericht weit umfassender über die sicherheitspolitische Lagebeurteilung informiert. Die politische Führung des Nachrichtendienstes ist mit den restlichen Bestimmungen des Artikels hinreichend abgedeckt. Die nachrichtendienstlich-sicherheitspolitische Berichterstattung des VBS an die zuständigen parlamentarischen Kommissionen ist durch die Streichung nicht betroffen (Art. 80). Sie wird gemäss den Bedürfnissen des Parlaments weitergeführt.

Mit der Streichung wird auch ein gewisser Widerspruch zu Absatz 2 beseitigt, gemäss dem die Dokumente in Zusammenhang mit den Aufgaben nach Absatz 1 nicht öffentlich zugänglich sind. Mit dem jährlichen Lagebericht des NDB, der die wichtigsten Lageentwicklungen aus nachrichtendienstlicher Sicht vorstellt, wird die Öffentlichkeit ohnehin über die Lagebeurteilung informiert.

Absatz 3

Die schon heute bestehende Berechtigung des Bundesrates, selbstständig völkerrechtliche Verträge im Bereich des Nachrichtendienstes abschliessen zu können, soll inhaltlich um die Bereiche Informationsbeschaffung und Ausbildung erweitert werden. Dabei kann es sich um Verträge handeln, die nach Artikel 13 Absatz 3 ISG als geheim zu klassifizieren sind. Derzeit besteht ein Trend hin zu einer gewissen Formalisierung der internationalen nachrichtendienstlichen Zusammenarbeit. Es wird jedoch auf absehbare Zeit hin kaum ein anderer Staat bereit sein, in diesem Bereich öffentlich zugängliche Verträge abzuschliessen.

Im neuen ISG ist die allgemeine Berechtigung des Bundesrates für den Abschluss von völkerrechtlichen Verträgen über die Informationssicherheit (Art. 87 ISG, in Kraft seit dem 1. Mai 2022) vorgesehen. Um Unklarheiten zu vermeiden, wird diese Zuständigkeit im NDG zusammen mit den anderen Bereichen, in denen der Bundesrat selbstständig Verträge zur nachrichtendienstlichen Zusammenarbeit abschliessen kann, auch weiterhin erwähnt.

Der Bundesrat erstattet der Bundesversammlung jährlich Bericht über die von ihm selbstständig abgeschlossenen völkerrechtlichen Verträge. Von vertraulichen oder geheimen Verträgen im Bereich des Nachrichtendienstes erhält hingegen nur die GPDel

Kenntnis (Art. 48*a* Abs. 2 RVOG). Darüber hinaus können die nachrichtendienstlichen Aufsichtsorgane AB-ND und GPDel selbstverständlich auch gestützt auf ihre Aufsichtsrechte weiterhin auf Anfrage das volle Einsichtsrecht in diese Dokumente erhalten. Kontrolle und Aufsicht sind damit gewährleistet.

Artikel 74

Die hier aufgehobenen Absätze werden in den neuen Abschnitt über Strafbestimmungen integriert, der vor den Schlussbestimmungen eingefügt wurde. Somit werden sämtliche Strafbestimmungen wie üblich am Ende des Gesetzestextes geregelt (hinsichtlich Nummerierung der Absätze siehe die Erläuterung zu Art. 83*a*).

2. Abschnitt:

Während der parlamentarischen Beratung haben die zuständigen Kommissionen und der Bundesrat vereinbart, in einem ersten Schritt die mit diesem Gesetz neu geschaffene AB-ND zu entwickeln und die schon bestehende UKI ihre Kontrollen weiter ausüben zu lassen und auf die Kabelaufklärung zu erweitern. So sollte die Aufsicht aufrechterhalten und sogar gestärkt werden. Die beiden Aufsichtsorgane arbeiten heute dementsprechend zusammen und koordinieren ihre Tätigkeiten, um Lücken in der Aufsicht zu verhindern.

In einem zweiten Schritt sollte eine Zusammenführung der Aufgaben der beiden Instanzen inklusive Übertragung der entsprechenden Kenntnisse überprüft werden. So würde unter anderem die Koordination der Tätigkeiten wegfallen und die parlamentarische Oberaufsicht und der NDB nur noch einen Ansprechpartner haben, der aber die gleiche Kontrolle ausübt. Die Unabhängigkeit der Aufsichtsbehörde bliebe dabei gewährleistet.

Die Aufgaben der UKI sollen nach Abwägung der Vor- und Nachteile neu vollumfänglich an die AB-ND übertragen werden. Die AB-ND verfügt heute schon über umfassende Aufsichtskompetenzen und überprüft die nachrichtendienstlichen Tätigkeiten des NDB, der KND sowie der vom NDB beauftragten Dritten und anderen Stellen auf ihre Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit.

Die UKI prüft spezifisch die Funkaufklärung auf Rechtmässigkeit und beaufsichtigt den Vollzug der genehmigten und freigegebenen Aufträge zur Kabelaufklärung. Zur Erfüllung ihrer Aufsichtstätigkeit haben beide Instanzen Zugang zu allen sachdienlichen Informationen und Unterlagen sowie Zutritt zu allen Räumlichkeiten der beaufsichtigten Stellen und können Empfehlungen aussprechen. Die AB-ND und die UKI arbeiten regelmässig zusammen.

Da die Aufsichtskompetenzen der AB-ND grundsätzlich auch jene der UKI abdecken, ist es sinnvoll, die Aufsichtstätigkeiten dieser beiden unabhängigen Stellen in einer einzigen Behörde zusammenzuführen, die bereits eine breite Übersicht über die nachrichtendienstlichen Tätigkeiten hat. Dadurch kann sichergestellt werden, dass die Überprüfung der Funk- und Kabelaufklärung weiterhin effizient und umfassend erfolgt. Deswegen wird der heutige Artikel 79 hinfällig und wird aufgehoben.

Darüber hinaus garantiert das umfassendere Aufsichtsmandat der AB-ND auch eine umfassendere Aufsicht, die sich nicht nur auf die Rechtmässigkeit der nachrichtendienstlichen Tätigkeiten, sondern auch auf deren Zweckmässigkeit und Wirksamkeit erstreckt. Schliesslich ermöglicht die Aufgabenübertragung auch die Schaffung von Synergien: Die AB-ND befasst sich exklusiv mit der Überprüfung der nachrichtendienstlichen Tätigkeiten. Die Mitglieder der UKI arbeiten hingegen im Milizsystem. Mit den raschen technischen Entwicklungen und den daraus folgenden komplexen Fragestellungen für die Abläufe im Tagesgeschäft wird es für diese Instanz zunehmend schwierig, mit verhältnismässigem Aufwand auf dem für die Überprüfungen nötigen Wissensstand zu bleiben. Die AB-ND ist aufgrund ihrer anderen Aufgaben gefordert, sich dieses Wissen sowieso anzueignen. Bereits heute hat sie in ihrem Personalbestand entsprechende Fachleute. Durch die vorhandenen Synergien kann die Qualität der Aufsicht weiterhin gewährleistet und mit verhältnismässigem Aufwand an die Entwicklungen angepasst werden. Mit dem Wegfall einer Aufsichtsinstanz reduziert sich der Koordinationsaufwand, ohne dass die Resultate der Überprüfungen an Qualität einbüssen würden. Durch die Bündelung der (Aufsichts-) Kräfte findet eine umfassende Kontrolle aus einer Hand statt. Mit dem Aufgaben- und Wissenstransfer von der UKI zur AB-ND kann die vom Parlament 2015 im Rahmen der Debatte zum NDG in Erwägung gezogene Lösung realisiert werden.

Diese Revision ist auch eine Gelegenheit, das Gesetz insbesondere durch eine Vereinfachung der Struktur leichter lesbar zu machen. Aus diesem Grund wird vorgeschlagen, Artikel 78 unter Berücksichtigung der verschiedenen Aufgaben, welche die AB-ND nach dem Gesetz zu erfüllen hat, nämlich Aufsicht, Koordination sowie Information der Öffentlichkeit, in vier separate Bestimmungen aufzuteilen. Ebenfalls im Sinne der besseren Lesbarkeit und da das VBS für die Umsetzung der Empfehlungen der AB-ND verantwortlich ist, wird dieser Punkt nun Gegenstand einer eigenen Bestimmung.

Artikel 75 Selbstkontrolle des NDB

In diesem Gesetz wird ansonsten der Ausdruck «kantonale Vollzugsbehörden» verwendet, was in diesem Artikel korrigiert wird.

Artikel 76 Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten

Sachüberschrift und Absätze 1 und 2

Die Artikel 76–78 zur AB-ND wurden in der parlamentarischen Phase eingeführt. Der Gesetzesentwurf des Bundesrates hatte eine Aufsicht in dieser Form nicht vorgesehen. Aufgrund der späten Einführung sind einige Begriffe und Konzepte im geltenden NDG systematisch nicht korrekt. So wird hier präzisiert, dass die geschaffene AB-ND nicht «Aufsichtsbehörde über den NDB» heisst, sondern «Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten», entsprechend der heutigen Praxis und wie im geltenden Artikel 78 Absatz 1 geregelt. Zudem wird hier die bereits in der VAND verwendete Abkürzung «AB-ND» eingeführt, die neu im ganzen Gesetzestext anstelle von «unabhängige Aufsichtsbehörde» verwendet wird.

Artikel 77

Absatz 2

Da hierfür grundsätzlich eine formell-gesetzliche Grundlage erforderlich ist, wird das bisher erst in Artikel 4 VAND geregelte Vorgehen zur Einreichung des jährlichen Budgetentwurfs der AB-ND an den Bundesrat via das VBS und dessen unveränderte Weiterleitung an die Bundesversammlung nun in Artikel 77 Absatz 2 integriert.

Absatz 3bis

Dieser Absatz übernimmt den Inhalt des zweiten Satzes des geltenden Absatzes 2 und präzisiert, dass die AB-ND ihr Personal selbst anstellt.

Artikel 78 Aufgabe der AB-ND

Diese Bestimmung gibt die Absätze 1 und 2 des geltenden Artikels 78 mit punktuellen redaktionellen Anpassungen wieder (neue Abs. 1 und 2) und konzentriert sich damit auf die Aufgaben der AB-ND, die beaufsichtigten Stellen und die Koordination mit den Tätigkeiten der anderen Aufsichtsstellen des Bundes und der Kantone.

Artikel 78a Befugnisse der AB-ND

Absätze 1 und 2

Diese Absätze übernehmen den Inhalt des geltenden Artikels 78 Absatz 4.

Absatz 3

Um die Erfüllung ihrer Aufgaben insbesondere bei der Aufsicht über die Kabelaufklärung zu gewährleisten (Übernahme der Aufsichtstätigkeiten der UKI, Art. 79 Abs. 2 NDG), wird im neuen Absatz 3 präzisiert, dass die AB-ND die Mitwirkung der Anbieterinnen von Post- und Fernmeldediensten und den Zutritt zu deren Räumlichkeiten verlangen kann.

Absatz 4

Die Begriffe zur Datenhaltung in Absatz 4, der den geltenden Artikel 78 Absatz 5 erster und dritter Satz übernimmt, werden dem neuen Datenhaltungskonzept und dem DSG angepasst. Dies führt inhaltlich zu keiner Änderung. Neu wird präzisiert, dass der Zugriff auf Daten der beaufsichtigten Stellen auch mittels Abrufverfahren (Online-Zugriff) erfolgen kann.

Absatz 5

Absatz 5 erwähnt neu ausdrücklich die Kompetenz der AB-ND, Personendaten aller Art zu bearbeiten. Diese Kompetenz besteht heute bereits, da der geltende Artikel 78 Absatz 5 die AB-ND ermächtigt, auf sämtliche Daten der beaufsichtigten Stellen zuzugreifen und die erhobenen Daten zu speichern. Dieser neue Absatz bringt das Gesetz in Einklang mit dem DSG, insbesondere mit dessen Artikel 34.

Die von der AB-ND bearbeiteten Daten können in die folgenden drei Kategorien unterteilt werden:

- Daten der beaufsichtigen Stellen: diese werden nach Absatz 6 nur solange aufbewahrt, wie es der Bearbeitungszweck erfordert.
- Verwaltungsdaten: Daten und Unterlagen, die für die Erfüllung der administrativen Aufgaben der AB-ND notwendig sind.
- Aufsichtsdaten: alle Daten und Unterlagen, welche die AB-ND selber erstellt, wie z. B. Korrespondenz zu Prüfungen, Protokolle der Anhörungen, Prüfberichte usw. Diese Daten sind sensitiv und erfordern einen besonderen Schutz bei der Bearbeitung und Archivierung (vgl. Art. 78*e* E-NDG und die entsprechenden Erläuterungen).

Absatz 6

Absatz 6 übernimmt die Regelung des geltenden Artikels 78 Absatz 5 zweiter Satz. Zudem präzisiert er, dass Unterlagen und Daten der beaufsichtigten Stellen vernichtet bzw. gelöscht werden, nachdem der Bearbeitungszweck erfüllt ist.

Artikel 78b Resultat der Prüfungen und Umsetzung der Empfehlungen

Diese Bestimmung enthält die Absätze 6 und 7 des geltenden Artikels 78. Sie konzentriert sich auf die Form des Resultats der von der AB-ND durchgeführten Prüfungen sowie den Empfänger der von ihr erstellten Berichte und legt die Zuständigkeit für die Umsetzung der abgegebenen Empfehlungen fest.

Die GPDel hat in Bezug auf die Tätigkeiten der AB-ND im Rahmen der Aufsicht über die KND und die allfälligen Empfehlungen der AB-ND eine Klärung verlangt. Aus diesem Grund wird das Gesetz präzisiert. Während aus Artikel 78 Absatz 1 klar hervorgeht, dass die Aufsichtstätigkeit der AB-ND sich auch auf die Tätigkeiten der KND erstreckt, ist die Frage der Empfehlungen der AB-ND, die sich an diese richten, bisher nur teilweise in der VAND (Art. 13 Abs. 1 VAND) geregelt. Der neue Artikel 78*b* behebt diese mangelnde Eindeutigkeit und präzisiert in Absatz 1, dass die AB-ND Empfehlungen an sämtliche Stellen abgeben kann, die nach Artikel 78 Absatz 1 E-NDG ihrer Aufsicht unterstehen. Durch diese Präzisierung ist nunmehr klar, dass die Empfehlungen der AB-ND sich an eine oder mehrere Stellen richten können, wenn die Empfehlungen die Zusammenarbeit zwischen mehreren Stellen betrifft. Ausserdem wird die Information an das kantonale Dienstaufsichtsorgan ebenfalls von der Verordnungs- auf die Gesetzesstufe gehoben.

Für die Umsetzung der Empfehlungen der AB-ND ist unabhängig davon, an welches Organ sie sich richten, das VBS oder die verantwortliche kantonale Stelle zuständig, wie es der neue Artikel 78*b* – der den aktuellen Artikel 78 Absatz 1 übernimmt – vorsieht. Im neuen Absatz 4 wird für Empfehlungen, die in die kantonale Zuständigkeit fallen, ein neues Verfahren für deren Validierung und allenfalls für deren Ablehnung durch kantonale Behörden eingeführt. Damit wird die Entscheidungskompetenz in den Kantonen analog wie auf Stufe Bund geregelt (vgl. Abs. 2) und es wird ein Anliegen der GPDel berücksichtigt.

Artikel 78c Zusammenarbeit mit ausländischen Aufsichtsbehörden und Organisationen

Die Grundsätze der Koordination der Aufsicht über die Nachrichtendienste mit ausländischen Behörden werden neu im Gesetz geregelt. Die Einzelheiten dieser internationalen Koordination werden in der VAND festgelegt. Die Gründe für diese Anpassung sind folgende:

Mit der Intensivierung der grenzüberschreitenden Zusammenarbeit der Nachrichtendienste und der technischen Entwicklung hat sich auch die gegenseitige Bekanntgabe von Informationen, im Speziellen von Personendaten, erhöht. Dieser Informations- und Datenaustausch mit ausländischen Nachrichtendiensten ist Teil der täglichen Arbeit des NDB. Er kann auf verschiedene Weise erfolgen, mündlich oder schriftlich. Durch die kontinuierliche Internationalisierung der nachrichtendienstlichen Tätigkeiten wächst auch die Bedeutung der internationalen Zusammenarbeit zwischen Aufsichtsbehörden. Diese Zusammenarbeit ist häufig die Voraussetzung für eine wirksame Aufsicht über die international tätigen Nachrichtendienste. Aus diesem Grund muss auch die AB-ND die Möglichkeit haben, mit ihren ausländischen Partneraufsichtsbehörden Informationen und Erfahrungen auszutauschen, so wie dies andere Schweizer Aufsichtsbehörden können (z. B. die Finanzmarktaufsicht oder der EDÖB).

Die internationale Koordination mit ausländischen Partnern spielt auch bei der nachrichtendienstlichen Ausbildung der Mitglieder der AB-ND eine wichtige Rolle. Die Entwicklung der Kenntnisse der Behörde und ihrer Mitglieder kann sich nicht allein auf die von den beaufsichtigten Behörden gelieferten Informationen stützen.

Artikel 78d Tätigkeitsbericht

Artikel 78*d* E-NDG übernimmt den Inhalt des geltenden Artikels 78 Absatz 3. Die spezifische Information des VBS erfolgt durch die Mitteilung des Resultats der einzelnen Prüfungen der AB-ND (Art. 78*b* Abs. 1).

Artikel 78e Archivierung

Absätze 1 und 2

Neu wird klargestellt, dass auch die AB-ND ihre nicht mehr ständig benötigten und zur Löschung bestimmten Daten (Aufsichts- und Verwaltungsdaten sowie weitere Unterlagen) dem BAR zur Archivierung anbietet, dass diese dort in besonders gesicherten Räumlichkeiten aufbewahrt werden und dass für diese Daten die verlängerte Schutzfrist gilt (vgl. Abs. 2). Die Daten der AB-ND basieren zu einem Grossteil auf Daten des NDB, der KND und der übrigen beaufsichtigten Stellen, weshalb das Geheimhaltungsinteresse gleich gross ist. Von den Daten sind nur die Findmittel im System des BAR abgespeichert. Die Daten selber sind auf von diesen unabhängigen Festplatten abgespeichert.

Auch die AB-ND vernichtet Daten, die das BAR als nicht archivwürdig beurteilt, wie zum Beispiel Administrativdaten, gleich nach deren Löschung, auch wenn deren Auf-

bewahrungsfrist noch nicht abgelaufen ist. Dies entspricht dem datenschutzrechtlichen Grundsatz, wonach Daten nur so lange bearbeitet werden dürfen, wie dies zur Aufgabenerfüllung notwendig ist (auch die Aufbewahrung bereits gelöschter Daten stellt eine Datenbearbeitung dar).

Artikel 79

Wie im allgemeinen Kommentar zum vorliegenden Abschnitt («Kontrolle und Aufsicht des NDB») festgehalten, übernimmt die AB-ND vollumfänglich die Aufgaben der UKI, mit den entsprechenden Befugnissen dieser Behörde. Somit kann Artikel 79, der zurzeit Wesen und Aufgaben der UKI regelt, ersatzlos gestrichen werden.

Artikel 80

Als Folge der Möglichkeit, auch Mitarbeiterinnen und Mitarbeiter von inländischen Amtsstellen mit einer Tarnidentität auszustatten (siehe Art. 18), wird die Orientierung des Bundesrates und der GPDel über den Zweck und die Zahl der Tarnidentitäten erweitert. Auf Begehren der GPDel soll zudem klargestellt werden, dass der Bericht auch über die Ausstattung von menschlichen Quellen mit Tarnidentitäten informiert.

In diesem Gesetz wird ansonsten der Ausdruck «kantonale Vollzugsbehörden» verwendet, was in Absatz 4 vereinheitlicht wird.

Artikel 83

Aus den gleichen Gründen wie bei anderen Verfügungen, ist auch den Beschwerden gegen Verfügungen, die im Zusammenhang mit Kabelaufklärungen erlassen wurden, die aufschiebende Wirkung zu entziehen. Es kann nicht bis zum Ausgang eines Beschwerdeverfahrens abgewartet werden, sonst könnten nachträglich gelieferte Informationen schon veraltet und nicht mehr nützlich oder die Daten gar nicht mehr vorhanden sein, falls die gesetzlichen Aufbewahrungsfristen bereits abgelaufen sind.

6a. Kapitel: Strafbestimmungen, Gerichtsbarkeit und Mitteilung

Mit diesem neuen Kapitel werden alle Strafbestimmungen am Schluss des Gesetzestextes geregelt.

Artikel 83a–83b

Die Begründung der Einführung der Strafbestimmung für Tätigkeitsverbote ist in den Erläuterungen zu Artikel 83*c* enthalten.

Artikel 83*b* E-NDG übernimmt die aufgehobenen Absätze 4, 4bis und 5 von Artikel 74. Der Wortlaut entspricht der Fassung von Artikel 74, die das Parlament am 25. September 2020 in Zusammenhang mit der Umsetzung des Übereinkommens des Europarats zur Verhütung des Terrorismus verabschiedete.[44] Diese Fassung trat am 1. Juli 2021 in Kraft.

44 BBl **2020** 7891

Da die Tätigkeits- und Organisationsverbote durch den Bundesrat erlassen werden, folgen die dazugehörigen Strafbestimmungen für die Strafverfolgung anderen Regeln als die übrigen in Artikel 83*c* E-NDG geregelten Verstösse.

Artikel 83c Ungehorsam gegen Verfügungen und Verletzung der Geheimhaltungspflicht

Absätze 1 und 2

Zurzeit sieht das Gesetz keine besonderen exekutorischen oder strafrechtlichen Sanktionen (z. B. Strafbestimmungen) für den Fall vor, dass die betroffenen Personen sich einem Auskunftsersuchen des NDB z. B. nach Artikel 25 Absatz 1 widersetzen. Administrative Zwangsmittel dienen der Durchsetzung von gesetzlichen Pflichten gegenüber Personen, die die ihnen obliegenden Pflichten missachten. Somit steht dem NDB derzeit nur das im Verfahrensrecht vorgesehene Instrumentarium (Art. 40 f. VwVG) zur Durchsetzung einer Anordnung nach Artikel 25 zur Verfügung. Es gibt lediglich die Möglichkeit, der betroffenen Person eine Busse wegen Ungehorsams nach Artikel 292 des Strafgesetzbuches (StGB)[45] anzudrohen. Nach Artikel 106 Absatz 1 StGB darf eine solche Busse höchstens 10 000 Franken betragen. Wird die Verfügung nicht befolgt, kann der NDB bei der zuständigen kantonalen Staatsanwaltschaft Strafanzeige wegen Ungehorsams gegen eine amtliche Verfügung einreichen.

Der NDB kann Verfügungen im Zusammenhang mit Auskunftspflichten Privater erlassen (Art. 25). Ebenfalls kann im Bereich der Kabelaufklärung der durchführende Dienst gegenüber einer Betreiberin von leitungsgebundenen Netzen oder einer Anbieterin von Telekommunikationsdienstleistungen Verfügungen erlassen, um Daten zu verlangen (Art. 43). Der durchführende Dienst ist nach Artikel 26 NDV das CEA, das beim Kommando Cyber angesiedelt ist.

Falls die Pflichten nach diesem Gesetz verletzt werden und die gesetzliche Aufgabenerfüllung des NDB behindert wird, soll eine neue Bestimmung die Bestrafung der verantwortlichen Personen ermöglichen. Die Bestimmung ist der Strafbestimmung im BÜPF (Art. 39) nachgebildet und übernimmt auch deren Strafdrohung. Deren Höhe rechtfertigt sich auch aufgrund des Umstands, dass eine Busse eine angemessen bestrafende Wirkung entfalten soll. Gerade im Bereich der Kabelaufklärung dürfte eine Busse von lediglich maximal 10 000 Franken bei den verantwortlichen Personen von vielen Fernmeldedienstanbieterinnen nicht die angestrebte Wirkung erreichen. Wie die Bestrafung nach Artikel 39 BÜPF soll die Bestrafung nach diesem Artikel nur subsidiär zu strengeren Strafbestimmungen erfolgen, die gleichzeitig nach anderen Gesetzen erfüllt sein könnten. Hierbei ist insbesondere an die Verletzung von Geheimhaltungspflichten (und evtl. an Begünstigung) zu denken, die im StGB eingehend geregelt sind. Möglich ist auch eine Urkundenfälschung nach Artikel 251 StGB.

Wenn bei der Kabelaufklärung eine Betreiberin von leitungsgebundenen Netzen oder eine Anbieterin von Telekommunikationsdienstleistungen die vom durchführenden Dienst erfragten Daten nicht liefert, machen sich die verantwortlichen Personen strafbar. Es ist möglich, dass die gleiche Betreiberin von leitungsgebundenen Netzen für

45 SR **311.0**

mehrere einzelne Kabelaufklärungen Daten liefern muss. Falls sie dabei mehrmals ihrer Pflicht nicht nachkommt, machen sich die verantwortlichen Personen wiederholt strafbar. Im Wiederholungsfall kann die Busse erhöht werden. Hier gelten die üblichen Strafzumessungskriterien.

Die Verletzung der Geheimhaltung gegenüber Dritten nach Artikel 19 Absatz 3 und Artikel 20 Absatz 2 ist gleichbedeutend mit einer Verletzung des Amtsgeheimnisses nach Artikel 320 StGB. Deswegen enthält das NDG diesbezüglich keine besondere Strafbestimmung, sondern nur eine Strafbestimmung, die sich an Privatpersonen richtet. Bis jetzt war eine Verletzung der Geheimhaltung gegenüber Dritten für Privatpersonen straflos.

Mit dem neuen Absatz 2 wird für Bagatellfälle die Möglichkeit geschaffen, für die Pflichtverletzung eines Unternehmensangehörigen das Unternehmen zur Bezahlung einer Busse zu verurteilen. Damit kann die Behörde unverhältnismässigen Untersuchungsaufwand vermeiden.

Anders als Private, die nach Artikel 25 dem NDB Auskünfte oder Aufzeichnungen liefern müssen, unterliegen die menschlichen Quellen nach Artikel 15 keiner Pflicht, Informationen zu liefern. Dementsprechend unterstehen die menschlichen Quellen auch nicht dieser Strafbestimmung.

Artikel 83d Gerichtsbarkeit

Absatz 1

Diese Bestimmung ermöglicht es dem NDB sowie dem durchführenden Dienst bei Kabelaufklärungen, nach den Grundsätzen des Verwaltungsstrafrechts gegen Personen vorzugehen, die den ihnen gegenüber verfügten Pflichten nicht nachkommen. Dasselbe gilt für die Verletzung der Geheimhaltung. Im Rahmen von Kabelaufklärungen erlässt der durchführende Dienst Verfügungen, weswegen er in diesem Absatz ebenfalls aufgeführt wird.

Absatz 2

Dieser Absatz übernimmt den aufzuhebenden Artikel 74 Absatz 6 und wird mit der Verfolgung und Beurteilung der Verletzung des Tätigkeitsverbots ergänzt.

Artikel 83e Mitteilung

Dieser Artikel übernimmt inhaltlich den aufzuhebenden Artikel 74 Absatz 7. Er betrifft die Verletzung des Organisationsverbots sowie des Tätigkeitsverbots.

Artikel 85 Vollzug durch die Kantone

Absatz 1

Die KND sind bereits heute dazu befugt, Informationen nach Artikel 6 Absatz 1 Buchstabe a zu beschaffen und zu bearbeiten. Neu sollen sie auch die Möglichkeit haben, gestützt auf einen Auftrag des NDB Informationen nach Artikel 6 Absatz 1 Buchstabe b (Informationen zu sicherheitspolitisch bedeutsamen Vorgängen

im Ausland und im Cyberraum) zu bearbeiten. Dies entspricht – ohne die neu hinzukommende Ergänzung um den Cyberraum – einerseits bereits der heutigen Praxis. Wenn bspw. ein KND damit beauftragt wird, Mitglieder einer Oppositionsbewegung, die in der Schweiz wohnen, anzusprechen und dahingehend zu sensibilisieren, dass diese von ihrem Heimatstaat ausspioniert werden könnten, müssen dem KND im Rahmen der Auftragserteilung auch Informationen nach Artikel 6 Absatz 1 Buchstabe b weitergegeben werden.

Die Bearbeitung solcher Informationen ist im Bereich der äusseren Sicherheit, aber auch bei der Aufklärung und Bekämpfung von ausländischen machtpolitischen Bedrohungen und Beeinflussungsaktivitäten wichtig. Diese sind dann sicherheitspolitisch relevant, wenn sie von Staaten ausgehen und sich gegen das Funktionieren eines Staats und einer Gesellschaft richten und darauf abzielen, die demokratische und rechtsstaatliche Ordnung zu unterminieren. Es kann dabei darum gehen, Entscheidungsfindungsprozesse zu verzögern, Entscheidungen in eine gewünschte Richtung zu lenken oder generell das Vertrauen in demokratische Prozesse und staatliches Handeln zu untergraben. Diese Aktivitäten gehen von ausländischen staatlichen Akteuren aus und können von sich in der Schweiz befindlichen Personen unterstützt werden. Auch hier müssen dem KND im Rahmen der Auftragserteilung Informationen nach Artikel 6 Absatz 1 Buchstabe b weitergegeben werden.

Absatz 2

Die Befugnis, die genehmigungsfreien Beschaffungsmassnahmen einzusetzen, ist zurzeit in Artikel 85 Absatz 1 geregelt. Wie bereits in den Erläuterungen zu Artikel 9 Absatz 3 E-NDG ausgeführt, haben die KND bei der Berichterstattung an den NDB die Datenbearbeitungsschranke von Artikel 5 Absatz 5 zu beachten.

Änderung anderer Erlasse

1. Bundesgesetz vom 21. März 1997[46] über Massnahmen zur Wahrung der inneren Sicherheit

Diese Änderungen tragen der Umsetzung der Motion Rieder vom 28. September 2017 (17.3862 «Ausreisesperren für potenzielle Gewaltextremisten») Rechnung.

Artikel 2

Die bestehenden präventiv-polizeilichen Massnahmen werden in Absatz 2 Buchstabe f um Massnahmen gegen Gewalt anlässlich von Demonstrationen und Kundgebungen ergänzt. Personen, bei denen aufgrund konkreter und aktueller Anhaltspunkte angenommen werden muss, dass sie ausreisen wollen, um sich im Ausland an einer Demonstration oder Kundgebung an Gewalttätigkeiten gegen Personen oder Sachen zu beteiligen, werden in ihrem Handeln und in ihrer Zielsetzung eingedämmt. Eine

46 SR **120**

Ausreisebeschränkung gegen diese Personen steht im Dienste der Gefahrenabwehr. Durch die präventiv-polizeilichen Massnahmen wird den Betroffenen verunmöglicht, ihren Anliegen mittels Gewalt Ausdruck zu verleihen.

Artikel 10a Amtshilfe zwischen schweizerischen Behörden

Die Wahrung der inneren oder äusseren Sicherheit der Schweiz ist eine Staatsaufgabe, die im Verbund unter Berücksichtigung bestehender Strukturen auf allen drei Staatsebenen – Bund, Kantone und Gemeinden – zu erfüllen ist. Die nationale Kooperation ist für eine wirksame Abwehr von Bedrohungen unerlässlich. Bund, Kantone und Gemeinden unterstützen einander in der Erfüllung ihrer Aufgaben und arbeiten zusammen. Sie sind verpflichtet, einander Amtshilfe zu leisten (vgl. Art. 4 Abs. 2 dieses Gesetzes sowie Art. 44 Abs. 2 BV). Von der Pflicht zur Amtshilfe im Einzelfall betroffen sein können je nach Fallkonstellation beispielsweise die Polizei-, Strafverfolgungs- und Justizbehörden (Gerichte) des Bundes und der Kantone, der NDB, die KND, das Staatssekretariat für Migration (SEM), kantonale Justizvollzugsbehörden, Kindes- und Erwachsenenschutzbehörden sowie Einwohner-, Migrations-, Sozial-, Steuer-, und Grundbuchämter. Von der Pflicht zur Amtshilfe im Einzelfall betroffen sind auch öffentlich-rechtliche Anstalten wie Invalidenversicherungsstellen oder die schweizerische Unfallversicherungsanstalt.

Bislang wurden Bestimmungen zur Amtshilfe bzw. zur Datenbearbeitung in den besonderen Abschnitten des BWIS geregelt. Neu sollen die Bestimmungen, soweit möglich, im gemeinsamen, bereits bestehenden 3. Abschnitt zusammengeführt werden. Spezielle Datenbearbeitungsbestimmungen wie beispielsweise jene zu den Aufgaben zum Schutz von Personen und Gebäuden in Artikel 23*b*, insoweit sie von den allgemeinen Bestimmungen nach dem 3. Abschnitt dieses Gesetzes abweichen, gehen vor.

Absätze 1 und 2

Hier wird die Amtshilfe zwischen dem fedpol sowie den Behörden des Bundes, der Kantone und der Gemeinden geregelt. Einerseits sind die genannten Behörden auf Verlangen im Einzelfall verpflichtet, dem fedpol die Informationen, einschliesslich besonders schützenswerter Personendaten nach Artikel 5 Buchstabe c Ziffern 1, 2 und 4–6 DSG bekannt zu geben, die für die Erfüllung der Aufgaben nach Artikel 2 dieses Gesetzes erforderlich sind. Nicht erfasst werden genetische Daten, die nach Artikel 5 Buchstabe c Ziffer 3 DSG als besonders schützenswerte Personendaten gelten. Andererseits ist das fedpol, soweit keine Geheimhaltungsinteressen entgegenstehen, verpflichtet, den Bundesbehörden, Behörden der Kantone und Gemeinden auf Verlangen im Einzelfall die Informationen und besonders schützenswerten Personendaten bekannt zu geben, die nach diesem Gesetz erhoben wurden, in einem sachlichen Zusammenhang mit den Aufgaben nach diesem Gesetz stehen und für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind.

Das fedpol ist darauf angewiesen, im Einzelfall Informationen, einschliesslich besonders schützenswerter Personendaten, über Personen, die von einer Massnahme nach diesem Gesetz betroffen sein können, zu erheben. Ein Einzelfall muss sich nicht zwingend auf eine einzelne Person beziehen, sondern kann beispielsweise auch eine be-

stimmte, mit Risiken verbundene Veranstaltung oder ein Ereignis betreffen. Gruppenersuchen sind erlaubt, d. h. es kann ein Informationsersuchen betreffend mehrere Personen über ein einzelnes Amtshilfeersuchen gestellt und sodann gebündelt bearbeitet werden. Besonders schützenswerte Personendaten Dritter dürfen erhoben werden, sofern dies im Einzelfall zur Erfüllung der Aufgaben nach diesem Gesetz erforderlich ist. Es ist sicherzustellen, dass die datenbearbeitende Stelle keine von einem Berufs-, Geschäfts-, und Fabrikationsgeheimnis erfassten Informationen erhält, die nicht mit dem Grund, aus dem die Datenbearbeitung erforderlich ist, zusammenhängt. Für die Erhebung der Daten nach diesem Gesetz sowie der nachfolgenden Bearbeitung ist keine Einwilligung der betroffenen Person oder der Drittperson erforderlich. Die nach diesem Gesetz erhobenen Daten werden nach den Artikeln 3 ff. des Bundesgesetzes vom 13. Juni 2008[47] über die polizeilichen Informationssysteme des Bundes (BPI) u. a. zur Prüfung, zum Erlass und zum Vollzug der Massnahmen bearbeitet. Die Datenbearbeitung mündet in der Regel in ein Verfahren nach dem VwVG.

Absatz 3

Das fedpol kann die Weitergabe von Informationen und besonders schützenswerten Personendaten nach Absatz 2 verweigern, wenn die Wahrung der inneren oder äusseren Sicherheit der Schweiz die Geheimhaltung erfordert.

Artikel 10b Amtshilfe gegenüber ausländischen Behörden

Aktivitäten, welche die innere oder äussere Sicherheit der Schweiz gefährden, sind räumlich nicht auf Kantonsgebiete beschränkt, sondern erstrecken sich je nach Situation resp. Organisation und Netzwerk auf die Gebiete mehrerer Kantone und Länder. Dieser Umstand macht eine enge, internationale Kooperation unabdingbar.

Absatz 1

Das fedpol kann zur Erfüllung der Aufgaben nach Artikel 2 sowie zur Erfüllung der Aufgaben nach Artikel 67 Absatz 4 sowie Artikel 68 AIG Informationen, einschliesslich besonders schützenswerter Personendaten nach Artikel 5 Buchstabe c Ziffern 1, 2 und 4–6 DSG, mit ausländischen Behörden austauschen, die in ihren Staaten gleichartige Aufgaben wie das fedpol erfüllen.

Ein Einreiseverbot und eine Ausweisung nach Artikel 67 Absatz 4 sowie Artikel 68 AIG bezwecken – wie die Massnahmen nach Artikel 2 BWIS – die Abwehr einer Gefahr für die innere oder äussere Sicherheit der Schweiz, weshalb zur Erfüllung der Aufgaben dieselben Amtshilfemöglichkeiten zur Verfügung stehen müssen. Behörden des Bundes, der Kantone und der Gemeinden sind bereits heute nach Artikel 97 Absätze 1 und 2 AIG verpflichtet, die für den Erlass sowie den Vollzug einer Ausweisung oder eines Einreiseverbotes notwendigen Daten bekannt zu geben.

Die Informationen, einschliesslich besonders schützenswerter Personendaten, die das fedpol auf dem Amtshilfeweg nach der vorliegenden Bestimmung erhält, sind gerichtlich verwertbar. Denkbar ist eine Übermittlung von polizeilichen Feststellungen und Erkenntnissen aus dem Ausland. Gegenseitige Gruppenersuchen sind als Amtshilfe

47 SR **361**

zu qualifizieren und demnach erlaubt. Denkbar ist zudem, dass das fedpol im begründeten Einzelfall, insbesondere im Falle von Ausreisebeschränkungen nach diesem Gesetz Informationen, einschliesslich besonders schützenswerter Personendaten, an mit gleichartigen Aufgaben betraute ausländische Behörden weitergibt, damit diese bei einer allfälligen Missachtung einer Massnahme angemessen reagieren können. Die zuständigen Behörden des Landes, in dem beispielsweise ein Anlass stattfindet, haben ein Interesse daran, vom fedpol über Ausreisebeschränkungen informiert zu werden, da die Gefahrenlage bei Veranstaltungen regelmässig hoch ist und die Sicherheitsvorkehrungen entsprechend aufwendig sind. Die Voraussetzungen zur Bekanntgabe von Personendaten ins Ausland nach den Artikeln 16 und 17 DSG sind zu beachten. Zulässig ist eine Weitergabe von Daten an ausländische Behörden namentlich, wenn sie zur Wahrung eines überwiegenden öffentlichen Interesses notwendig ist (Art. 17 Abs. 1 Bst. c Ziff. 1 DSG).

Absatz 2

Gibt das fedpol einer ausländischen Behörde Informationen bekannt, dürfen diese nur für das betreffende Verfahren oder die betreffende amtliche Handlung verwendet werden, die dem Amtshilfeersuchen zugrunde liegt. Wenn die Daten anschliessend in einem Strafverfahren verwendet werden sollen, gelten die Grundsätze der internationalen Rechtshilfe in Strafsachen. Informationen aus der internationalen Amtshilfe dürfen Dritten nur bekannt gegeben werden, wenn das fedpol dies vorgängig genehmigt. Geheimhaltungsinteressen wie der Quellenschutz sind zu wahren. Die empfangende ausländische Behörde hat diese Einschränkungen einzuhalten.

Artikel 10c *Datenbekanntgabe zwischen Fedpol und Unternehmen mit öffentlich-rechtlichem Auftrag sowie Betreiberinnen von kritischen Infrastrukturen*

Absatz 1

Unternehmen mit öffentlich-rechtlichem Auftrag sowie Betreibinnen von kritischen Infrastrukturen sind auf Verlangen verpflichtet, die Informationen, einschliesslich besonders schützenswerter Personendaten nach Artikel 5 Buchstabe c Ziffern 1, 2 und 4-6 DSG, bekannt zu geben, die für die Erfüllung der Aufgaben nach Artikel 2 dieses Gesetzes sowie zur Erfüllung der Aufgaben nach Artikel 67 Absatz 4 sowie Artikel 68 AIG erforderlich sind.

Zur Abwendung einer Gefährdung der inneren Sicherheit, beispielsweise durch Sabotage, Spionage oder einen terroristischen Anschlag, respektive zur Gefährdungsbeurteilung ist das fedpol zum Schutz von Polizeigütern darauf angewiesen, von Unternehmen mit öffentlich-rechtlichem Auftrag (z. B. Schweizerischen Bundesbahnen, Flughafenbetreiberinnen, kantonalen Energieversorgern) sowie Betreiberinnen von kritischen Infrastrukturen (z. B. Trafo-Stationen im Stromverteilnetz, Kernkraftwerken) Informationen und besonders schützenswerte Personendaten einzuverlangen.

Absatz 2

Das fedpol kann Unternehmen mit öffentlich-rechtlichem Auftrag sowie Betreiberinnen von kritischen Infrastrukturen Informationen und besonders schützenswerte Personendaten bekannt geben, die für die Abwehr einer Gefahr erforderlich sind. Die Übermittlung kann Angaben zu den «modi operandi» beinhalten, die für die Abwehr einer Bedrohung erforderlich sind. Vorausgesetzt ist, dass tatsächlich eine Gefährdung für Personen oder Anlagen, Gebäude und die sonstige Infrastruktur vorliegt oder die Bedrohungssituation die Übermittlung der Informationen rechtfertigt. Es sind nur diejenigen Daten zu übermitteln, die für die Abwehr der Gefahr erforderlich sind. Der Datenaustausch zwischen Unternehmen mit öffentlich-rechtlichem Auftrag sowie Betreiberinnen von kritischen Infrastrukturen ist auf der Grundlage dieses Gesetzes nicht vorgesehen.

Artikel 10d Antrag an fedpol

Behörden des Bundes, der Kantone und der Gemeinden können beim fedpol Massnahmen nach Artikel 2 dieses Gesetzes sowie Massnahmen nach Artikel 67 Absatz 4 sowie Artikel 68 AIG beantragen. Ein Antrag ist zu begründen. Das schliesst nicht aus, dass das fedpol selbstständig tätig wird und diese Massnahmen von sich aus erlässt, soweit die entsprechenden Voraussetzungen erfüllt sind.

Artikel 14

Absatz 1

Neu eingefügt wird der Verweis auf die präventiv-polizeiliche Ausweisung und das Einreiseverbot im Sinne von Artikel 67 Absatz 4 sowie Artikel 68 AIG, die das fedpol zur Wahrung der inneren oder äusseren Sicherheit gegenüber ausländischen Staatsangehörigen erlässt. Das führt dazu, dass sich das fedpol zum Erlass dieser Entfernungs- und Fernhaltemassnahmen auf die Informationsbeschaffungsmöglichkeiten nach Artikel 14 Absatz 2 BWIS stützen kann. Das fedpol und die Kantone können diese Daten wie bereits nach dem geltenden Recht beschaffen, selbst wenn dies für die betroffenen Personen nicht erkennbar ist.

Artikel 23h

Die Bestimmung zur Datenbearbeitung nach dem 5. Abschnitt ist aufzuheben, da der Regelungsinhalt mit den gemeinsamen Bestimmungen des 3. Abschnitts, mit den Artikeln 3 ff. und 18 BPI und – sofern ein Verfahren daraus resultiert – mit Artikel 12 VwVG abgedeckt wird.

Artikel 23i

Die Bestimmung zur Antragsstellung durch Behörde nach dem 5. Abschnitt ist aufzuheben, da der Regelungsinhalt mit den gemeinsamen Bestimmungen des 3. Abschnitts abgedeckt wird.

Artikel 23r

Die Amtshilfe braucht in Absatz 2 nicht mehr genannt zu werden, da sie mit den gemeinsamen Bestimmungen des 3. Abschnitts abgedeckt wird.

Artikel 24a

Absatz 4

Diese Bestimmung muss neu formuliert werden, da Artikel 13 BWIS, auf den verwiesen wird, auf den 1. September 2017 aufgehoben wurde. Die neue Formulierung enthält keinen Verweis auf einen anderen Artikel mehr, sondern nennt direkt die (ursprünglich dort aufgeführten) Stellen, die eine Mitteilungspflicht haben. Zusätzlich werden die Gerichte von Bund und Kantonen genannt. Gerichtsurteile, die in Zusammenhang mit Gewalttätigkeiten anlässlich von Sportveranstaltungen ergehen, sind erforderlich zur Überprüfung der im elektronischen Informationssystem nach Artikel 24*a* eingetragenen Massnahmen (Anpassung oder gegebenenfalls Aufhebung der Massnahme aufgrund nachträglichen Freispruchs). Bislang gelangten die Urteile unvollständig und auf Umwegen (z. B. via Polizeibehörden) an das fedpol. Neu sollen Urteile in Zusammenhang mit Gewalttätigkeiten anlässlich von Sportveranstaltungen direkt durch die urteilenden Gerichte an das fedpol weitergeleitet werden.

Artikel 24c

Absatz 2

Der Wortlaut ist an die einheitliche Formulierung im Bereich der präventiv-polizeilichen Massnahmen anzupassen. Eine Ausreisebeschränkung kann demnach gegen eine Person verfügt werden, gegen die kein Rayonverbot oder keine Meldeauflage besteht, wenn «aufgrund konkreter und aktueller Anhaltspunkte davon ausgegangen werden muss», dass sie sich im Bestimmungsland an Gewalttätigkeiten beteiligen wird. Die Voraussetzungen nach dem bestehenden Absatz 2 haben sich als nicht praxisgerecht erwiesen (vgl. Urteil des Bundesverwaltungsgerichts F-5247/2024 vom 20. Februar 2025 E. 6.4.2). Die präventiv-polizeiliche Massnahme ist, wie die übrigen Massnahmen nach diesem Gesetz, zur Abwehr einer künftigen Gefahr konzipiert. Sie ist nicht an das Vorliegen eines hängigen oder abgeschlossenen Strafverfahrens anzuknüpfen. Entscheidend ist, ob eine polizeiliche Gefahr vorliegt. Die verfügende Behörde arbeitet nicht delikt-, sondern gefahrenorientiert. Sie muss regelmässig innert kurzer Frist oder bei Gefahr im Verzug mit den ihr zum gegebenen Zeitpunkt zur Verfügung stehenden Informationen – wie beispielsweise polizeilichen Feststellungen und Erkenntnisse, Aussagen von Fanbeauftragten der Sportvereine oder des Sicherheitspersonals der Stadien, die auf eine künftige Gewalttätigkeit hinweisen – über den Erlass der Massnahme entscheiden. Dementsprechend kann auch nicht ausschlaggebend sein, ob die zum Zeitpunkt der Verfügung vorliegenden Erkenntnisse in strafrechtlich genügsamer Form eine Straftat im Sinne des StGB nachweisen oder nicht. Vielmehr müssen die vorliegenden aktuellen und konkreten Anhaltspunkte zum Schluss führen, dass es mit hinreichender Wahrscheinlichkeit zu Gewalttätigkeiten im Bestimmungsland der Sportveranstaltung kommen wird, was je nach Fall mit prognostischen Unsicherheiten

verbunden ist. Die Ausführungen zu einem gewalttätigen Verhalten sowie der entsprechende Nachweis dazu sind in den Artikeln 4 und 5 der Verordnung vom 4. Dezember 2009[48] über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN anzupassen bzw. aufzuheben.

5b. Abschnitt: Massnahmen gegen Gewalt anlässlich von Demonstrationen und Kundgebungen

Für die neuen Massnahmen gegen Gewalt anlässlich von Demonstrationen und Kundgebungen wird ein zusätzlicher Gliederungstitel bzw. ein Abschnittstitel nötig. Der Abschnitt wird nach dem 5*a*. Abschnitt (Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen) eingefügt.

Artikel 24d Ausreisebeschränkung

Die Ausreisebeschränkung ist eine präventiv-polizeiliche Massnahme. Sie dient der Sicherung der demokratischen und rechtsstaatlichen Grundlagen, bzw. es soll verhindert werden, dass sich Personen an Gewaltakten im Zusammenhang mit Demonstrationen oder Kundgebungen im Ausland beteiligen. Die Massnahme soll frühzeitig angeordnet werden. Das fedpol ist befugt die Bewegungsfreiheit einzelner Personen einzuschränken, soweit die zu schützenden Rechtsgüter es rechtfertigen. Bei Missachtung einer Ausreisebeschränkung droht im Sinne von Artikel 292 StGB eine Busse.

Es darf keine Ausreisebeschränkung erlassen werden, die sie sich gegen die rechtmässige Ausübung einer politischen, weltanschaulichen oder religiösen Demonstration und Kundgebung richtet. Politische Aktivitäten wie auch Meinungs- und Glaubensäusserungen, mit welchen Veränderungen des Staates und der Gesellschaft angestossen werden sollen, dürfen nicht durch Ausreisebeschränkungen beschnitten werden. Protest und Empörung sind in einer demokratischen Gesellschaft unverzichtbar. Die Grund- und Menschenrechte schützen Glaubens- und Meinungsäusserungen sowie politische Aktivitäten, die durch einen Teil der Gesellschaft positiv oder gleichgültig aufgenommen werden, aber auch solche, die einen Teil der Bevölkerung beleidigen, schockieren oder stören. Das fordert der Pluralismus, die Toleranz und die Aufgeschlossenheit, ohne die es keine demokratische Gesellschaft gäbe.[49] Grund- und Menschenrechte werden jedoch missbraucht, wenn sie angerufen werden, um die demokratische und rechtsstaatliche Grundordnung gewaltsam zu bekämpfen. Die eigene Meinung durch Gewalt gegen andere Personen oder Sachen auszudrücken, ist vom sachlichen Geltungsbereich des Rechts auf freie Meinungsäusserung nicht gedeckt.[50] Gefährderinnen und Gefährder, bei denen gewaltsame Handlungen nicht ausgeschlossen werden können, müssen die Einschränkung ihrer Freiheitsrechte, soweit verhältnismässig, in Kauf nehmen. Die verantwortlichen Behörden haben das neue Präventionsinstrument sorgfältig einzusetzen. Die Begründungsdichte eines Entscheids ist

48 SR **120.52**
49 Vgl. Grundsatzurteil des Europäischen Gerichtshofes für Menschenrechte in *Handyside v. the United Kingdom*, judgment of 7 December 1976, application no. 5493/72, § 49.
50 BGE *143* I 147 E 3.2

an der zeitlichen Dimension und an den innert dieser Frist verfügbaren Informationen auszurichten.

Absatz 1

Das fedpol ist als Polizeibehörde des Bundes für die Verfügung von Ausreisebeschränkungen gegenüber Gefährderinnen und Gefährdern zuständig bzw. kann einer Person die Ausreise aus der Schweiz in ein bestimmtes Land für eine bestimmte Zeitdauer untersagen. Der Absatz definiert die Voraussetzungen, unter denen eine Ausreisebeschränkung verfügt werden darf.

Buchstabe a

Eine Person, gegen die eine Ausreisebeschränkung erlassen werden soll, muss sich gemäss einer strafrechtlichen Verurteilung oder polizeilichen oder nachrichtendienstlichen Erkenntnissen an Gewalttätigkeiten gegen Personen oder Sachen beteiligt haben. Entsprechende Erkenntnisse können sich beispielsweise aus Angaben zu einem hängigen Strafverfahren, polizeilichen oder nachrichtendienstlichen Feststellungen sowie einer Wegweisungsverfügung ergeben. Die Beteiligung an einem gewaltsamen Verhalten kann, muss aber nicht im Zusammenhang mit einer Demonstration oder Kundgebung stehen.

Buchstabe b

Zusätzlich muss aufgrund konkreter und aktueller Anhaltspunkte angenommen werden, dass die betroffene Person ausreisen will, um sich im Bestimmungsland an einer Demonstration oder Kundgebung an Gewalttätigkeiten gegen Personen oder Sachen zu beteiligen. Konkrete Anhaltspunkte für künftiges gewalttätiges Verhalten liegen vor, wenn sich entsprechende Befürchtungen durch das Verhalten der betroffenen Person begründen lassen. Das fedpol hat gestützt auf das bisherige Verhalten der betroffenen Person die Wahrscheinlichkeit einer möglichen künftigen Gewaltbegehung darzulegen. Eine solche Einschätzung ist mit Unsicherheiten verbunden. Aktuell sind entsprechende Anhaltspunkte dann, wenn sie zum Zeitpunkt der Anordnung der Ausreisebeschränkung vorliegen. Zeitlich weit zurückliegende Befürchtungen, die zum massgebenden Zeitpunkt nicht mehr sicherheitsrelevant erscheinen, können für sich genommen nicht zur Begründung einer aktuellen Gefahr angeführt werden. Sie können jedoch im Rahmen der Gesamtwürdigung zusammen mit weiteren Anhaltspunkten von Relevanz sein.

Absatz 2

Nicht nur die direkte Ausreise in das Bestimmungsland ist verboten, sondern auch Ausreisen in andere Länder, mit denen das Verbot umgangen werden könnte. Damit soll verhindert werden, dass betroffene Personen durch alternative Reiserouten trotzdem an der Veranstaltung teilnehmen. Die Ausreisebeschränkung schliesst also Ausreisen in gewisse Drittländer mit ein, um die Reise in das Bestimmungsland über ein Drittland zu verhindern. Begründete Ausnahmen von der Beschränkung sind möglich, wenn die Person wichtige Gründe geltend machen kann und der Zweck der Massnahme dadurch nicht gefährdet wird. Über die Ausnahmebewilligung entscheidet das fedpol im Rahmen einer summarischen Interessenabwägung.

Absatz 3

Die Ausreisebeschränkung wird im automatisierten Polizeifahndungssystem nach Artikel 15 BPI (RIPOL) eingetragen, sodass die Behörden mit Zugriff auf RIPOL informiert sind und die Ausreisebeschränkung vollziehen können. Das Fahndungssystem RIPOL wird regelmässig von mit Sicherheitsaufgaben betrauten Behörden abgefragt. Die Grenzbehörden erhalten auch eine Mitteilung, sodass sie für den fraglichen Zeitraum sensibilisiert sind. Zusätzlich kann das fedpol die zuständigen Sicherheitsbehörden im Ausland informieren, sodass diese auf die Ausreisebeschränkung reagieren können, beispielsweise mit einer Einreisebeschränkung oder einer örtlichen Wegweisung. Dabei darf das fedpol besonders schützenswerte Personendaten bekannt geben (vgl. Art. 10*b* BWIS). Der nationale Teil des Schengener Informationssystems (N-SIS; Art. 16 BPI) sieht keine Ausschreibungskategorien für Ausreisebeschränkungen für gewalttätige Extremistinnen und Extremisten vor, weshalb die Information nicht über den SIS-Kanal erfolgen kann.

Erfahrungen aus dem Bereich der Ausreisebeschränkungen gegen Gewalt anlässlich von Sportveranstaltungen zeigen, dass Ausreisebeschränkungen präventiv wirken: Die mit einer Beschränkung belegte Person sieht im Hinblick auf die Strafandrohung oftmals von einer Ausreise ab.

Artikel 24e Dauer der Ausreisebeschränkung

Die Einschränkung der Bewegungsfreiheit darf nur so lange andauern, wie sie unbedingt notwendig ist, um eine Teilnahme der betreffenden Person an Gewaltakten zu verhindern. Die Ausreisebeschränkung darf deshalb für maximal drei Tage vor der Veranstaltung und längstens bis einen Tag nach deren Ende verfügt werden. So wird sichergestellt, dass die Beschränkung nur für eine verhältnismässige Dauer erfolgt.

5c. Abschnitt: Gemeinsame Bestimmungen zum 5., 5a. und 5b. Abschnitt

Die gemeinsamen Bestimmungen zu den Abschnitten 5 und 5*a* werden aufgrund des neu eingeführten Abschnitts 5*b* (Massnahmen gegen Gewalt anlässlich von Demonstrationen und Kundgebungen) neu im Abschnitt 5*c* (zuvor 5*b*) geregelt; die neuen Massnahmen nach dem 5*b.* Abschnitt werden in den Geltungsbereich der gemeinsamen Bestimmungen aufgenommen.

Artikel 24f

Absatz 2

Ausreisebeschränkungen gegen gewalttätig-extremistische Aktivitäten dürfen – analog den Ausreisebeschränkungen gegen Gewalt anlässlich von Sportveranstaltungen – gegenüber Personen ab dem sechzehnten Altersjahr verfügt werden. Die tiefe Altersgrenze trägt dem Umstand Rechnung, dass auch minderjährige Personen eine hohe Gewaltbereitschaft aufweisen, und sie betont den präventiven Charakter der Massnahme: Die Polizeipraxis zeigt, dass etliche bereits sehr junge Personen von gewalttätig-extremistischen Gruppierungen für ihre Zwecke instrumentalisiert werden. Beispielsweise waren 2018 bei einer nicht bewilligten Kundgebung in der Schweiz 40 Minderjährige beteiligt. Vermummte Personen verursachten einen Sachschaden

von rund 100 000 Franken. Insgesamt 147 Personen, davon 21 minderjährig, wurden wegen verschiedener Delikte (u. a. Landfriedensbruch, Ungehorsam gegen amtliche Verfügung, Hinderung einer Amtshandlung, Gewalt und Drohung gegen Beamte, Widerhandlung gegen das Sprengstoffgesetz vom 25. März 1977[51], Sachbeschädigungen) angezeigt. Die jüngste Person war zum Zeitpunkt der Festnahme dreizehn Jahre alt. Eine Ausreisebeschränkung hat also auch eine Schutzfunktion für Jugendliche in dem Sinne, dass diese mit einer behördlichen Anordnung konfrontiert sind, die sie davon abhält, sich an organisierten Gewalttätigkeiten zu beteiligen.

Artikel 24g

Absatz 1

Die bestehende Bestimmung zum Rechtsweg wird ergänzt, sodass sie auch die Ausreisebeschränkung zur Verhinderung von Gewalt anlässlich von Demonstrationen und Kundgebungen umfasst.

Absatz 2

Das Beschwerderecht richtet sich grundsätzlich nach Artikel 48 VwVG. Das zusätzliche Beschwerderecht nach Absatz 2 Buchstaben a und b dieses Gesetzes wurde im Rahmen des Bundesgesetzes vom 25. September 2020[52] über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) eingeführt. Es ist lediglich in entsprechenden Verfahren erforderlich und soll deshalb nur in Verfahren nach dem 5. Abschnitt gelten, nicht hingegen bei Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen oder von Demonstrationen und Kundgebungen.

Artikel 28

Absatz 2

Mit der Änderung wird ein falscher Verweis im Gesetz korrigiert, der durch eine frühere Rechtsänderung entstanden ist. Eine materielle Änderung des geltenden Rechts ist damit nicht verbunden.

2. Informationssicherheitsgesetz vom 18. Dezember 2020[53]

Artikel 45

Absätze 6 Buchstabe c und 7

Wie bereits mehrfach erwähnt, werden mit dem Revisionsentwurf nicht mehr Informationssysteme geregelt, sondern die Datenbearbeitung. Deshalb wird in Artikel 45 Absatz 6 Buchstabe c ISG der Begriff «INDEX NDB» aufgehoben. Stattdessen wird

51 SR **941.41**
52 AS **2021** 565
53 SR **128**

der Zugriff in Absatz 7 geregelt. Dies entspricht der in Artikel 58*e* Absatz 1 Buchstabe c NDG statuierten, bereits heute bestehenden Zugriffsberechtigung der Fachstellen für Personensicherheitsprüfungen.

Artikel 56

Absatz 3

Analog zum Zugriff der Fachstellen für Personensicherheitsprüfungen erhält neu auch die für Betriebssicherheitsverfahren zuständige Fachstelle eine Zugriffsberechtigung, siehe dazu die Erläuterungen zu Artikel 58*e* Absatz 1 Buchstabe d E-NDG. Dies wird hiermit auch im ISG entsprechend abgebildet.

Artikel 73d Absatz 2 und 76a Absatz 2

In Artikel 73*d* Absatz 2 ISG wird der geltende Verweis auf Artikel 6 Absätze 1 Buchstabe a, 2 und 5 NDG mit Artikel 6 Absatz 1 Buchstabe b NDG ergänzt. Diese Ergänzung ist vergleichbar mit derjenigen, die für Artikel 85 Absatz 1 E-NDG vorgeschlagen wird: Auch Informationen im Bereich der äusseren Sicherheit sind bei der Weiterleitung von Informationen über Cybervorfälle durch das Bundesamt für Cybersicherheit von Bedeutung. Die gleiche Anpassung ist aus dem gleichen Grund auch in Artikel 76*a* Absatz 2 ISG vorzunehmen.

3. Ausländer- und Integrationsgesetz vom 16. Dezember 2005[54]

Artikel 75

Absatz 3

Mit dem Mantelerlass bzw. dem PMT wurde ein neuer, zusätzlicher ausländerrechtlicher Haftgrund der Gefährdung der inneren oder äusseren Sicherheit der Schweiz in Artikel 75 Absatz 1 Buchstabe i, Artikel 76 Absatz 1 Buchstabe b Ziffer 1 sowie Artikel 76*a* Absatz 2 Buchstabe j AIG geschaffen. Die Gefährdung der inneren oder äusseren Sicherheit wird folglich als konkretes Anzeichen erfasst, das befürchten lässt, dass sich die betroffene Person der Durchführung der Weg- bzw. Ausweisung entziehen will (vgl. dazu die Botschaft vom 22. Mai 2019[55] zum Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus sowie das Urteil des Bundesgerichts vom 15. Januar 2025[56]).

In der Praxis hat es sich als Problem erwiesen, wenn nach Artikel 75 Absatz 1 AIG lediglich Personen, die keine Kurzaufenthalts-, Aufenthalts- oder Niederlassungsbewilligung besitzen, in Vorbereitungshaft genommen werden können. Sofern eine ausländische Person mit einer solchen Bewilligung die innere oder äussere Sicherheit der Schweiz gefährdet, kann das fedpol ihr gegenüber eine Ausweisung verfügen (Art. 68

54 SR **142.20**
55 BBl **2019** 4751 S. 4807
56 Urteil des Bundesgerichts 2C 577/2024 vom 15. Januar 2025 E. 6.2.2

Abs. 1 AIG). Sie wird mit einem befristeten oder unbefristeten Einreiseverbot verbunden (Art. 68 Abs. 3 AIG). Wenn die betroffene Person erheblich oder wiederholt gegen die öffentliche Sicherheit und Ordnung verstossen hat oder diese gefährdet oder die innere oder die äussere Sicherheit gefährdet, ist die Ausweisung sofort vollstreckbar (Art. 68 Abs. 4 AIG). Bei einer Ausweisung nach Artikel 68 AIG besteht grundsätzlich ein grosses und legitimes Interesse des Gemeinwesens an einer Entfernung und Fernhaltung (vgl. dazu die Botschaft vom 8. März 2002[57] zum Bundesgesetz über die Ausländerinnen und Ausländer). Eine ausländerrechtliche Haft ist nach geltendem Recht vor der Eröffnung des erstinstanzlichen Ausweisungsentscheids nicht möglich, wenn die betroffene Person über eine Kurzaufenthalts-, Aufenthalts- oder Niederlassungsbewilligung verfügt. In Fällen der Gefährdung der inneren oder äusseren Sicherheit soll deshalb die Anordnung der Vorbereitungshaft neu auch in diesen Fällen während des erstinstanzlichen Ausweisungsverfahrens möglich sein. Das Vorliegen einer Gefährdung der inneren oder äusseren Sicherheit ist wie bei Artikel 75 Absatz 1 Buchstabe i, Artikel 76 Absatz 1 Buchstabe b Ziffer 1 und Artikel 76*a* Absatz 2 Buchstabe j AIG aufgrund der Erkenntnisse von des fedpol oder des NDB zu beurteilen.

Die Vorbereitungshaft soll die Durchführung eines Ausweisungsverfahrens sicherstellen. Ein solches Verfahren wird durch das fedpol aufgenommen, wenn aufgrund erster, konkreter Anzeichen von einer Gefährdung der inneren oder äusseren Sicherheit ausgegangen wird. Ist aufgrund dieser Gefährdung zu befürchten, dass sich die betroffene Person der Durchführung der Ausweisung entziehen will, ermöglicht die neue Bestimmung die Anordnung der Vorbereitungshaft. Bei der Haftanordnung ist der Grundsatz der Verhältnismässigkeit nach Artikel 36 Absatz 3 BV in jedem Einzelfall zu berücksichtigen. Die Vorbereitungshaft darf nur unter der Voraussetzung angeordnet werden, dass der Vollzug der Entfernungsmassnahme absehbar, d. h. rechtlich und tatsächlich möglich ist (Art. 80 Absatz 6 Bst. a AIG). Das fedpol als verfügende Behörde hat im Rahmen des Ausweisungsverfahrens allfällige Vollzugshindernisse, je nach Zielstaat insbesondere die Einhaltung des Rückschiebeverbot und des Folterverbots, zu prüfen. Kommt das fedpol während der Vorbereitungshaft nach Artikel 75 Absatz 3 AIG bzw. während dem Ausweisungsverfahren zum Schluss, dass die Absehbarkeit des Vollzuges nicht gegeben ist, muss die betroffene Person aus der Haft entlassen werden.

Für Staatsangehörige von EU- oder EFTA-Mitgliedstaaten gilt der Vorbehalt von Artikel 2 Absätze 2 und 3 AIG. Diese Bestimmungen müssen innerhalb des Rahmens angewandt werden, der durch Artikel 5 Anhang I des Abkommens vom 21. Juni 1999[58] zwischen der Schweizerischen Eidgenossenschaft einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits über die Freizügigkeit (FZA) bzw. durch Artikel 5 Anhang K Anlage 1 des Übereinkommens vom 4. Januar 1960[59] zur Errichtung der Europäischen Freihandelsassoziation (EFTA-Übereinkommen) und die entsprechende Rechtsprechung des Gerichtshofs der Europäischen Union vorgegeben ist. Dies bedeutet insbesondere, dass eine Haft nur dann

57 BBl **2002** 3814
58 SR **0.142.112.681**
59 SR **0.632.31**

gerechtfertigt werden kann, wenn das persönliche Verhalten der Person, gegen welche die Haft verfügt wird, eine tatsächliche, gegenwärtige und hinreichend schwere Bedrohung für die innere oder äussere Sicherheit der Schweiz darstellt. Die blosse Existenz von strafrechtlichen Verurteilungen kann für sich allein genommen nicht automatisch eine solche Haft begründen.

Nach Eröffnung des Ausweisungsentscheids kann eine Ausschaffungshaft nach Artikel 76 AIG angeordnet werden, sofern die weiteren Haftvoraussetzungen ebenfalls weiterhin erfüllt sind.

Nach Artikel 61 Absatz 1 Buchstabe d AIG erlischt eine ausländerrechtliche Bewilligung einer Person mit dem erstinstanzlichen Entscheid, dass sie ausgewiesen wird.

Artikel 101

Absatz 1

Mit der Aufnahme des fedpol in den Anwendungsbereich dieser Norm wird eine gesetzestechnische Lücke geschlossen. Auch das fedpol führt mit den Einreiseverboten (Art. 67 Abs. 4 AIG) sowie Ausweisungen (Art. 68 AIG) zur Wahrung der inneren oder äusseren Sicherheit der Schweiz Verfahren nach diesem Gesetz. Das fedpol muss deshalb Personendaten von Ausländerinnen und Ausländern, einschliesslich besonders schützenswerter Personendaten, sowie von an Verfahren nach diesem Gesetz beteiligten Dritten bearbeiten oder bearbeiten lassen können, soweit diese Daten zur Erfüllung der gesetzlichen Aufgaben des fedpol benötigt werden.

4. Bundesgesetz vom 20. Juni 2003[60] über das Informationssystem für den Ausländer- und den Asylbereich

Artikel 9

Absatz 1 und 2

Der NDB verfügt heute über den Zugriff im Abrufverfahren auf das Zentrale Migrationsinformationssystem (ZEMIS), das der Bearbeitung von Personendaten aus dem Ausländer- und dem Asylbereich dient.

Das vormals im AIG geregelte Informationssystem zur Ausstellung von schweizerischen Reisedokumenten und von Bewilligungen zur Wiedereinreise an Ausländerinnen und Ausländer (ISR) wurde aufgehoben[61] und die Daten wurden ins ZEMIS überführt. Der Verwendungszweck des ZEMIS wurde entsprechend auf Aufgaben im Zusammenhang mit der Ausstellung von schweizerischen Reisedokumenten und von Bewilligungen zur Wiedereinreise für ausländische Staatsangehörige aus dem Ausländerbereich und aus dem Asylbereich ausgeweitet.

60 SR **142.51**

61 Ziff. I des Bundesgesetzes vom 14. Dez. 2018 über die Ausländerinnen und Ausländer und die Integration (Verfahrensregelungen und Informationssysteme), in Kraft seit 15. Okt. 2023; BBl **2018** 1685, AS **2019** 1413 und **2023** 548.

Das ISR war für gewisse Kategorien von Ausländerinnen und Ausländern das Pendant zum Informationssystem Ausweisschriften (ISA) nach Artikel 11 des Ausweisgesetzes vom 22. Juni 2001[62]. Der Zugriff des NDB auf das ISA wurde bereits mit dem PMT geregelt. Auch der Zugriff auf die Daten des ehemaligen ISR zur Identifikation einer Person ist unabdingbar für das lückenlose Recherchieren durch den NDB. Ohne diesen Zugriff ist der NDB oft nicht in der Lage, eine Person zu identifizieren und muss deshalb zu anderen Massnahmen greifen, die einen grösseren Eingriff in die Persönlichkeitsrechte darstellen können. Sämtliche Informationen zu möglichen Reisen und die Beschaffung von Dokumenten sind von Wichtigkeit, z. B. für die Früherkennung von möglichen Dschihadreisenden oder für die Verhinderung von Reisen in Kriegsgebiete. Mit diesem Zugriff auf das ISR kann der NDB mit milderen Mitteln arbeiten, die in einem besseren Verhältnis zum Persönlichkeitsschutz stehen.

Wie erwähnt gehört der NDB bereits zu den Behörden die über eine Zugriffsberechtigung auf die Daten des ZEMIS für gewisse Zwecke verfügen. Aufgrund der Übernahme der Daten des ISR ins ZEMIS benötigt der NDB diesen Zugriff aber auch zum Zweck der Personenidentifikation im Zusammenhang mit der Bearbeitung sicherheitspolitisch bedeutsamer Vorgänge im Ausland. Artikel 9 Absatz 1 Buchstabe l Ziffer 1 und Absatz 2 Buchstabe l Ziffer 1, welche die Zwecke festlegen, zu denen der NDB auf die Daten des ZEMIS im Abrufverfahren zugreifen kann, sollen deshalb jeweils mit der Erfüllung der Aufgaben des NDB nach Artikel 6 Absatz 1 Buchstabe b NDG ergänzt werden.

Die Details zum Zugriff im Abrufverfahren werden wie üblich im Verordnungsrecht geregelt.

5. Parlamentsgesetz vom 13. Dezember 2002[63]

Artikel 142

Absätze 2 und 3

Die Aufnahme der AB-ND in Artikel 142 Absatz 2 ParlG ist das Pendant zu Artikel 77 Absatz 2 NDG. So kann dem Erfordernis einer formell-gesetzlichen Grundlage vollständig Rechnung getragen werden. Der Bundesrat ist der Ansicht, dass die AB-ND auch in Artikel 142 Absatz 3 ParlG aufgenommen werden sollte und dass diese selbst am besten in der Lage ist, ihren Voranschlag vor der Bundesversammlung zu vertreten, wenn sich dies als notwendig erweisen sollte. Der Wortlaut orientiert sich an der Fassung, die das Parlament am 25. September 2020 in Zusammenhang mit der Revision des DSG verabschiedete und die am 1. September 2023 in Kraft getreten ist.

Die hier formalrechtlich statuierte Sonderstellung der AB-ND wird auch zu einer Ergänzung von Artikel 1 Absatz 2 der Finanzhaushaltverordnung vom 5. April 2006[64] führen.

62 SR **143.1**
63 SR **171.10**
64 SR **611.01**

6. Verwaltungsgerichtsgesetz vom 17. Juni 2005[65]

Artikel 23

Absatz 2 Buchstabe b

Infolge der Anpassung resp. Neustrukturierung von Artikel 29 NDG muss der Verweis in Artikel 23 Absatz 2 Buchstabe b VGG angepasst werden.

7. Strafgesetzbuch[66]

Artikel 66a

Absatz 1 Buchstabe p

Infolge der Aufhebung bzw. der Umplatzierung von Artikel 74 Absatz 4 NDG muss in dieser Bestimmung ein Verweis angepasst werden.

8. Strafprozessordnung[67]

Artikel 269 Absatz 2 Buchstabe n und 286 Absatz 2 Buchstabe l

Infolge der Aufhebung bzw. der Umplatzierung von Artikel 74 Absatz 4 NDG muss in beiden Bestimmungen ein Verweis angepasst werden.

9. Strafregistergesetz vom 17. Juni 2016[68]

Artikel 46

Die Zugangsrechte des fedpol zur Wahrnehmung gewisser präventiv-polizeilicher Aufgaben werden durch die neue Ziffer 11 in Buchstabe a ausgedehnt. Das fedpol erhält neu für die Verhängung und Aufhebung von präventiv-polizeilichen Massnahmen im Zusammenhang mit der Terrorismusabwehr sowie zur Abwendung von Gewalt anlässlich von Demonstrationen und Kundgebungen nach dem BWIS dieselben Zugangsrechte auf den Behördenauszug 2 (Art. 38 des Strafregistergesetzes), über die es bereits im Rahmen von ausländerrechtlichen Fernhaltemassnahmen verfügt (vgl. Art. 46 Bst. a Ziff. 4). Somit kann das fedpol zwar erkennen, ob bei einer möglichen Gefährderin oder einem möglichen Gefährder zu einem gewissen Deliktstyp ein hängiges Strafverfahren oder ein Grundurteil im Strafregister erfasst ist, aber nicht auf

65 SR **173.32**
66 SR **311.0**
67 SR **312.0**
68 SR **330**

welchem genauen Sachverhalt dieser Deliktsvorwurf beruht. Die zuständige Stelle des fedpol muss solche Informationen nachträglich auf dem Amtshilfeweg direkt bei der zuständigen Strafbehörde einholen. Bei Gefahr im Verzug kann folglich die Prüfung von Sachverhaltsangaben zu hängigen oder abgeschlossenen Strafverfahren, die für die Verhängung genannter Massnahmen relevant sein können, lediglich summarisch erfolgen.

Bei den Änderungen der Buchstaben b und c handelt es sich um rein terminologische Anpassungen. Im NDG wird der Begriff «menschliche Quellen» anstelle von «Informanten» verwendet. Zudem statuiert Artikel 9 NDG, welche kantonalen Behörden mit dem NDB zusammenarbeiten, und bezeichnet diese als «kantonale Vollzugsbehörden». Dieser Begriff wird in Buchstabe c übernommen.

10. Rechtshilfegesetz vom 20. März 1981[69]

Artikel 11a

Absatz 3

Der heutige Artikel 11*a* Absatz 3 des Rechtshilfegesetzes (IRSG) ist seit dem 1. Januar 2010 in Kraft und enthält noch den Verweis auf den Vollzug des BWIS durch den NDB. Die Tätigkeiten, die im heutigen Artikel unter Vollzug des BWIS durch den NDB erwähnt sind, sind heute im NDG integriert. Als das NDG verabschiedet wurde, wurde es versäumt, die entsprechende Anpassung im IRSG vorzunehmen. Die vorgeschlagene Änderung ist somit nur redaktioneller, nicht aber materieller Natur. Das Verordnungsrecht wird anschliessend angepasst.

11. Bundesgesetz vom 13. Juni 2008[70] über die polizeilichen Informationssysteme des Bundes

Artikel 15

Absatz 1 Buchstabe j

Nach Artikel 24*d* Absatz 3 BWIS werden die Ausreisebeschränkungen im RIPOL ausgeschrieben. Die gesetzliche Grundlage für das RIPOL wird im Buchstaben j ergänzt.

Artikel 18

Absatz 5 Buchstabe d

69 SR **351.1**
70 SR **361**

Mit dem neuen Absatz wird eine Grundlage für die Datenhaltung geschaffen. Die Systeme enthalten logisch getrennte Informationen und besonders schützenswerte Personendaten, die für die Sicherstellung, Beschlagnahme und Einziehung von Propagandamaterial mit zu Gewalt aufrufendem Inhalt, für die Beschlagnahme gefährlicher Gegenstände, für Ausreisebeschränkungen zur Verhinderung von Gewalt anlässlich von Sportveranstaltungen sowie gegen Gewalt anlässlich von Demonstrationen und Kundgebungen notwendig sind. Für die Zulässigkeit der Datenbearbeitung ist in Artikel 3 Absätze 2 ff. BPI gesorgt.

Absatz 6

Die Daten nach Absatz 5 Buchstabe b werden höchstens fünfzehn Jahre aufbewahrt. Die Daten nach Buchstabe c werden analog der Dauer der verfügten Massnahme aufbewahrt, da ein Einreiseverbot nach Artikel 67 Absatz 4 resp. Artikel 68 Absatz 3 AIG für eine Dauer von mehr als fünf Jahren und in schwerwiegenden Fällen unbefristet verfügt werden kann. Die Daten nach Buchstabe d werden höchstens zehn Jahre aufbewahrt.

Absatz 7

Der Zugriff auf die Systeme mittels automatisiertem Abrufverfahren ist den Mitarbeitenden des fedpol sowie dem BJ zur Erfüllung seiner Aufgaben nach dem IRSG vorbehalten. Zugriff auf die Systeme zur Bearbeitung der Daten nach Absatz 5 Buchstaben b–d haben die Mitarbeitenden des fedpol, die für die Bearbeitung entsprechender Daten zuständig sind. Details zu den Zugriffsrechten sind nicht in einem formellen Gesetz festzuhalten, sondern auf tieferer Stufe zu regeln.

Artikel 18a Beschaffung und Bearbeitung sicherheitsrelevanter Daten über Stellenbewerberinnen und Stellenbewerber und Beauftragte

Mit dem neuen Artikel 7 Absätze 1 Buchstabe e und 1bis–2 sowie Artikel 7*a* E-NDG sieht der NDB zusätzliche Massnahmen zum Schutz und zur Sicherheit seiner Mitarbeiterinnen und Mitarbeiter, seiner Einrichtungen und der von ihm bearbeiteten Daten vor (vgl. oben). Zwei dieser neuen Massnahmen, nämlich die Überprüfung von Personen im laufenden Anstellungsverfahren sowie die Überprüfung von Personen und Unternehmen, die sich um Aufträge des fedpol bewerben oder solche ausführen, benötigt das fedpol ebenso. Die vom fedpol wahrgenommenen Aufgaben erstrecken sich über das gesamte Spektrum von präventiv-polizeilichen Massnahmen zur Wahrung der inneren oder äusseren Sicherheit der Schweiz, gerichtspolizeilicher Tätigkeit in Bereichen schwerer und schwerster Kriminalität über den Betrieb polizeilicher Informationssysteme bis hin zum Schutz von Magistratspersonen und Gebäuden des Bundes sowie von völkerrechtlich geschützten Personen und Gebäuden. Die Erfüllung dieser Aufgaben stellt hohe Anforderungen an die Vertrauenswürdigkeit der Mitarbeiterinnen und Mitarbeiter. Dieser Anspruch gilt auch gegenüber Personen und Unternehmen, die sich um Aufträge des fedpol bewerben oder solche ausführen.

Das fedpol klärt bei Personen, die in der engsten Auswahl stehen, im Anstellungsverfahren bereits heute ab, ob die betroffene Person Gegenstand eines hängigen Administrativ- oder Strafverfahrens ist, ob ihr gegenüber eine entsprechende Sanktion ausgesprochen worden ist oder ob sonst strafrechtlich relevante Feststellungen vorliegen.

Diese Abklärungen erfolgen jeweils gestützt auf eine vorgängige Einwilligung der betroffenen Person im Sinne von Artikel 17 Absatz 2 Buchstabe c DSG (Abs. 3). Es hat sich in der Praxis gezeigt, dass diese Massnahme künftig systematisch durchgeführt werden muss und es hierfür einer entsprechenden Rechtsgrundlage bedarf.

Wurde keine Personensicherheitsprüfung oder kein Betriebssicherheitsverfahren durchgeführt, so kann das fedpol neu über eine Person oder ein Unternehmen, die oder das sich um Aufträge des fedpol bewirbt oder solche ausführt, entsprechende Daten beschaffen und bearbeiten.

Mit dieser inhaltlichen Erweiterung müssen sich die Überprüfungen neu auf eine spezielle formell-gesetzliche Grundlage stützen können. Sie soll mit einem neuen Artikel 18*a* BPI geschaffen werden. Dieser lehnt sich in seinem Wortlaut eng an die vom NDB vorgesehene Regelung nach Artikel 7*a* Absätze 2–4 NDG an. Mit dem Titel «Beschaffung und Bearbeitung sicherheitsrelevanter Daten über Stellenbewerberinnen und Stellenbewerber und Beauftragte» soll eine begriffliche Abgrenzung zu den «Personensicherheitsprüfungen» nach dem ISG sowie den «Vertrauenswürdigkeitsprüfungen» nach Artikel 20*b* des Bundespersonalgesetzes vom 24. März 2000[71] vorgenommen werden. Erfasst werden von diesen Überprüfungen Personen, die in der engsten Auswahl für eine Anstellung beim fedpol stehen, wobei die Überprüfung auf jeden Fall vor der Übernahme der neuen Funktion beim fedpol erfolgt sein muss (Abs. 1), sowie Personen oder Unternehmen, die sich um Aufträge des fedpol bewerben oder solche ausführen (Abs. 2).

In der Praxis sollen vor allem die folgenden im BPI geregelten Informationssysteme abgefragt werden: NES (Art. 10, 11 und 13), IPAS (Art. 12 und 14), RIPOL (Art. 15), nationaler Polizeiindex (Art. 17) und ORMA (Art. 18) sowie zusätzlich das Informationssystem HOOGAN nach Artikel 24*a* BWIS.

Wird anlässlich einer solchen Überprüfung durch das fedpol ein mutmasslich strafbares Verhalten festgestellt, so erstattet das fedpol Anzeige bei den zuständigen Strafverfolgungsbehörden.

Das fedpol verfügt über kein formelles Gesetz, das seine Aufgaben umfassend regelt, so wie es das NDG für den NDB darstellt. Es bietet sich vorliegend an, die neue Gesetzesbestimmung zur Regelung der Überprüfungen durch das fedpol im BPI einzufügen. Einerseits sind dort jene Informationssysteme geregelt, auf die sich das Amt bei diesen Überprüfungen zum grössten Teil abstützt. Andererseits findet sich im BPI mit Artikel 17 Absatz 4 Buchstabe l bereits eine andere Gesetzesbestimmung im Bereich der Personensicherheitsprüfung. Diese personalrechtliche Materie ist im BPI somit nicht gänzlich neu.

71 SR **172.220.1**

12. Militärgesetz vom 3. Februar 1995[72]

Artikel 99

Absatz 5

Infolge der Änderungen der Bestimmungen über die AB-ND im NDG muss ein Verweis angepasst werden.

13. Waffengesetz vom 20. Juni 1997[73]

Artikel 9

Absatz 2

Artikel 9 des Waffengesetzes (WG) ist seit dem 12. Dezember 2008 in Kraft. Zu diesem Zeitpunkt waren die Aufgaben des fedpol und des Inlandnachrichtendienstes im BWIS geregelt und die kantonalen Vollzugsbehörden waren für beide die gleichen. Mit dem Inkrafttreten des NDG wurden die Aufgaben der beiden Ämter gesetzlich klar getrennt. Somit kann ein Kanton eine Vollzugsbehörde für den Vollzug des BWIS und eine andere Vollzugsbehörde für den Vollzug des NDG bestimmen. Da in der Praxis die Vollzugsbehörden nach dem NDG die Stellungnahme zum Waffenerwerb abgeben, muss in Artikel 9 WG auf das NDG verwiesen werden, während der Verweis auf das BWIS nicht mehr notwendig ist.

Artikel 32c

Absatz 7

Der Zugriff auf das gemeinsame harmonisierte Informationssystem (ARMADA) nach Artikel 32a Absatz 3 WG soll dem NDB eine bessere Einschätzung des Bedrohungspotenzials einer Person durch Hinweise auf den Besitz oder den Entzug einer Waffe oder die Verweigerung eines Waffenerwerbsgesuchs ermöglichen. Vor dem Hintergrund verschiedener rechtsextremistisch motivierter Terroranschläge (z. B. Christchurch / Hanau) ist das Thema noch wichtiger geworden. Zudem ist bekannt, dass Personen aus dem salafistischen oder gewaltbereiten islamistischen Umfeld versuchen, sich zu bewaffnen. Zeitnahe Abklärungen sind zwingend notwendig, um eine seriöse Einschätzung der Bedrohung der inneren oder äusseren Sicherheit zu tätigen.

Tritt diese Vorlage vor dem BAZG-VG in Kraft, so ist die im BAZG-VG vorgesehene Änderung dieser Bestimmung hinfällig.

72 SR **510.10**
73 SR **514.54**

14. Strassenverkehrsgesetz vom 19. Dezember 1958[74]

Artikel 89e

*Buchstabe a^bis^*

Mit der Teilinkraftsetzung der Änderung vom 15. Juni 2012 des Strassenverkehrsgesetzes vom 19. Dezember 1958 (SVG) am 1. Januar 2019[75] wurden die mit Inkrafttreten des NDG teilweise neu verankerten Zugriffe des NDB im Abrufverfahren auf die Systeme des Bundesamts für Strassen, die durch das neue Informationssystem Verkehrszulassung ersetzt wurden, irrtümlicherweise gestrichen. Hier handelt es sich um ein gesetzgeberisches Versehen, welches mit der vorliegenden Ergänzung korrigiert wird.

15. Bundesgesetz vom 18. März 2016[76] betreffend die Überwachung des Post- und Fernmeldeverkehrs

Artikel 14 Übermittlung der Überwachungsdaten an das fedpol

Verschiedene redaktionelle Anpassungen werden in dieser Bestimmung vorgenommen, damit sie mit der Formulierung des analogen Artikels 14*a* übereinstimmt. Materiell bleibt der Artikel unverändert. Die im Verarbeitungssystem des Diensts ÜPF enthaltenen Daten sind in Artikel 8 BÜPF aufgeführt und enthalten auch Angaben über Fernmeldedienste (Art. 8 Bst. c BÜPF), also die Auskünfte (Art. 7 Bst. c BÜPF).

Absatz 1

Die Übermittlung der Daten vom Dienst ÜPF an das fedpol erfolgt über das Verarbeitungssystem des Diensts ÜPF weiterhin im Abrufverfahren. Wie bisher darf nach Buchtstabe a der Datentransfer nur durchgeführt werden, wenn das fedpol nach dem anwendbaren Recht zur entsprechenden Datenbearbeitung berechtigt ist. Zudem dürfen nach Buchstabe b nur die Personen Daten bearbeiten, die diese Daten für ihre berufliche Aufgabenerfüllung benötigen. Die Zugriffe sind in den Bestimmungen der verschiedenen Systeme des BPI geregelt (Art. 10 Abs. 4, 12 Abs. 6, 13 Abs. 3 und 18 Abs. 7 BPI). Dabei wird es sich vor allem um die Auswertung von Informationen im Rahmen von Strafuntersuchungen sowie präventiv-polizeilicher Massnahmen zur Abwehr von terroristischen Gefahren handeln. Die Verweise auf das BPI werden von Absatz 1 in Absatz 2 verschoben. Der geltende Absatz 2 wird aufgehoben, da das fedpol nur zur Bearbeitung von Daten aus dem Verarbeitungssystem berechtigt ist, wenn die entsprechende Person über Zugriffsrechte auf das Verarbeitungssystem und auf die Daten beim fedpol verfügt. Somit ist der geltende Absatz 2 in Absatz 1 Buchstabe a dieser Bestimmung enthalten.

Absatz 2

74 SR **741.01**
75 AS **2018** 4985
76 SR **780.1**

Die Artikel 10, 12 und 13 BPI werden mit Artikel 18 BPI ergänzt. Bei Letzteren handelt es sich um die Geschäfts- und Aktenverwaltungssysteme des fedpol. Artikel 18 BPI ist seit dem 1. Juni 2022 in Kraft und wurde mit dem Bundesgesetz vom 25. September 2020[77] über polizeiliche Massnahmen zur Bekämpfung von Terrorismus eingeführt. Das Verb «kopiert» wird durch «abspeichern und kennzeichnen» ersetzt, was wie bisher die Vervielfältigung der Daten aus dem Verarbeitungssystem durch die Strafverfolgungsbehörde ermöglichen soll.

Artikel 14a Übermittlung der Überwachungsdaten an den NDB

Wie bei Artikel 14 werden in dieser Bestimmung redaktionelle Änderungen vorgenommen. Neu werden nur noch Daten erwähnt, da der NDB keine unterschiedlichen Informationssysteme mehr hat. Die im Verarbeitungssystem enthaltenen Daten sind in Artikel 8 BÜPF beschrieben und enthalten auch die Angaben über Fernmeldedienste (Art. 8 Bst. c BÜPF), also die Auskünfte (Art. 7 Bst. c BÜPF). Materiell bleibt auch dieser Artikel unverändert. Die Erläuterungen zu Artikel 14 gelten sinngemäss für den NDB. Analog zu Artikel 14 Absatz 2 wird in Absatz 2 klargestellt, dass die Daten aus dem Verarbeitungssystem des Diensts ÜPF als Daten aus GEBM nach Artikel 49 Buchstabe c NDG abgespeichert und kennzeichnet werden. Diese Formulierung ersetzt das Verb «kopiert werden» im geltenden Absatz 1.

Artikel 15

Absatz 1 Buchstabe b

In dieser Bestimmung muss die in Artikel 14 eingeführte Bezeichnung «fedpol» verwendet werden.

Artikel 21

Absatz 3

Die Polizeibehörden und der NDB sind zur Erfüllung ihrer gesetzlichen Aufgaben bisweilen darauf angewiesen, fernmeldetechnische Zugangsmittel (z. B. Prepaid SIM-Karten) und Dienste einsetzen zu können, bei welchen diese Behörden und ihre Mitarbeiterinnen und Mitarbeiter weder in den Verzeichnissen noch in den Systemen der Anbieterinnen von Fernmeldediensten und des Diensts ÜPF erscheinen. Sie brauchen solche Zugangsmittel namentlich zum Schutz ihrer Mitarbeiterinnen und Mitarbeiter, ihrer Kontakte und Quellen, aber auch ihrer technischen Methoden und Fähigkeiten (z. B. bei der Kommunikation während Observationen von Personen mit Zugang zu fortgeschrittenen technischen Mitteln z. B. in Kreisen der organisierten Kriminalität oder der Spionage).

Der speziellen Schutzmassnahmen bedürfen diejenigen Mitarbeiterinnen und Mitarbeiter der Polizeibehörden und des NDB, die ihre gesetzlichen Aufgaben unter Verwendung ihrer wahren Identität erfüllen, also ohne den Schutz durch eine Tarnidentität. Mitarbeiterinnen und Mitarbeiter mit einer solchen Tarnidentität (verdeckte

77 AS **2021** 565, **2022** 300; BBl **2019** 4751

Ermittlerinnen und Ermittler nach Art. 285*a* StPO und mit einer Tarnidentität ausgestattete Personen nach den Art. 17 und 18 NDG) können fernmeldetechnische Zugangsmittel unter Verwendung dieser Tarnidentität nach dem normalen Verfahren erwerben, ohne ihre wahre Identität offenlegen zu müssen, und sind dadurch ausreichend geschützt.

Mit dem neuen Absatz 3 soll die gesetzliche Grundlage geschaffen werden, dass die Anbieterinnen von Fernmeldediensten zwar die Kenntnis haben, dass berechtigte Behörden Teilnehmende von bestimmten geschützten Zugangsmitteln und Diensten sind, aber diese Daten bestmöglich schützen und nur berechtigten Behörden auf Anfrage über den Dienst ÜPF bekannt geben. Die Anbieterinnen von Fernmeldediensten erfüllen damit alle ihre Pflichten betreffend die Identifikation der Teilnehmenden und der Auskunftserteilung an berechtigte Behörden, verhindern aber eine Kenntnisnahme durch potenzielle Kriminelle und schützen so die operativen Tätigkeiten von Polizeibehörden und des NDB. Dabei können die Anbieterinnen von Fernmeldediensten verpflichtet werden, geeignete Methoden zu treffen, um eine weitere Verbreitung der Daten zu verhindern. Bei den Anbieterinnen von Fernmeldediensten hat heute eine grosse und nicht kontrollierbare Anzahl Personen Zugriff auf deren Systeme und somit auf die Daten, die zur Erteilung der Auskünfte gespeichert werden. Nicht alle Anbieterinnen von Fernmeldediensten können deshalb heute mit ihren Systemen sicherstellen, dass diese nicht durch Kriminelle ausgenützt werden, um beispielsweise verdeckte Fahnder zu identifizieren und deren Aufgabe zu gefährden. Deshalb ist es nötig, dass die Anbieterinnen von Fernmeldediensten verpflichtet werden können, technische Lösungen zu implementieren oder Methoden zu finden, um diesen Schutz zu gewährleisten. Diese Massnahmen zur Gewährleistung der Vertraulichkeit können auch herangezogen werden, um exponierte Personen wie Bundesrätinnen und Bundesräte oder bestimmte Politikerinnen und Politiker zu schützen.

Artikel 33

Absatz 4

Nach Artikel 33 Absatz 4 BÜPF erhebt der Dienst ÜPF von den Anbieterinnen von Fernmeldediensten eine Gebühr für den Überprüfungsaufwand. Diese Bestimmung hat sich in der Praxis nicht bewährt. In den meisten Fällen kann der Überprüfungsaufwand kaum ohne grossen administrativen Aufwand nachgewiesen werden.

Bei bedeutenden Anbieterinnen von Fernmeldediensten muss das Überprüfungsverfahren kontinuierlich wiederholt werden, da viele ihrer Dienste einer ständigen technologischen Weiterentwicklung unterliegen. Ohne Abschluss des Verfahrens ist es allerdings schwierig, den Überprüfungsaufwand zu benennen. In der Praxis konnte einzig kleinen und mittleren Unternehmen (sog. KMU) der Überprüfungsaufwand in Rechnung gestellt werden, bei welchen das Verfahren abgeschlossen werden konnte, da ihre Dienste weniger stark von der technologischen Weiterentwicklung betroffen sind. Es erscheint nicht angebracht, den Überprüfungsaufwand einzig den KMU in Rechnung zu stellen. Dies entspricht auch dem Postulat Vitali vom 16. September 2019 (19.4031 «Für ein verhältnismässiges Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs»), das fordert, die rechtlichen Grundlagen im

BÜPF «KMU-freundlicher» zu gestalten. Der administrative Aufwand zur Erbringung des Nachweises über den geleisteten Überprüfungsaufwand übersteigt ausserdem meist die in Rechnung gestellte Gebühr. Durch die Streichung dieser Gebühr entfällt einerseits der administrative Aufwand für den Dienst ÜPF, der mit der Erstellung des Nachweisattests und der Rechnungstellung verbunden war. Andererseits sind die Anbieterinnen von Fernmeldediensten, insbesondere die KMU, künftig von der Pauschalgebühr von 500 Franken pro geprüften Dienst entlastet. Dabei ist zu berücksichtigen, dass es sich bei dieser Gebühr um keinen nennenswerten Betrag handelt und sie zudem nur sehr selten in Rechnung gestellt wurde. Aus diesen Gründen erscheint der Verzicht auf die Erhebung dieser Gebühr sowohl aus administrativer als auch aus finanzieller Sicht sinnvoll. Artikel 33 Absatz 4 BÜPF ist deshalb aufzuheben.

Artikel 39

Absatz 4

Wie in Artikel 83*c* NDG soll auch in Artikel 39 BÜPF die Regelung von Artikel 7 VStrR für Bussen von höchstens 20 000 Franken zur Anwendung kommen. Mit dieser Änderung wird für Bagatellfälle die Möglichkeit geschaffen, bei durch natürliche Personen begangenen Übertretungen das Unternehmen (juristische Person, Kollektiv- oder Kommanditgesellschaft oder Einzelfirma) zur Bezahlung einer Busse zu verurteilen. Damit kann die Behörde unverhältnismässigen Untersuchungsaufwand vermeiden. Wie in Artikel 83*c* NDG und in Artikel 89 des Bundesgesetzes vom 15. Dezember 2000[78] über Arzneimittel und Medizinprodukte wird der Betrag der Busse auf höchstens 20 000 Franken festgesetzt (anstelle von 5000 Franken wie im geltenden Art. 7 VStrR).

16.–22.

Im NDG wird der Ausdruck «kantonale Vollzugsbehörden» verwendet, was in diesen Erlassen übernommen wird.

23. Vorläuferstoffegesetz vom 25. September 2020[79]

Artikel 18

Absatz 1

Wie bereits mehrfach erwähnt, werden mit dem Revisionsentwurf nicht mehr Informationssysteme geregelt, sondern die Datenbearbeitung. Deshalb wird in Artikel 18 Absatz 1 Buchstabe h der Begriff «INDEX NDB» durch «Daten nach Artikel 49 Buchstabe j NDG» ersetzt.

78 SR **812.21**
79 SR **941.42**

6 Auswirkungen

6.1 Auswirkungen auf den Bund

Die AB-ND kann den zusätzlichen Aufwand für die Übernahme der Aufgaben der UKI dank Effizienzsteigerungen, die durch die Konsolidierung ihrer Organisation und von Tätigkeiten erreicht werden konnten, kompensieren. Der Transfer der Aufgaben der UKI zur AB-ND führt somit zu einer Reduktion um die bisher für die UKI eingesetzten Ressourcen der Bundesverwaltung (3 Mitglieder und 1 Sekretärin oder Sekretär innerhalb der Bundesverwaltung, die einen Teil ihres Pensums für die UKI leisten).

Mit der allgemeinen Verschlechterung der sicherheitspolitischen Lage einerseits und der Ausweitung des Anwendungsbereichs der GEBM auf den gewalttätigen Extremismus sowie die Möglichkeit der Überwachung von Beziehungen zwischen Personen und Finanzintermediären nach dem GwG andererseits ist eine Erhöhung der operativen Fälle zu erwarten (vgl. auch die Ausführungen zu Art. 27 E-NDG). Die effiziente, bedrohungsgerechte und durchhaltefähige Bearbeitung dieser Zusatzfälle erfordert mehr Personalressourcen beim NDB. Der geschätzte personelle Mehrbedarf beläuft sich dabei auf zwei Operationsteams sowie die entsprechenden Mitarbeitenden in Querschnitts- und Unterstützungsfunktionen (wie Rechtsberatung, Personalführung, Informatikdienstleistungen oder operative Sicherheit, was durchschnittlich 25 % des Bedarfs an operativem Personal entspricht). Jedes Operationsteam besteht grundsätzlich aus einer Operationsführerin oder einem Operationsführer, einer operativen Mitarbeiterin oder einem operativen Mitarbeiter, einer Auswerterin oder einem Auswerter, sowie einer Datenanalystin oder einem Datenanalysten. Somit beziffert sich der Mehrbedarf an Personalressourcen beim NDB auf 10 Vollzeitstellen (FTE), namentlich 8 Stellen in operativer und 2 Stellen in unterstützender Funktion. Die personellen Mehrausgaben für 10 FTE entsprechen 1,8 Millionen Franken jährlichen Kosten, die zusätzlichen Sachausgaben 520 000 Franken (Berechnung auf Basis von Standardwerten). Dazu kämen noch Arbeitsplatzkosten, deren Umfang von der konkreten Lösung abhängt (zusätzliche Büroräume oder Unterbringung in bestehenden Bundesliegenschaften).

Die neuen Aufgaben nach dem BWIS führen beim fedpol zu Mehraufwand. Die Anzahl der zu erlassenden Verfügungen im Bereich der Ausreisebeschränkungen zur Verhinderung von Gewalt anlässlich von Demonstrationen und Kundgebungen lässt sich nicht abschätzen. Im Gegensatz zu den bereits bestehenden Ausreisebeschränkungen zur Verhinderung von Gewalt anlässlich von Sportveranstaltungen, bei denen sich die relevanten internationalen Sportveranstaltungen jeweils im ungefähr gleichen Rahmen bewegen, lässt sich die Anzahl relevanter Demonstrationen und Kundgebungen im Ausland, die das Interesse von potenziell betroffenen Personen in der Schweiz wecken, nicht vorhersagen. Die Sicherheitslage ist dynamischen Prozessen unterworfen, die schwer vorhersehbar sind. Der Aufwand für den Erlass einer Ausreisebeschränkung zur Verhinderung von Gewalt anlässlich von Demonstrationen und Kundgebungen ist zudem nicht vergleichbar mit dem im Bereich der Sportveranstaltungen. Bei Verfügungen gegen Gewalt anlässlich von Sportveranstaltungen handelt es sich oftmals um Massenverfügungen, bei denen sich der Sachverhalt jeweils analog präsentiert, der Sachverhalt leichter erstellbar ist und die entsprechenden Nachweise bei

klar definierten Kontaktstellen kantonaler Behörden schneller einholbar sind. Bei Ausreisebeschränkungen für Demonstrationen und Kundgebungen handelt es sich hingegen in jedem Fall um Verfügungen, bei denen eine umsichtige Abwägung öffentlicher versus privater Interessen erforderlich ist. Ausgenommen davon sind Verfügungen, die wegen Gefahr im Verzug erlassen werden müssen. Die Absicht zur Gewaltausübung und Reiseabsicht lassen sich im Unterschied zu Verfügungen betreffend die Verhinderung von Gewalt anlässlich von Sportveranstaltungen nicht aufgrund einer Zugehörigkeit einer Fangruppierung nachweisen und es besteht keine nationale Datenbank analog dem System HOOGAN nach Artikel 24*a* BWIS über bisheriges gewalttätiges Verhalten von Betroffenen. Die entsprechenden Nachweise sind vielmehr jeweils amtshilfeweise bei verschiedenen Behörden einzuholen, was den Einsatz von grösseren Ressourcen erfordert. Schliesslich dürfte eine Ausreisebeschränkung, die in die politische Meinungsäusserungsfreiheit eingreift, eine ausführlichere Begründungsdichte erfordern als eine Massnahme zur Verhinderung der Teilnahme an einer Sportveranstaltung, welche – wenn nicht vor Ort – zumindest am Fernseher oder über anderweitige Medien mitverfolgt werden kann. Der Aufwand pro Verfügung dürfte sich auf nicht weniger als zehn Arbeitstage belaufen. Bei einer Beschwerde käme ein zusätzlicher Aufwand von vier bis fünf Tagen hinzu. Sollte der gesamte Rechtsmittelweg ausgeschöpft werden, ist mit Aufwänden von bis zu fünfzehn Arbeitstagen zur rechnen. Schliesslich ist darauf hinzuweisen, dass es sich um präventiv-polizeiliche Massnahmen zur Gefahrenabwehr handelt, deren Erledigung je nach Fallkonstellation keinen Aufschub duldet. Die neue Aufgabe wird für Fedpol also zu einem erheblichen Mehraufwand führen. Dieser kann mit den bestehenden Ressourcen des fedpol nicht bestritten und aufgrund des fachspezifischen Profils auch nicht durch fedpol-interne Verschiebungen von Personalressourcen aufgefangen werden. Aus diesem Grund bedarf es zur Umsetzung der neuen Massnahme 2 FTE.

Bei Fedpol entsprechen die erläuterten personellen Mehrausgaben für 2 FTE 360 000 Franken jährlichen Kosten. Die zusätzlichen Sachausgaben belaufen sich auf insgesamt 160 000 Franken pro Jahr. Sie setzen sich aus dem Anspruch auf unentgeltliche Rechtspflege mit jährlich geschätzten 60 000 Franken und zusätzlichen für die Fallführung und -analyse benötigten IT-Mitteln von 100 000 Franken zusammen.

Insgesamt führt die Vorlage also zu personellen Mehrausgaben von 2,16 Millionen Franken jährlichen Kosten (12 FTE) und zu zusätzlichen Sachausgaben von 680 000 Franken (sowie noch nicht bezifferbaren Arbeitsplatzkosten, siehe dazu oben).

6.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Die neuen Ausreisebeschränkungen nach dem BWIS können bei den Kantonen zu zusätzlichem Aufwand führen, weil sie ihre Anträge gegenüber dem fedpol begründen müssen.

Die Vorlage hat keine spezifischen Auswirkungen auf Gemeinden, urbane Zentren, Agglomerationen und Berggebiete hat. Die entsprechenden Fragen wurden daher nicht vertieft untersucht.

6.3 Auswirkungen auf die Volkswirtschaft

Vereinzelt könnten bei gewerbsmässigen Betreiberinnen von Beherbergungsbetrieben sowie bei Banken, Händlerinnen und Händlern oder Finanzintermediären nach dem GwG Aufwände entstehen, weil sie neu verpflichtet sind, dem NDB auf Anfrage hin Auskünfte zu erteilen oder Daten zu liefern.

Zudem können auch Kosten bei den Fernmeldedienstanbieterinnen entstehen. Diese werden aber in der Regel nach dem BÜPF bzw. den dazugehörigen Verordnungen entschädigt.

Direkte Auswirkungen auf weitere volkswirtschaftliche Gruppen oder auf die Gesamtwirtschaft sind keine ersichtlich. Indirekt werden durch ein sicheres und gesellschaftlich stabiles Umfeld die wirtschaftlichen Rahmenbedingungen verbessert, was den Standort Schweiz stärkt. Da die Auswirkungen auf den Bund wie dargelegt gering sind, konnte wie in Ziffer 4.2 ausgeführt auf eine Regulierungsfolgeabschätzung verzichtet werden.

6.4 Auswirkungen auf die Gesellschaft

Belastende Auswirkungen auf die Gesellschaft sind nicht zu erwarten.

Die Einführung einer Ausreisebeschränkung bei Gewalt anlässlich von Demonstrationen und Kundgebungen im BWIS leistet einen Beitrag an die öffentliche Sicherheit im In- und Ausland, indem verhindert wird, dass sich in der Schweiz ansässige Personen an gewalttätig-extremistischen Aktivitäten im Ausland beteiligen. Sie hat ausserdem, wie auch die im NDG vorgesehene Ausweitung des Anwendungsbereichs der GEBM auf gewalttätigen Extremismus, einen präventiven Schutzeffekt insbesondere auf jüngere Personen, die sich in einer gewalttätig-extremistischen Szene befinden und damit einem gewaltbereiten und gewalttätigen Umfeld ausgesetzt sind.

Indirekt wirken sich die – aufgrund der Gesamtheit der in der Vorlage vorgeschlagenen Änderungen – verbesserte Sicherheitslage und ein stabiles Umfeld positiv auf das individuelle und kollektive Sicherheitsempfinden und damit auf die Gesellschaft aus.

6.5 Auswirkungen auf die Umwelt

Belastende Auswirkungen auf die Umwelt sind nicht zu erwarten.

6.6 Andere Auswirkungen

Die geplanten Änderungen führen zu einer verbesserten und effizienteren Leistungserbringung im nachrichtendienstlichen Bereich, was sich positiv auf die internationale Zusammenarbeit auswirken und das internationale Ansehen der Schweiz nachhaltig entsprechend beeinflussen dürfte.

7 Rechtliche Aspekte

7.1 Verfassungsmässigkeit

Das NDG stützt sich auf Artikel 54 Absatz 1 BV für den Bereich der äusseren Sicherheit der Schweiz und für den Bereich Staatsschutz im Inland auf die inhärente Kompetenz des Bundes, die notwendigen Massnahmen zu seinem Schutz und zum Schutz seiner Organe und Institutionen zu treffen (für die im Ingress stellvertretend Artikel 173 Absatz 2 BV genannt wird). Die Befugnis des Bundes zur Gesetzgebung auf dem Gebiet des Strafrechts stützt sich auf Artikel 123 Absatz 1 BV, so auch für die neu im NDG vorgesehenen Strafbestimmungen der Artikel 83*a*–83*d*, in welche die heute in Artikel 74 NDG verankerte Strafbestimmung aufgenommen wird.

Im gleichen Rahmen bewegt sich auch die vorliegende Gesetzesrevision. Sie überschreitet die Grenzen der genannten Kompetenzen nicht.

Die Vorlage enthält zudem zur Umsetzung der Motion Rieder vom 28. September 2017 (17.3862 «Ausreisesperren für potenzielle Gewaltextremisten») Regelungen, die das Polizeirecht des Bundes punktuell ergänzen. Es handelt sich um eine Ausreisebeschränkung, mit welcher verhindert werden soll, dass sich Personen an Gewaltakten im Zusammenhang mit Demonstrationen oder Kundgebungen im Ausland beteiligen. Für den Bereich der auswärtigen Angelegenheiten verfügt der Bund mit Artikel 54 Absatz 1 BV über eine umfassende Rechtsetzungskompetenz.

Der Bundesrat stützt sich folglich auf eine ausreichende Verfassungsgrundlage. Detailliertere Ausführungen dazu finden sich in der Botschaft zum Nachrichtendienstgesetz. [80]

Die vorgeschlagenen Änderungen erlauben Grundrechtseinschränkungen, insbesondere Einschränkungen des Grundrechts auf Schutz der Privatsphäre und der informationellen Selbstbestimmung nach Artikel 13 BV und die persönliche Freiheit nach Artikel 10 BV (vgl. die nachfolgenden Hinweise zu den einzelnen Bestimmungen der Vorlage). Nach Artikel 36 BV erfordert die Zulässigkeit von Grundrechtseinschränkungen, dass diese gesetzlich vorgesehen sind und durch ein öffentliches Interesse oder durch den Schutz der Grundrechte Dritter gerechtfertigt werden sowie dass dabei der Grundsatz der Verhältnismässigkeit und der Kerngehalt der Grundrechte gewahrt bleiben.

80 BBl **2014** 2105 S. 2228

In Bezug auf die für schwere Grundrechtseingriffe erforderliche gesetzliche Grundlage sind die Voraussetzungen mit dem Erlass eines formellen Bundesgesetzes erfüllt. Die vorgesehenen Bestimmungen genügen auch dem Bestimmtheitsgebot.

Artikel 5 Absatz 6

Die vorgesehene Ausweitung der Beschaffung und Bearbeitung von Daten, welche die politische Betätigung oder die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit betreffen, ist mit einem verstärkten Eingriff in diese Grundrechte verbunden. Für die Verhältnismässigkeit dieser Ausweitung wird auf die Erläuterungen zu dieser Bestimmung verwiesen.

Artikel 6 Absatz 1 Buchstabe b, Artikel 19 Absatz 2 Buchstabe f und Artikel 39 Absatz 1

Durch die vorgesehene Ausweitung des Aufgabenbereichs des NDB auf politisch bedeutsame Vorgänge im Cyberraum ergeben sich gegenüber dem geltenden Recht zusätzliche Sachverhalte, die Beschaffungsmassnahmen ermöglichen, die in die Grundrechte betroffener Personen, insbesondere in das Recht auf Schutz der Privatsphäre und informationelle Selbstbestimmung (Art. 13 BV), eingreifen. Das praktische Bedürfnis und die Verhältnismässigkeit dieser Erweiterung nachrichtendienstlicher Tätigkeit wird in den Erläuterungen zu Artikel 6 dargelegt. Zudem ist die Verhältnismässigkeit einer Beschaffungsmassnahme jeweils im konkreten Anwendungsfall zu prüfen.

Artikel 7 und 7a

Die neuen Bestimmungen über die Auswertung der Nutzung von Daten und Geräten des NDB durch die Mitarbeiterinnen und Mitarbeiter sowie betreffend Einholung von Informationen über Mitarbeiterinnen und Mitarbeiter, Stellenbewerberinnen und Stellenbewerber sowie Beauftragte des NDB sind mit Eingriffen in deren Grundrecht auf Privatsphäre und informationelle Selbstbestimmung (Art. 13 BV) verbunden. Für die Verhältnismässigkeit dieser Ausweitung wird auf die Erläuterungen zu diesen Bestimmungen verwiesen.

Artikel 14 Absatz 3

Mit der vorgeschlagenen Änderung, wonach im Rahmen von Observationen Ortungsgeräte ohne gerichtliche Genehmigung eingesetzt werden dürfen, ist gegenüber dem geltenden Recht ein stärkerer Eingriff in das Recht auf Schutz der Privatsphäre (Art. 13 BV) verbunden. Zur Grundrechtskonformität dieser Massnahme wird im Einzelnen auf die Erläuterungen zu dieser Bestimmung verwiesen.

Artikel 25 Absatz 1 Buchstabe a

Die Ausdehnung der Auskunftspflicht Privater auf Beherbergungsbetriebe und gewerbsmässige Betreiberinnen und Betreiber von Transportinfrastrukturen kann das Grundrecht betroffener Personen auf ihre Privatsphäre nach Artikel 13 BV einschränken. Die Anpassung der Bestimmung liegt aber im öffentlichen Interesse, da solche Auskünfte für das frühzeitige Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit wichtig und erforderlich sein können, insbesondere um Reisebewegungen von Zielpersonen in den Bereichen Terrorismus, gewalttätiger Extremismus und verbotener Nachrichtendienst festzustellen. Weitere Hinweise zur Verhältnismässigkeit können den Erläuterungen zu dieser Bestimmung entnommen werden.

Artikel 26 Absatz 1 Buchstaben f und g

Beim Einsatz von GEBM kann es zu schwerwiegenden Grundrechtseingriffen kommen. Dies gilt auch für die mit dieser Vorlage neu vorgesehenen Massnahmen nach Artikel 26 Absatz 1 Buchstaben f und g (Einholen von Auskünften bei Finanzintermediären). Betroffen sind dabei die oben genannten Grundrechte nach Artikel 13 BV.

GEBM können nur angeordnet werden, wenn eine konkrete Bedrohung oder die Wahrung weiterer wichtiger Landesinteressen dies erfordern, die Schwere der Bedrohung die Massnahme rechtfertigen und andere nachrichtendienstliche Abklärungen bisher erfolglos geblieben sind, sonst aussichtslos wären oder unverhältnismässig erschwert würden. Das Vorliegen dieser Voraussetzungen wird vorgängig richterlich (Bundesverwaltungsgericht) geprüft und genehmigt. Anschliessend muss zusätzlich eine politische Freigabe erfolgen (Vorsteherin oder Vorsteher VBS nach vorheriger Konsultation der Vorsteherin oder des Vorstehers von EDA und EJPD). Nach Abschluss der Operation werden den überwachten Personen der Grund, die Art und die Dauer der Überwachung mit GEBM mitgeteilt. Unter besonderen Umständen kann zwar ein Verzicht auf diese Mitteilung oder ein Aufschub derselben erfolgen, aber auch dies braucht eine richterliche Genehmigung. Gegen die Mitteilung resp. gegen die Anordnung der GEBM kann wiederum Beschwerde beim Bundesverwaltungsgericht erhoben werden, mit Weiterzugsmöglichkeit ans Bundesgericht.

Die Aspekte des öffentlichen Interesses und der Verhältnismässigkeit können den Erläuterungen zu dieser Bestimmung entnommen werden.

Artikel 27 Absatz 1

Die vorgesehene Anpassung erweitert den Anwendungsbereich von GEBM auf Bedrohungen der inneren oder äusseren Sicherheit der Schweiz, die von gewalttätigem Extremismus oder sicherheitspolitisch bedeutsamen Vorgängen im Ausland oder im Cyberraum ausgehen, sowie auf Bedrohungen wichtiger internationaler Sicherheitsinteressen. Dies kann sowohl das Grundrecht Betroffener nach Artikel 10 BV als auch nach Artikel 13 BV einschränken. Die Erläuterungen zu dieser Bestimmung weiter oben enthalten ausführliche Ausführungen dazu, weshalb sowohl das öffentliche Interesse an dieser Erweiterung als auch deren Verhältnismässigkeit gegeben sind.

Massnahmen nach BWIS

Weitere Grundrechtseingriffe können im Zusammenhang mit den Massnahmen gegen Gewalttätigkeiten an Demonstrationen und Kundgebungen stattfinden. Artikel 24*d* E-BWIS sieht neu vor, dass das fedpol einer Person die Ausreise aus der Schweiz in ein bestimmtes Land untersagen kann, wenn nachgewiesen ist, dass sie sich in der Vergangenheit an Gewalttätigkeiten beteiligt hat und angenommen wird, dass sie sich künftig an einer Demonstration oder Kundgebung im Ausland an Gewalttätigkeiten beteiligt. Eine Ausreisebeschränkung nach Artikel 24*d* E-BWIS stellt einen Eingriff in die verfassungsrechtlich verankerte Bewegungsfreiheit (Art. 10 Abs. 2 BV) sowie die Niederlassungsfreiheit (Art. 24 Abs. 2 BV) dar. Des Weiteren wird je nach den Umständen des Einzelfalls ein Eingriff in die Versammlungsfreiheit (Art. 23 BV) sowie in die Meinungs- und Informationsfreiheit (Art. 16 BV) vorliegen.

Der Eingriff beschneidet die betroffene Person während der Dauer der angeordneten Ausreisebeschränkung in ihrer Freiheit. Das begründet grundsätzlich ein privates Interesse, dass auf die präventiv-polizeiliche Massnahme verzichtet wird. Die Bestimmung wurde auf eine Weise konzipiert, mit der das Verhältnismässigkeitsprinzip gewahrt bleibt. Es können lediglich Personen mit einer Ausreisebeschränkung belegt werden, die bereits gewalttätig in Erscheinung getreten sind. Damit hat die Massnahme zum Ziel, die wiederholte Gewaltanwendung zu verhindern. Grund- und Menschenrechte werden missbraucht, wenn sie angerufen werden, um die demokratische und rechtsstaatliche Grundordnung gewaltsam zu bekämpfen. Das soll über die neue Massnahme verhindert werden. Die Dauer einer Ausreisebeschränkung ist von Gesetzes wegen kurzgehalten. Die Ausreisebeschränkung beginnt frühestens drei Tage vor der Veranstaltung und dauert längstens bis einen Tag nach deren Ende (Art. 24*e* E-BWIS). Der Grundrechtseingriff kann demnach lediglich so lange erfolgen, wie dieser zwingend erforderlich ist. Ausnahmen zur Ausreisebeschränkung sind gesetzlich vorgesehen (Art. 24*d* Abs. 2 E-BWIS). Sie können vom fedpol bewilligt werden, wenn die betreffende Person wichtige Gründe für den Aufenthalt im Bestimmungsland geltend macht. Schliesslich steht es jeder von einer Ausreisebeschränkung betroffenen Person zu, Beschwerde gegen die präventiv-polizeiliche Massnahme vor einem unabhängigen Gericht (Bundesverwaltungsgericht, danach Bundesgericht) zu erheben (Art. 24*g* E-BWIS). Vor der Anordnung einer Ausreisebeschränkung ist jeweils im Einzelfall zu prüfen, ob die Anordnung einer Ausreisebeschränkung geeignet und erforderlich ist sowie ob das öffentliche Interesse der Verhinderung von Gewalt anlässlich von Demonstrationen und Kundgebungen das private Interesse der Teilnahme überwiegt. Eine Ausreisebeschränkung kann demnach in der rechtsanwendenden Praxis verhältnismässig umgesetzt werden. Die vorliegende gesetzliche Ausgestaltung der neu einzuführenden Ausreisebeschränkungen berücksichtigt die verfassungsmässigen Vorgaben zur Wahrung der Grund- und Menschenrechte.

Massnahmen nach dem AIG

Die Vorbereitungshaft für Personen mit Kurzaufenthalts-, Aufenthalts- oder Niederlassungsbewilligung während der Durchführung eines Ausweisungsverfahrens bei Gefährdung der inneren oder äusseren Sicherheit bedeutet einen schweren Eingriff in

die persönliche Freiheit der betroffenen Personen (Art. 10 Abs. 2 BV). Hinsichtlich des öffentlichen Interesses an dieser Massnahme und ihrer Verhältnismässigkeit wird auf die Erläuterungen zu Artikel 75 Absatz 3 AIG verwiesen.

Massnahmen nach dem BPI

Die neuen Bestimmungen betreffend die Einholung und Bearbeitung von Informationen über Stellenbewerberinnen und Stellenbewerber sowie Beauftragte des fedpol sind mit Eingriffen in deren Grundrecht auf Privatsphäre und informationelle Selbstbestimmung (Art. 13 BV) verbunden. Hinsichtlich des öffentlichen Interesses an dieser Massnahme und ihrer Verhältnismässigkeit wird auf die Erläuterungen zu Artikel 18*a* BPI verwiesen.

Die in dieser Vorlage vorgeschlagenen Neuerungen sind namentlich auch unter Berücksichtigung des vorgesehenen Erlasses auf dem Weg der ordentlichen Gesetzgebung verfassungskonform; die rechtsstaatlichen Prinzipien werden eingehalten.

7.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Von der Vorlage betroffen sind die EMRK, der internationale Pakt über bürgerliche und politische Rechte[81] (UNO-Pakt II), das FZA und das EFTA-Übereinkommen sowie das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[82] (Datenschutzkonvention 108+[83]). Insbesondere betroffen sind der Schutz der Privatsphäre (Art. 8 EMRK; Art. 17 UNO-Pakt II), die Bewegungsfreiheit und für Personen mit Schweizer Bürgerrecht, ebenfalls die Niederlassungsfreiheit (Art. 12 UNO-Pakt II), die Meinungsäusserungs- und Versammlungsfreiheit (Art. 10 und 11 EMRK; Art. 19 UNO-Pakt II) sowie das Recht auf eine wirksame Beschwerde (Art. 13 EMRK; Art. 14 UNO-Pakt II).

Die Vorlage steht sowohl in Bezug auf ihre allgemeine Zielrichtung wie auch hinsichtlich der einzelnen Bestimmungen im Einklang mit der EMRK und dem UNO-Pakt II. Gemäss der EMRK kann die Ausübung grundlegender Rechte (wie beispielsweise die Achtung des Privat- und Familienlebens nach Art. 8 oder die Versammlungsfreiheit nach Art. 11 EMRK) eingeschränkt werden, wenn die Einschränkung gesetzlich vorgesehen ist, ein legitimes Ziel verfolgt und in einer demokratischen Gesellschaft notwendig ist.

81 SR **0.103.2**
82 SR **0.235.1**
83 Aktualisiertes Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 18. Mai 2018, abrufbar unter: www.coe.int > Rechtsstaatlichkeit > Datenschutz > Convention 108 and Protocols > Modernisation of Convention 108. Die Schweiz hat die Konvention 108+ (bzw. die Weiterentwicklung der Konvention 108) ratifiziert, diese ist aber noch nicht in Kraft getreten.

Die vorliegende Revision erfüllt die Voraussetzungen an ein Gesetz im materiellen Sinne gemäss der EMRK. Deren Vorgabe eines legitimen Ziels und der Notwendigkeit der Massnahmen in einer demokratischen Gesellschaft entsprechen derjenigen des öffentlichen Interesses und der Verhältnismässigkeit (vgl. oben). Der Pakt II garantiert in Bezug auf die vorliegend zur Diskussion stehenden Grundrechte keinen weitergehenden Schutz als die EMRK oder die BV.

Im Zusammenhang mit dem Schutz der Privatsphäre und dem Recht auf eine wirksame Beschwerde ist zu beachten, dass durch diese Vorlage verursachte Eingriffe, ab einer gewissen Schwere, vor ihrer Anwendung ein gerichtliches (Bundesverwaltungsgericht) Genehmigungsverfahren durchlaufen müssen, nach Abschluss der Operation der betroffenen Person mitgeteilt werden müssen und auch nachträglich einer richterlichen Kontrolle (Bundesverwaltungsgericht mit Weiterzugsmöglichkeit an das Bundesgericht) zugeführt werden können. Dies trifft nicht auf die in Artikel 14 Absatz 3 vorgesehene Massnahme zu. Näheres kann den Erläuterungen zu diesem Artikel entnommen werden.

Auch gegen Verfügungen basierend auf den Bestimmungen des BWIS (Ausreisebeschränkungen nach Art. 24*d* f. BWIS) kann beim Bundesverwaltungsgericht (mit Weiterzugsmöglichkeit an das Bundesgericht) Beschwerde geführt und eine Einschränkung der durch internationale Übereinkommen gewährten Rechte gerügt werden.

Im Zusammenhang mit der Einführung eines Tatbestands der Vorbereitungshaft für Inhaberinnen und Inhaber einer Kurzaufenthalts-, Aufenthalts- oder Niederlassungsbewilligung sind die Anforderungen des FZA sowie des EFTA-Übereinkommens zu beachten, sofern es sich um Staatsangehörige der EU oder der EFTA handelt. Im Einzelnen wird auf die Erläuterungen zu Artikel 75 Absatz 3 AIG verwiesen.

Zum Schutz von personenbezogenen Daten werden verschiedene wirksame Massnahmen insbesondere im Sinne der Datenschutzkonvention 108+ ergriffen (Eingangsprüfung, die sicherstellt, dass der NDB nur Daten bearbeitet, die einen Aufgabenbezug aufweisen und nicht unter die Datenbearbeitungsschranke fallen; Prüfung auf Richtigkeit der Daten; Festlegung restriktiver Zugriffsberechtigungen; Qualitätssicherungsmassnahmen, welche die Rechtmässigkeit, Verhältnismässigkeit und Richtigkeit der Datenbearbeitung sicherstellen und zur Anonymisierung oder Löschung von Daten führen, die nicht mehr für die Aufgabenerfüllung benötigt werden; Überprüfung von Daten vor deren Bekanntgabe an Dritte, die sicherstellt, dass die Daten den rechtlichen Vorgaben genügen und dass ihre Bekanntgabe rechtmässig und im konkreten Fall notwendig ist; Auskunftsrecht, dass den betroffenen Personen Zugang zu den über sie bearbeiteten Personendaten gewährt).

Die im Gesetzesentwurf neu vorgesehenen Tätigkeiten erfolgen damit völkerrechtskonform und sind mit den internationalen Verpflichtungen der Schweiz vereinbar.

7.3 Erlassform

Nach Artikel 164 BV und Artikel 22 Absatz 1 ParlG erlässt die Bundesversammlung alle wichtigen rechtsetzenden Bestimmungen in der Form eines Bundesgesetzes.

7.4 Unterstellung unter die Ausgabenbremse

Mit der Vorlage werden weder neue Subventionsbestimmungen (die über einem Schwellenwert liegende Ausgaben nach sich ziehen) geschaffen, noch neue Verpflichtungskredite / Zahlungsrahmen (mit Ausgaben über einem Schwellenwert) beschlossen. Die Vorlage ist somit nicht der Ausgabenbremse (Art. 159 Abs. 3 Bst. b BV) unterstellt.

7.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Die Vorlage tangiert die geltende Aufgabenteilung oder die Aufgabenerfüllung durch Bund und Kantone bezüglich der nachrichtendienstlichen Tätigkeiten nicht. Die Vorlage schafft kein Missverhältnis zwischen Kostentragung und Aufgabenerfüllung. Die finanzielle Beteiligung, die in Form der im geltenden Artikel 85 Absatz 5 geregelten Abgeltung an die Kantone für die im Auftrag des Bundes erfüllten Aufgaben nach dem NDG erfolgt, ist angemessen.

7.6 Delegation von Rechtsetzungsbefugnissen

Der Entwurf ergänzt nur in einem Bereich die Rechtsetzungsbefugnisse, die an den Bundesrat delegiert werden. Die bereits bestehende Kompetenz des Bundesrates, selbstständig völkerrechtliche Verträge im Bereich des Nachrichtendienstes abzuschliessen, wird inhaltlich erweitert. Diese Ermächtigung ist rechtmässig, da sie wie von Artikel 7*a* RVOG vorgeschrieben, durch ein Bundesgesetz erteilt wird. Die in nachrichtendienstlichen Bereichen abzuschliessenden völkerrechtlichen Verträge müssen nach Artikel 13 Absatz 3 ISG oftmals als geheim klassifiziert werden. Trotz der zunehmenden Tendenz, die internationale nachrichtendienstliche Zusammenarbeit zu formalisieren, wird zudem kein anderer Staat bereit sein, schriftliche Übereinkommen abzuschliessen, wenn diese danach veröffentlicht werden müssen. Aus Effizienzgründen ist es daher angezeigt, die Kompetenz zum Abschluss dieser Verträge von Beginn an dem Bundesrat zu übertragen. Die Regelung in Artikel 70 Absatz 3 ist zudem hinreichend konkretisiert. Weitere Ausführungen dazu finden sich in den Erläuterungen zur Anpassung dieses Artikels.

Die Bestimmungen zum 4. Kapitel beauftragen den Bundesrat wie bisher mit der Regelung der Einzelheiten der Datenbearbeitung, inhaltlich ändert sich an dessen Recht-

setzungsbefugnissen aber nichts, abgesehen von der logischen Anpassung der geltenden Delegationen für die heutigen Informations- und Speichersysteme (vgl. dazu oben die jeweiligen Erläuterungen zu den Art. 54, 55, 58 und 60).

7.7 Datenschutz

7.7.1 Datenschutz allgemein

Die Vorlage stellt sicher, dass die Bearbeitung personenbezogener Daten unter Einhaltung von datenschutzrechtlichen und verfassungsmässigen Standards erfolgt.

In datenschutzrechtlicher Hinsicht wird ein rechtsetzungstechnischer Systemwechsel notwendig, um einerseits den vollen Nutzen der Digitalisierung auszuschöpfen und andererseits den Regelungen des Datenschutzgesetzes entsprechen zu können. Daher werden in dieser Revisionsvorlage die betroffenen Bestimmungen technologieneutral ausgestaltet. Anstelle der gesetzlichen Auflistung von einzelnen Informationssystemen wird ausgewiesen, für welche nachrichtendienstlichen Aufgaben welche Kategorien von Daten bearbeitet werden dürfen. Dies entspricht den geltenden datenschutzrechtlichen Grundsätzen, wonach festzulegen ist, welche Daten zu welchem Zweck bearbeitet werden dürfen (vgl. dazu auch die allgemeinen Ausführungen zum 4. Kapitel oben).

Der Entwurf regelt die Prüfung der beim NDB und bei den KND eingehenden Daten (die Prüfung bezieht sich auf den Aufgabenbezug und die Datenbearbeitungsschranke, wobei in Abweichung zum DSG auch als unrichtig erkannte Daten bearbeitet werden dürfen, wenn diese entsprechend gekennzeichnet werden), die Kategorien von Daten, die bearbeitet werden dürfen, die zulässigen Datenbearbeitungszwecke, die Zugriffsberechtigungen, die Qualitätssicherungsmassnahmen, welche die Rechtmässigkeit, Verhältnismässigkeit und Richtigkeit der Datenbearbeitung sicherstellen und zur Anonymisierung oder Löschung nicht mehr für die Aufgabenerfüllung benötigter Daten führen, die Bekanntgabe von Daten, das Auskunftsrecht, das sich neu grundsätzlich nach den Bestimmungen des DSG richtet (vgl. aber das im DSG nicht vorgesehene indirekte Auskunftsrecht und die Beschwerdemöglichkeit ans Bundesverwaltungsgericht) und die Archivierung von Daten.

7.7.2 Datenschutz-Folgeabschätzung

Zum Entwurf wurde eine Datenschutz-Folgeabschätzung (DSFA) nach Artikel 22 DSG erstellt. Die DSFA hat der EDÖB formell und materiell geprüft.

Die DSFA vom 20. Dezember 2024 identifiziert folgende datenschutzrechtliche Hauptrisiken:

- die «unheimliche Erfahrung» bzw. den Umstand, dass die betroffenen Personen wissen oder glauben, dass der NDB Daten über sie sammelt, aber nicht wissen warum;
- die Verletzung der gesetzlichen Vorgaben und dadurch Unterlaufen der Qualitätssicherung und Beschränkungen;

- die Verletzung gesetzlicher Vorgaben (Verhältnismässigkeit), wodurch Arbeitsprodukte auf Basis von veralteten nachrichtendienstlichen Daten entstehen können, die wiederum folgenreiche Massnahmen haben können;
- der NDB übergibt dem BAR Dokumente, die möglicherweise noch zu schützende Quellen offen nennen.

Zusammengefasst sollen folgende Massnahmen diesen Hauptrisiken entgegenwirken:

- ausführlichere Kommunikation über das, was der NDB tut (mehr Transparenz); Verwendungssperre für Dokumente ohne Ablageprüfung; Verkürzung der Aufbewahrungsfrist für Personendaten aus öffentlich zugänglichen Quellen; Verzicht auf Aufschübe bei der Geltendmachung des Auskunftsrechts nach Artikel 63 ff.;
- Aktualisierung und Präzisierung von Vorgaben und Weisungen; Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter;
- Löschung veralteter oder nicht mehr benötigter nachrichtendienstlicher Daten; Aktualisierung und Präzisierung von Vorgaben und Weisungen betreffend die Erstellung von Arbeitsprodukten; Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter.

Nach Umsetzung dieser Massnahmen verbleiben keine hohen Restrisiken.

Im Bereich der Datensicherheit wurden folgende Hauptrisiken identifiziert:

- die Manipulation von Informationen, Hard- oder Software vorsätzlich oder durch Fehlmanipulationen;
- das Ausspähen von Informationen, Spionage und das Abhören, vorsätzlich oder durch Fehlmanipulationen;
- der Missbrauch von Personendaten, vorsätzlich oder durch Fehlmanipulationen.

Zusammengefasst sollen folgende Massnahmen diesen Hauptrisiken bei der Datensicherheit entgegenwirken:

- die Umsetzung des IT-Grundschutzes des Bundes;
- die Durchführung regelmässiger Audits (die Einhaltung der Rechtsgrundlagen und der Sicherheitsanforderungen wird regelmässig sowohl durch interne als auch externe Auditoren geprüft; die Ergebnisse werden protokolliert und identifizierte Lücken werden gepflegt);
- die technische Prüfung (mit sog. Penetrations-Tests wird durch externe, spezialisierte Firmen die Resilienz der IT-Infrastruktur geprüft; die Ergebnisse werden protokolliert und identifizierte Lücken werden gepflegt).

Nach Umsetzung dieser Massnahmen verbleibt als einziges hohes Restrisiko das Ausspähen von Informationen, Spionage und das Abhören vorsätzlich oder durch Fehlmanipulationen. Diesbezüglich haben die verantwortlichen Stellen im NDB alle zur

Verfügung stehenden technischen und organisatorischen Massnahmen getroffen, um die Datensicherheit zu gewährleisten.

7.7.3 Stellungnahme des EDÖB zur DSFA des NDB vom 28. Januar 2025

Die Stellungnahme des EDÖB vom 28. Januar 2025 hält fest, dass die DSFA sorgfältig erarbeitet wurde, dass die für die Prüfung benötigten Informationen dem EDÖB vorgelegt wurden und dass die aufgeführten Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person den gesamten, neu eingeführten Datenbearbeitungsprozess abdecken. Bei mehreren festgestellten Risiken sind gemäss dem EDÖB zweckmässige Massnahmen vorgesehen. Nebst dem einzigen hohen Restrisiko (Ausspähen) bleibt das Risiko eines menschlichen Fehlverhaltens bestehen. Hier schlug der EDÖB unter Beachtung von Artikel 23 Absatz 3 DSG keine weitere Massnahme vor.

Der EDÖB hat in den drei folgenden Bereichen beantragt, dass das Ausmass und die Qualität der neuen Bearbeitungen sowie die dazugehörigen (neuen) Risiken in der DSFA abgebildet werden:

- Paradigmenwechsel von der Regelung einzelner Informationssysteme hin zu einer technologieneutralen Formulierung der Aufgaben des NDB;
- neue Datenbearbeitung, die sich durch die Ausdehnung der Aufgabe des NDB im Cyberraum (vgl. Art. 6 Abs. 1 Bst. b) ergibt;
- neue Datenbearbeitung, die sich aus der Umstrukturierung des Nachrichtenverbunds (Art. 5 Abs. 6 Bst. e) ergibt.

Hier geht der NDB davon aus, dass grundsätzlich keine bedeutend neuen Datenbearbeitungen stattfinden, weder quantitativ noch qualitativ, da die Neuerungen zum grossen Teil der bisherigen Praxis des NDB entsprechen. Nichtsdestotrotz wird der NDB diese Ausführungen im Rahmen der weiteren Arbeiten an der DSFA einbringen.

7.7.4 Grundrechtseingriffe

Der vorliegende Entwurf stellt sicher, dass die Bearbeitung personenbezogener Daten unter Einhaltung von datenschutzrechtlichen und verfassungsmässigen Standards erfolgt.

Die Datenbearbeitung kann insbesondere den Schutz der Privatsphäre und der informationellen Selbstbestimmung nach Artikel 13 BV tangieren. Vor diesem Hintergrund enthält der Entwurf klare gesetzliche Regelungen, welche die Zulässigkeit der Datenbearbeitung an strenge Voraussetzungen knüpfen. Insbesondere müssen alle Datenbearbeitungen verhältnismässig, zweckgebunden und notwendig für die Erfüllung der Aufgaben des NDB sein.

Der vorliegende Entwurf enthält verschiedene Massnahmen zum Schutz von personenbezogenen Daten, wie z. B. die Eingangsprüfung aller Daten, die periodische Qua-

litätssicherung von nachrichtendienstlichen Daten oder die Gewährleistung der Auskunftsrechte. Im Rahmen des Auskunftsrechts zu nachrichtendienstlichen Daten kann die Rechtmässigkeit der Datenbearbeitung und die Rechtfertigung der Einschränkung oder des Aufschubs der Auskunft durch den EDÖB oder anschliessend durch das Bundesverwaltungsgericht überprüft werden.

Insgesamt trägt die im Entwurf geregelte Datenbearbeitung dazu bei, dass der NDB seine sicherheitspolitischen Aufgaben weiterhin wirkungsvoll erfüllen kann, ohne dabei die verfassungsmässigen Grundrechte unverhältnismässig zu beeinträchtigen.