Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Nachrichtendienst des Bundes NDB

Erläuterungen

zur **Verordnung über den Nachrichtendienst (Nachrichtendienstverordnung, NDV) und zur Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB)**

1 Vorbemerkung

Für das Nachrichtendienstgesetz vom 25 September 2015[1] (NDG) sind drei Verordnungen vorgesehen: Einerseits die „allgemeine“ Verordnung über den Nachrichtendienst (NDV), andererseits die Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB), welche die Datenhaltung, -pflege und Qualitätssicherung regelt und die Betrieb, Inhalt und Nutzung der im NDG definierten Informationssysteme des NDB betrifft. Die Struktur der NDV folgt nicht streng jener des NDG, sondern unterstützt primär die externen Nutzer und behandelt Interna für den Nachrichtendienst des Bundes erst am Schluss. Hinzu kommt die Verordnung über die Aufsicht über die nachrichtendienstliche Tätigkeit (VAND), die dem Bundesrat separat unterbreitet und erläutert wird.

2 Erläuterungen zur NDV

1. Kapitel: Zusammenarbeit

1. Abschnitt: Zusammenarbeit des NDB mit inländischen Stellen

Gegenstand des 1. Abschnitts bilden die allgemeinen Grundsätze der Zusammenarbeit mit den wichtigsten (nicht abschliessend aufgezählten) Partnern des NDB im Inland. Sie entsprechen dem heutigen Status Quo und orientieren sich am Grundsatz der gegenseitigen Unterstützung. Nicht Gegenstand des 1. Abschnitts bilden die konkreten Formen der Zusammenarbeit, so insbesondere diejenige mit den kantonalen Vollzugsstellen. Die diesbezüglichen Befugnisse und Kompetenzen bei der selbstständigen Informationsbeschaffung sind in Artikel 85 NDG (Vollzug durch die Kantone) bereits umfassend geregelt. Selbstredend besteht daneben die Möglichkeit, dass der NDB die kantonalen Vollzugsstellen mit der Durchführung weiterer Massnahmen beauftragt. In diesem Bereich handeln die kantonalen Vollzugsstellen folglich nicht selbständig, sondern mit ausdrücklichem Auftrag des NDB, der dafür auch in der Verantwortung steht.

Art. 1 Zusammenarbeit des NDB mit inländischen Stellen und Personen

In der Verordnung wurde darauf verzichtet, die Zusammenarbeit und Beauftragung in der Beschaffung nach Artikel 34 NDG sowie die Bekanntgabe von Personendaten an Dritte nach Artikel 62 NDG expressis verbis zu nennen. Dies weil sie ausdrücklich im Gesetz vorgesehen sind, somit ohnehin anwendbar sind, vor allem jedoch um unnötige Redundanzen zwischen Gesetz und Verordnung zu vermeiden.

Art. 2 Zusammenarbeit des NDB mit Konferenzen der Kantone

Die ausdrückliche Nennung des Zusammenarbeitszweckes erfolgt auf einhelligen Wunsch der Kantone.

Art. 5 Zusammenarbeit des NDB mit dem fedpol

Es wird ausdrücklich vorgesehen, dass sich der NDB und das Bundesamt für Polizei (fedpol) beim Einsatz und der Nutzung von operativen Ressourcen und Mitteln gegenseitig unterstützen. Damit soll vermieden werden, dass dort, wo es mit den verschiedenen Aufgaben vereinbar ist, kostspieliges Gerät doppelt angeschafft und unterhalten werden muss oder dass es zu Doppelspurigkeiten bei der Ausbildung kommt. Die Weitergabe von Informationen nach Absatz 2 ist nicht abschliessend; fedpol und der NDB arbeiten beispielsweise auch in gemeinsamen Leitungsausschüssen und Gremien wie bei der operativen Koordination der Terrorismusbekämpfung oder im Sonderstab Geiselnahme eng zusammen. Die Zusammenarbeit zwischen dem NDB und fedpol basiert inskünftig nicht länger auf gegenseitigen Vereinbarungen, wird jedoch im Rahmen der bisherigen Praxis weitergeführt.

Art. 6 Abgeltung der Vollzugstätigkeiten der Kantone und Beurteilung der Aufgabenerfüllung

Die im Vernehmlassungsentwurf von kantonaler Seite stark kritisierte Regelung wurde überarbeitet und mit der KKPKS bereinigt. Der überarbeitete Wortlaut orientiert sich stärker an der bis anhin geltenden Regelung; die Kantone sollen keinesfalls finanziell schlechter gestellt werden als bisher.

2. Abschnitt: Zusammenarbeit des NDB mit ausländischen Stellen

Die Zusammenarbeit mit ausländischen Stellen orientiert sich an der heutigen Rechtslage und ergänzt diese mit bewährter Praxis.

Art. 7 Jährliche Festlegung der Grundsätze der Zusammenarbeit

Die jährliche Festlegung der Grundsätze der Zusammenarbeit entspricht heutiger Praxis und wird neu auf Verordnungsebene verankert.

Art. 8 Zuständigkeiten

Gleich wie bisher ist der NDB für nachrichtendienstliche Kontakte im Rahmen des NDG „single point of contact“ zu anderen ausländischen Dienststellen, die Aufgaben im Sinne des NDG erfüllen. Das bisherige bewährte Konzept soll somit weitergeführt werden. Mit Blick auf den kleinen Grenzverkehr ist vorgesehen, dass der NDB die Wahrnehmung von Kontakten mit ausländischen Nachrichtendiensten beschränkt auf bestimmte Themengebiete an kantonale Vollzugsbehörden delegieren kann. Auch vertritt der NDB die Schweiz in internationalen nachrichtendienstlichen Gremien. Im militärischen Bereich ist bei der Festlegung einer gemeinsamen Partnerdienstpolitik und Erstellung einer Kontaktplanung Ansprechpartner des NDB der Nachrichtendienst der Armee, der sich seinerseits insbesondere mit dem Militärischen Nachrichtendienst

[1] BBl **2015** 7211

(MND), dem Kommando Spezialkräfte (KSK) und den Swiss Armed Forces International Command (SWISSINT) austauscht.

Art. 10 Internationale Vereinbarungen von beschränkter Tragweite

Der NDB erhält neu die Möglichkeit, wie andere Amtsstellen auch, selbständig internationale Vereinbarungen mit ausländischen Nachrichtendiensten oder anderen ausländischen Dienststellen, die Aufgaben im Sinne des NDG erfüllen, abzuschliessen. Nach Artikel 48*a* des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[2] kann der Bundesrat die Zuständigkeit zum Abschluss völkerrechtlicher Verträge an ein Departement delegieren. Bei Verträgen von beschränkter Tragweite kann er diese Zuständigkeit auch an eine Gruppe oder an ein Bundesamt delegieren. Folglich ist der NDB einzig befugt, selbständig internationale Vereinbarungen von beschränkter Tragweite über technische Belange im Bereich des Nachrichtendienstes abzuschliessen. Zu denken ist etwa an eine Vereinbarung über technische Standards eines nach Schweizer Recht zulässigen Übermittlungs- oder Informationssystems mit einem ausländischen Dienst. Vereinbarungen, die die Kriterien von Artikel 80 Absatz 3 NDG erfüllen (auf längere Dauer angelegt, substanzielle finanzielle Konsequenzen oder von grösserer rechtlicher oder politischer Bedeutung), sind weiterhin dem Bundesrat zu unterbreiten.

2. Kapitel: Informationsbeschaffung

1. Abschnitt: Grundsätze

Art. 12 Operationen

Die Definition des Begriffs Operationen ist notwendig, weil bei den genehmigungspflichtigen Beschaffungsmassnahmen die gesetzliche Mitteilungspflicht (bzw. deren Aufschub oder das davon Absehen) nach Artikel 33 NDG durch den Abschluss der jeweiligen Operation ausgelöst wird. Auch soll damit ermöglicht werden, zwischen der einfachen Bearbeitung nachrichtendienstlicher Fragestellungen und der Führung eines viel weitergehenden, meist komplexen – und unter besonderem Augenmerk der Aufsichtsorgane stehenden – nachrichtendienstlichen Fallkomplexes zu unterscheiden. Der NDB muss solche Operationen formell eröffnen und abschliessen und gesondert dokumentieren.

Art. 13 – 16 Zusammenarbeit mit inländischen Amtsstellen, mit ausländischen Amtsstellen im Inland, mit Privaten im Inland und mit ausländischen Amtsstellen oder Privaten im Ausland sowie Erteilung von Beschaffungsaufträgen

Nach Artikel 34 NDG kann der NDB eine Beschaffungsmassnahme selbst durchführen oder mit in- oder ausländischen Amtsstellen zusammenarbeiten bzw. diese mit der Durchführung beauftragen, sofern die andere Stelle Gewähr dafür bietet, die Beschaffung entsprechend den Bestimmungen dieses Gesetzes durchzuführen. Auch kann er ausnahmsweise mit Privaten zusammenarbeiten oder Privaten Aufträge erteilen, wenn dies aus technischen Gründen oder wegen des Zugangs zum Beschaffungsobjekt erforderlich ist und die betreffende Person Gewähr dafür bietet, die Beschaffung entsprechend den Bestimmungen dieses Gesetzes durchzuführen.

Regelungsbedarf besteht für die Zusammenarbeit *im Inland mit*

- inländischen Amtsstellen,
- ausländischen Amtsstellen,
- Privaten

Gewähr für eine gesetzeskonforme Beschaffung im Inland ist gemäss Verordnung dann gegeben, wenn

- bei einer inländischen Amtsstelle die Beschaffung im Rahmen der ordentlichen Tätigkeit der inländischen Amtsstelle erfolgt oder, falls die Beschaffung ausserhalb der ordentlichen Tätigkeit der inländischen Amtsstelle erfolgt, wenn diese über die für die Beschaffung notwendigen Fertigkeiten sowie Kenntnisse der massgebenden gesetzlichen Bestimmungen verfügt oder vom NDB diesbezüglich sorgfältig instruiert wurde.
- der ausländischen Amtsstelle oder einer privaten Person die für die Informationsbeschaffung massgebenden schweizerischen Bestimmungen mitgeteilt und soweit notwendig erläutert wurden und die ausländische Amtsstelle bzw. die private Person bestätigt, sich an die schweizerischen Bestimmungen zu halten.

Für die Zusammenarbeit und Beauftragung in der Beschaffung mit oder von ausländischen Amtsstellen oder von Privaten im Ausland gelten erleichterte Bedingungen. Dies rechtfertigt sich mit Blick darauf, dass der NDB mit über hundert ausländischen Sicherheitsbehörden auf aller Welt Kontakte unterhält und es den jeweiligen landesspezifischen Besonderheiten gleich wie der Souveränität von ausländischen Sicherheitsdiensten Rechnung zu tragen gilt.

Die Zusammenarbeit oder Beauftragung muss in jedem Fall dokumentiert werden. Abgesehen von inländischen Amtsstellen hat der NDB zudem im Verlaufe der Informationsbeschaffung (soweit möglich) die Einhaltung der massgebenden gesetzlichen Bestimmungen zu kontrollieren. Stellt der NDB fest, dass diese nicht eingehalten werden (und kann dieser Mangel nicht innert nützlicher Frist behoben werden), besteht keine Gewähr mehr für einen gesetzeskonformen Vollzug und der NDB beendet die Zusammenarbeit unverzüglich unter gleichzeitiger Information der unabhängigen Aufsichtsbehörde.

Art. 17 - 18 Nachrichtendienstliche Informationsquellen / Quellenschutz

Hinsichtlich des Quellenschutzes sind die zentralen Grundsätze bereits in Artikel 35 NDG enthalten. Auf Verordnungsebene wird nun präzisiert, was als nachrichtendienstliche Informationsquelle gilt. Es sind dies menschliche Quellen, in- und ausländische Nachrichtendienste und Sicherheitsbehörden, mit denen der NDB zusammenarbeitet, sowie technischen Quellen. Für die nicht bereits im Gesetz geregelten Fälle wird in der Verordnung das Prinzip der einzelfallweisen

[2] SR **172.010**

Interessenabwägung zwischen der informationsersuchenden und der zu schützenden Quelle verankert. Dabei ist eine vom NDB oder in seinem Auftrag von kantonalen Vollzugsbehörden geführte menschliche Quelle umfassend zu schützen, wenn ihr selber eine ernsthafte Gefahr für die physische oder psychische Integrität droht. Gleich wie bisher soll – wenn die Umstände es erfordern – der Schutz auch der Quelle nahestehende Personen umfassen (z.B. Familienangehörige, Lebenspartner usw.).

Die in Absatz 4 in Bezug auf menschliche Quellen einzelfallweise vorgesehene Zusammenarbeit mit fedpol gründet auf Artikel 14 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[3] und betrifft Schutzmassnahmen. Der NDB trägt dabei die gesamten Kosten, wobei einzelfallweise mit der Eidgenössischen Finanzverwaltung und fedpol eine Lösung zu erarbeiten ist.

Technische Quellen sind umfassend zu schützen, ausser wenn deren Bekanntgabe die Auftragserfüllung des NDB weder direkt noch indirekt gefährdet. Zu betonen bleibt, dass der Quellenschutz für den NDB von höchstem Interesse ist. Wenn er ihn nicht ausreichend sicherstellen kann, wäre das Risiko gross, vom internationalen Informationsaustausch abgeschnitten zu werden, mit entsprechenden Folgen für die Sicherheit der Schweiz.

Art. 19 **Berichterstattung über Operationen und Quellen** Die Aufsichtsorgane haben unbesehen der Berichtspflicht jederzeit umfassenden Zugang zu allen sachdienlichen Informationen und Unterlagen sowie Zutritt zu allen Räumlichkeiten des NDB.

2. Abschnitt: Auskunftsplicht bei einer konkreten Bedrohung

Die Regelung der Auskunfts- und Meldepflichten übernimmt im Wesentlichen das heutige Regelwerk mit bewährten und eingespielten Abläufen: der NDB arbeitet eng mit den Kantonen zusammen, gewährt diesen aber bei der Auftragserfüllung ein hohes Mass an Autonomie.

Da die in Artikel 24 NDG neu vorgesehene Anhaltung zur Identifikation und Befragung von Personen ausschliesslich durch Angehörige eines kantonalen Polizeikorps erfolgt, besteht auf Verordnungsebene kein Regelungsbedarf.

Art. 20 Abs. 2

Die Auflistung der Organisationen in Anhang 1, denen der Bund oder die Kantone die Erfüllung öffentlicher Aufgaben übertragen hat, wurde gegenüber dem heutigen Recht mit der Finanzmarktaufsicht, der Eidgenössischen Elektrizitätskommission und der Eidgenössischen Kommunikationskommission ergänzt.

Nach Artikel 20 Absatz 4 NDG legt der Bundesrat in einer nicht öffentlichen Liste fest, welche Vorgänge und Feststellungen dem NDB unaufgefordert zu melden sind. Er umschreibt den Umfang der Meldepflicht und das Verfahren der Auskunftserteilung. Diese nicht öffentliche Liste kann, entgegen den auf einem redaktionellen Versehen beruhenden (teilweise missverständlichen) Ausführungen in der Botschaft zum NDG, Meldepflichten zu Vorgängen und Feststellungen enthalten, die aus Geheimhaltungsgründen nicht veröffentlicht werden dürfen, als auch solche, die keiner Geheimhaltung unterliegen. Da die Meldepflichten die Informationsbeschaffung betreffen, gilt es zudem Artikel 67 NDG Rechnung zu tragen, wonach amtliche Dokumente betreffend die Informationsbeschaffung erklärtermassen nicht dem Öffentlichkeitsprinzip unterliegen und deshalb - folgerichtig - auch nicht publiziert werden sollen.

3. Abschnitt: Genehmigungspflichtige Beschaffungsmassnahmen

Die gesetzliche Regelung der genehmigungspflichtigen Beschaffungsmassnahmen ist sehr detailliert und umfassend. Auf Verordnungsebene besteht deshalb kaum Regelungsbedarf:

Art 21 Durchsuchen von Räumlichkeiten, Fahrzeugen oder Behältnissen

Das Durchsuchen von Räumlichkeiten, Fahrzeugen oder Behältnissen ist zu dokumentieren. Da die Durchsuchung verdeckt, d.h. in Abwesenheit der betroffenen Person erfolgt, soll die Dokumentierung in erster Linie dazu dienen, allfällige später gegenüber dem NDB erhobene Missbrauchsvorwürfe und/oder Schadenersatzansprüche zu widerlegen. Erlauben es die Verhältnisse vor Ort, kann die Dokumentierung auch mittels Bild- und/oder Tonaufnahmen erfolgen. Bei den anderen genehmigungspflichtigen Beschaffungsmassnahmen erfolgt die Dokumentierung durch die Sammlung der entsprechenden Daten im Speichersystem für Daten aus genehmigungspflichtigen Beschaffungsmassnahmen.

Art. 22 Genehmigungsverfahren und Freigabe

Das Genehmigungsverfahren und das Freigabeverfahren sind durch den NDB bzw. das VBS jederzeit nachvollziehbar in schriftlicher oder elektronischer Form zu dokumentieren.

Art. 23 Schutz von Berufsgeheimnissen

Der in Artikel 28 NDG verankerte Schutz von Personen, die einer der in Artikel 171 – 173 der Strafprozessordnung[4] (StPO) genannten Berufsgruppen angehören, wird auf Verordnungsebene präzisiert: Wird eine *Zielperson* in Anwendung von Artikel 27 NDG überwacht, und gehört sie einer der in Artikel 171 – 173 StPO genannten Berufsgruppen an, ist durch eine vorgängige Selektion („Triage“) der bei der Beschaffung erhobenen Daten sicherzustellen, dass der NDB keine Berufsgeheimnisse erfährt, die keinen Bezug zur konkreten Bedrohung haben, die Grund für die angeordnete Überwachung ist; in solchen Fällen muss der NDB deshalb im Genehmigungsverfahren das Bundesverwaltungsgericht unaufgefordert darauf hinweisen und die entsprechende Selektion beantragen. Die Aussonderung und Vernichtung geschützter Daten erfolgt unter Aufsicht des Bundesverwaltungsgerichts.

---

3 SR **172.010.1**
4 SR **312.0**

Gar nicht zulässig ist gemäss Artikel 28 Absatz 2 NDG die Anordnung einer genehmigungspflichtigen Beschaffungsmassnahme gegenüber einer *Drittperson*, die einer der in Artikel 171 – 173 StPO genannten Berufsgruppe angehört. Das betrifft beispielsweise Fälle, in denen die eigentliche Zielperson den Fernmeldeanschluss eines Berufsgeheimnisträgers benutzt. Eine Überwachung dieses Anschlusses ist nicht möglich.

4. Abschnitt. Eindringen in Computersysteme und –netzwerke im Ausland

Art. 24

Nach Artikel 37 Absatz 1 NDG kann der NDB in ausländische Computersysteme und Computernetzwerke eindringen, die für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet werden. Über die Durchführung einer solchen Massnahme entscheidet der Bundesrat. Davon zu unterscheiden ist das Eindringen in Computersysteme und Computernetzwerke im Ausland nach Artikel 37 Absatz 2 NDG um dort vorhandene oder von dort aus übermittelte Informationen über Vorgänge im Ausland zu beschaffen. Hier prüft die Vorsteherin oder der Vorsteher des VBS den Antrag. Hält er diesen für begründet, konsultiert er dier Vorsteherin oder den Vorsteher des EDA und die Vorsteherin oder den Vorstehers des EJPD und entscheidet alsdann über die Durchführung einer solchen Massnahme.

Zur Entlastung der Entscheidungsträger und zur Sicherstellung zeitnaher Entscheide sieht die Verordnung vor, dass die Konsultation der Vorsteherin oder des Vorstehers des EDA bzw. des EJPD und daran anschliessend der Entscheid der Vorsteherin oder des Vorstehers des VBS bei der Bearbeitung eines Falles oder Fallkomplexes (z.B. Entführungsfall XY) auch einmalig erfolgen kann. Eine solche Bewilligung für einen Fall oder Fallkomplex beinhaltet – soweit notwendig – auch mehrfaches Eindringen in Computersysteme oder Computernetzwerke bei der gleichen oder bei unterschiedlichen Personen (soweit diese mit dem bewilligten Fall oder Fallkomplex in Zusammenhang stehen). Mit anderen Worten ausgedrückt handelt es sich um eine zwar umfassende, aber auf einen Fall oder Fallkomplex beschränkte Bewilligung (umfassende Fall- oder Fallkomplex bezogene Bewilligung wie beispielsweise, während der Dauer einer Entführung in Computersysteme der Entführergruppe einzudringen oder die Bewilligung, nach einem abgewehrten Cyberangriff während eines befristeten Zeitraums in die Computersysteme des Angreifers einzudringen, um dessen Identität und/oder weitere Angriffe und/oder weitere Opfer festzustellen).

5. Abschnitt: Kabelaufklärung

Auftraggeber eines Kabelaufklärungsauftrages ist der NDB. Die Umsetzung erfolgt jedoch nicht durch den NDB, sondern durch den durchführenden Dienst. Durchführender Dienst ist das Zentrum für elektronische Operationen (ZEO) der Führungsunterstützungsbasis der Armee. Dieses stellt einerseits durch interne Massnahmen sicher, dass die Auftragserfüllung einzig im Rahmen der vom Bundesverwaltungsgericht erteilten Genehmigung erfolgt. Anderseits beschafft das ZEO die notwendigen technischen Einrichtungen und ist Kontaktstelle zu den Betreiberinnen von leitungsgebundenen Netzen und den Anbieterinnen von Telekommunikationsdienstleistungen. Diese haben dem ZEO jederzeit Zutritt zu den für die Kabelaufklärung benötigten Räumen zu gewähren um ihm die Installation von technischen Komponenten zur Umsetzung von Kabelaufklärungsaufträgen zu ermöglichen.

Die Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsdienstleistungen sind nach Artikel 27 Absatz 1 verpflichtet, dem ZEO technische Angaben zu liefern. Diese technischen Angaben umfassen insbesondere:

- Spezifikationen des Übertragungsmediums d.h. die physische Beschaffenheit der Kabel
- verwendete Technologien zur Übertragung der Signale auf dem Medium (d.h. verwendete Multiplexmethoden wie Art und Anzahl der Wellenlängen, Codierung der Wellenlängen)
- Protokolle
- Bandbreiten und eventuell Datenvolumen
- Verwendungszweck der auf dem Kabel vorhandenen Verbindungen
- Endpunkte der Kabel (Adresse, Mietmöglichkeit, Anschlussmöglichkeiten, Klima, Strom, usw.)

Die technischen Angaben sind für einen rechtsgenügenden, fundierten Antrag an das Bundesverwaltungsgericht erforderlich und ermöglichen es, diesem im konkreten Anwendungsfall darzulegen, bei welchen Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsdienstleistungen potenziell relevante Daten vorliegen. Andererseits sind die technischen Angaben auch nötig, um die im Falle einer späteren Übernahme von Signalen und deren Umwandlung in Daten notwendige technische Ausrüstung zu bestimmen und zu beschaffen.

Art. 28 Datenbearbeitung

Der Begriff Daten ist die Gesamtheit aller Erfassungen aus der Funk- und Kabelaufklärung (Oberbegriff). Er setzt sich zusammen aus den Kommunikationsinhalten (z.B. Sprache, Text, Bilder) und den Verbindungsdaten. Verbindungsdaten sind erfasste Daten, die nicht Kommunikation sind, angereichert mit den von den Erfassungssystemen hinzugefügten Informationen („Session Related Informations“ wie beispielsweise Zeitpunkt der Erfassung). Davon zu unterscheiden ist der Begriff "Resultat". Resultate sind die aus den erfassten Daten erstellten Produkte (d.h. die auftragskonformen Informationen), die an den NDB weitergeleitet werden.

Die Fristen von 18 Monaten (Vernichtung erfasste Kommunikation) und 5 Jahren (Vernichtung erfasste Verbindungsdaten) sind identisch mit denjenigen für die Vernichtung der Kommunikation bzw. der Verbindungsdaten bei der Funkaufklärung (vgl. Art. 4 der Verordnung über die elektronische Kriegführung und die Funkaufklärung, VEKF; SR 510.292). Gleich wie bei der Funkaufklärung entspricht die Frist von 18 Monaten auch bei der Kabelaufklärung der Zeitdauer, in welcher eine Retrosuche, d.h. ein Durchsuchen gespeicherter Kommunikationsinhalte für einen mit neuen Suchbegriffen angereicherten, bestehenden Auftrag, eine nachrichtendienstliche Relevanz verspricht bzw. für eine Rückschau nachrichtendienstlich relevant ist (5-Jahres Frist).

Art. 30 Entschädigung für die Betreiberinnen von leitungsgebundenen Netzen und die Anbieterinnen von Telekommunikationsdienstleistungen

Die Betreiberinnen von leitungsgebundenen Netzen und die Anbieterinnen von Telekommunikationsdienstleistungen haben Anspruch auf Entschädigung ihrer im Rahmen der Kabelaufklärung erbrachten Leistungen. Bei der aktuellen Revision des Bundesgesetzes vom 6. Oktober 2000[5] betreffend die Überwachung des Post- und Fernmeldeverkehrs wurde die bisherige Praxis beibehalten, wonach für die Nutzung der Überwachungsinfrastruktur keine Vollkostenentschädigung verlangt werden kann, sondern eine angemessene Entschädigung im Anwendungsfall; dieser Grundsatz soll auch für die Kabelaufklärung übernommen werden. Es besteht sonst namentlich kein Anreiz für die Betreiberinnen von leitungsgebundenen Netzen und die Anbieterinnen von Telekommunikationsdienstleistungen, nach kostengünstigen Lösungen zu suchen.

3. Kapitel: Besondere Bestimmungen über den Datenschutz

Die Regelungen über die Bekanntgabe von Personendaten nach heutigem Recht hat sich gut bewährt; sie wird von der Verordnung weitestgehend übernommen.

Art. 33 Bekanntgabe von Personendaten durch kantonale Vollzugsbehörden

Grundlage von Artikel 33 bildet in erster Linie Artikel 46 Absatz 3 NDG, welcher die Datenbearbeitung in den Kantonen regelt.

Der Begriff der Strafverfolgungsbehörden in den Absätzen 1 – 3 bezieht sich auf ein laufendes oder unmittelbar vor der Eröffnung stehendes Strafverfahren. Die konkrete Verwendung einer Information in einem Strafverfahren richtet sich nach Artikel 34 NDV.

Die Datenbekanntgabe nach Absatz 5 der Verordnung hat Ausnahmecharakter und soll einzig in notwehr- oder notstandsähnlichen Situationen schnelles behördliches Handeln ermöglichen. Der NDB ist unverzüglich zu benachrichtigen.

Art. 34 Bekanntgabe von Informationen an Strafverfolgungsbehörden

Für die Strafverfolgungsbehörden im zivilen Bereich kann auf Artikel 12 StPO verwiesen werden. Zu den Strafverfolgungsbehörden im militärischen Bereich gehören Oberauditorat, Militärjustiz und Militärpolizei, so dass auch hier eine gesetzliche Grundlage für den Informationsaustausch besteht.

4. Kapitel: Politische Steuerung, Prüfverfahren und Verbote

Art. 36 Wahrung weiterer wichtiger Landesinteressen

Das NDG deckt den engeren sicherheitspolitischen Interessenbereich im Zuständigkeitsbereich des VBS ab. Anträge betreffend die Wahrung weiterer wichtiger Landesinteressen dürften deshalb in erster Linie von ausserhalb des VBS eingereicht werden. So wäre es beispielsweise denkbar, dass das Eidgenössische Finanzdepartement den Einsatz des NDB beantragt, um Erkenntnisse über Absichten ausländischer Staaten zu gewinnen, die dem Finanzplatz Schweiz aus wirtschaftlichen Interessen schaden wollen.

Jedes Departement und jeder Kanton kann einen entsprechenden Antrag bzw. Gesuch einreichen. Der Antrag bzw. das Gesuch hat sich u.a. zu Art, Schwere und Dringlichkeit der konkreten Bedrohung als solches und zur Dauer des beantragten Einsatzes des NDB zu äussern bzw. die Einsatzdauer ist im jeweiligen Beschluss des Bundesrates zeitlich zu begrenzen. Ist keine Begrenzung nach Tagen, Monaten oder Jahren möglich, wird festzulegen sein, in welchem Zeitintervall der Einsatz des NDB zu überprüfen ist, und/oder welche Kriterien für die Weiterführung oder Beendigung des Einsatzes massgebend sind. Auch die einzusetzenden nachrichtendienstlichen Mittel sind zu konkretisieren. Hier wird sich in erster Linie die Frage stellen, ob auf den Einsatz bestimmter nachrichtendienstlicher Mittel verzichtet werden soll, wie z.B. auf das Eindringen in fremde Computersysteme (Art. 36 Abs. 2 NDG) oder etwa das Anwerben von menschlichen Quellen im Ausland. Damit der Antrag bezüglich Aufwand und Machbarkeit plausibilisiert werden kann, sieht die Verordnung eine vorgängige Konsultation des NDB vor.

Schliesslich ist darauf hinzuweisen, dass die vorliegenden Ausführungsbestimmungen auf Artikel 3 NDG gründen, der seinerseits eine schwere und unmittelbare Bedrohung voraussetzt. Bei einer unmittelbaren Bedrohung müssen vorhersehbar rasch Abwehrmassnahmen ergriffen werden. Je unmittelbarer eine Bedrohung ist, umso knapper wird deshalb die Begründung ausfallen müssen, ansonsten sich die Bedrohung bis zum Vorliegen der Begründung verwirklich haben wird. Um Aussicht auf Erfolg zu haben, werden sich Aufträge, die den Aufbau von besonderen personellen Ressourcen und von besonderem Wissen erfordern, über einen angemessenen Zeitraum erstrecken müssen. Der NDB hat und schafft keine personellen oder finanziellen Ressourcen auf Reserve.

Art. 37 und 38 Prüfverfahren bzw. Einstellung von Prüfverfahren

Das Prüfverfahren wurde aus dem bisherigen Verordnungsrecht zum Bundesgesetz vom 21. März 1997[6] über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) übernommen. Es dient der Klärung, ob eine Person bzw. Organisation oder Gruppierung in die Beobachtungsliste aufzunehmen ist. Dazu sammelt und bearbeitet der NDB alle sachdienlichen Daten; Artikel 5 Absatz 8 NDG ist anwendbar. Sobald Klarheit über das weitere Vorgehen besteht, ist das Prüfverfahren einzustellen. Klarheit über das weitere Vorgehen besteht im Wesentlichen dann, wenn eine Aufnahme in die Beobachtungsliste erfolgt (Verdacht bestätigt sich) oder wenn die zum Prüfverfahren führenden Anhaltspunkte entkräftet wurden, also keine Aufnahme in die Beobachtungsliste erfolgt (Verdacht bestätigt sich nicht) oder wenn innert zweier Jahre nach Eröffnung des Prüfverfahrens keine zusätzlichen sicherheitsrelevanten Erkenntnisse gewonnen werden können

[5] SR **780.1**
[6] SR **120**

(Anfangsverdacht wird durch Zeitenlauf hinfällig). Ein eingestelltes Prüfverfahren kann bei gegebenen Voraussetzungen jederzeit wieder eröffnet werden.

Die Durchführung eines Prüfverfahrens ist indessen nicht Voraussetzung, um eine Organisation in die Beobachtungsliste aufzunehmen. Sind die Kriterien für eine Aufnahme gegeben, so kann diese auch sofort erfolgen.

Art. 40 Tätigkeitsverbot

Gemäss Artikel 73 Absatz 3 NDG hat das antragstellende Departement bei einem Tätigkeitsverbot regelmässig zu prüfen, ob die Anordnungsvoraussetzungen noch erfüllt sind. Die Verordnung legt für die Prüfung eine jährliche Kadenz fest. Eine jährliche Prüfkadenz scheint angemessen, weil sich ein Tätigkeitsverbot bei seinem Erlass auf einen Beschluss des Bundesrates und damit auf eine umfassende Abklärung der Tatsachen- und Rechtslage abstützt, auf höchstens fünf Jahre befristet werden muss und einer umfassenden Prüfung vor Bundesverwaltungsgericht zugänglich ist, dessen Entscheid an das Bundesgericht weitergezogen werden kann. Auch dürfen einzig Tätigkeiten verboten werden, welche die innere oder äussere Sicherheit konkret bedrohen und dazu dienen, terroristische oder gewalttätig-extremistische Aktivitäten zu fördern. Damit beschränkt sich das Verbot gegenüber der betroffenen Person auf Tätigkeiten, die die Sicherheit der Schweiz konkret bedrohen. In allen anderen Tätigkeiten bleibt die betroffene Person frei.

Bei der periodischen Überprüfung eines Tätigkeitsverbots ist vorab zu prüfen, ob die Sicherheit der Schweiz immer noch gefährdet wäre, wenn die Person die verbotene Tätigkeit wieder ausüben würde, bzw. ob die äusseren Umstände immer noch so sind, dass eine Wiederaufnahme dieser Tätigkeit wahrscheinlich ist (z.B. Fortbestehen eines bewaffneten Konflikts im Ausland). Nicht ausschlaggebend ist, ob die Person das Verbot befolgt hat. Verstösse gegen das Verbot wären strafrechtlich zu ahnden, während die Einhaltung des Verbots das beabsichtigte Ergebnis ist und nicht für sich alleine zu dessen Aufhebung führen kann. Die Praxis zum heutigen Tätigkeitsverbot nach BWIS hat gezeigt, dass die zu überprüfenden sicherheitspolitischen Verhältnisse nicht so rasch ändern, als dass sie einer halbjährlichen Überprüfung bedürfen. Die neue Verordnung sieht deshalb ein jährliches Prüfintervall vor.

5. Kapitel: Dienstleistungen und Gebühren

Art. 43 Gebühren

Die vom NDB im ausschliesslichen Interesse Dritter erbrachten Dienstleistungen sind grundsätzlich gebührenpflichtig. Da dies nicht immer angemessen scheint, sieht die Verordnung vor, dass unter bestimmten Voraussetzungen ganz darauf verzichtet oder die Gebühr zumindest reduziert werden kann. So wenn beispielsweise die Erhebung der Gebühr mehr Aufwand verursacht, als die Dienstleistung überhaupt kostet, oder wenn andere Gründe bei der Dienstleistung oder beim Gebührenpflichtigen die Erhebung einer Gebühr als unverhältnismässig erscheinen lassen.

6. Kapitel: Kontrolle

Art. 44 Selbstkontrolle innerhalb des NDB

Absatz 2 schafft eine Verpflichtung für den NDB eine Kontrolle über alle Informationsbeschaffungen mit technischen Mitteln zu führen. Dies schafft eine Schnittstelle zur VIS-NDB: Der NDB betreibt mit der Applikation SCC (Sensor Control Center) das Informationssystem ISCO (Funk- und Kabelaufklärung, vgl. Art. 55ff. VIS-NDB). Diese Applikation ist auch geeignet für die Steuerung von weiteren Sensoren (IMINT, TECHINT). Die dabei anfallenden Daten gehören aber nicht zu ISCO , weshalb sie nicht in den besonderen Bestimmungen zu ISCO geregelt werden können. Da sich auch weder der allgemeine Teil der VIS-NDB, noch die Bestimmungen zu GEVER für eine Regelung dieser Anwendung der Applikation eignen, wurde sie als Pflicht zur Selbstkontrolle in Artikel 44 aufgenommen. Sie betrifft nur die Daten zur Sensorsteuerung. Die Bearbeitung von Personendaten, die aus dieser Informationsbeschaffung resultieren, richtet sich nach den Bestimmungen der VIS-NDB.

7. Kapitel: Interne Schutz und Sicherheitsmassnahmen

Die Verordnung übernimmt für die Schutz und Sicherheitsmassnahmen weitgehend den Regelungsgehalt der bewährten, heute bereits auf Weisungsebene bestehenden Vorschriften und der geübten Praxis.

Art. 46 Durchführende Stelle

Der Verordnungsentwurf sieht vor, dass der NDB für Taschen-, Personen- und Raumkontrollen Dritte beiziehen kann. Es geht also nicht um die Abgabe der Verantwortung für die Durchführung der Massnahme (die vollumfänglich beim NDB bleibt), sondern um den Beizug von unter der Verantwortung des NDB agierenden Unterstützungskräften. Wenn auch nicht in der Verordnung ausdrücklich vorgesehen, sind Ort und Zeit entsprechender Kontrollen festzuhalten und allfällige besondere Vorkommnisse sind so genau wie möglich zu dokumentieren und schriftlich zu protokollieren.

Art. 47 Taschen- und Personenkontrollen

Die im NDG verankerte Befugnis des NDB zur Durchführung von Taschen- und Personenkontrollen schliesst im Rahmen des Verhältnismässigkeitsprinzips den zur Umsetzung und nötigenfalls auch Durchsetzung erforderlichen Zwang mit ein. Der NDB kann somit die Kontrollen selbst durchführen. Ergibt sich aus der Kontrolle, dass ein Verdacht auf eine strafbare Handlung vorliegt (z.B. Datendiebstahl), ist der NDB gestützt auf Artikel 218 StPO befugt, eine auf frischer Tat ertappte Person bis zum Eintreffen der Polizei festzuhalten (vorläufige Festnahme als "Jedermanns recht"), wobei er auch hier das Verhältnismässigkeitsprinzip beachten muss. Die Massnahme darf nur eingesetzt werden, wenn sie unbedingt nötig ist und Gewalt darf nur als äusserstes Mittel angewendet werden (Art. 200 StPO). Genügt eine mildere Massnahme, um die Person der Strafverfolgung zuzuführen, so ist ein Festhalten nicht erlaubt. Als weitere Schutzmassnahme soll auch ausgehende Post stichprobenweise auf ihren Inhalt hin überprüft werden können. Eine Verletzung des Brief-, Post- und Fernmeldeverkehrs

liegt hier nicht vor, weil die Kontrolle nicht private Post, sondern die Amtspost des NDB betrifft (NDB als Absender öffnet von ihm zum Versand vorgesehene eigene Post).

Art. 50 Einsatz von Bildübertragungs- und Bildaufzeichnungsgeräten sowie Mitführen von elektronischen Geräten

Die wichtigsten Neuerungen betreffen den Einsatz von Bildübertragungs- und Bildaufzeichnungsgeräten bei Archiv-, Tresor- und Lagerräumen sowie bei Zutrittszonen zu Räumlichkeiten des NDB. Hier präzisiert die Verordnung, dass betroffene Personen einerseits mit einem gut sichtbaren Hinweisschild auf Bildübertragungs- bzw. Bildaufzeichnungsgeräte hinzuweisen sind, und dass andererseits die Aufnahmen bei Nichtgebrauch rasch, d.h. nach 30 Tagen zu löschen sind, es sei denn, eine Aufnahme werde zur Beweissicherung bei einem Missbrauchsfall benötigt. In diesem Fall darf die Aufnahme bis zum rechtskräftigen Abschluss des entsprechenden Verfahrens aufbewahrt werden. Die Frist von 30 Tagen ist angemessen, weil es nicht - wie beim Einsatz von Videosystemen normalerweise üblich - um die Abwehr von Vandalenschäden geht, sondern um die Verhinderung bzw. rückwirkende Aufklärung von Datendiebstählen oder -manipulationen, bis zu deren Entdeckung eine gewisse Zeit verstreichen kann.

8. Kapitel: Bewaffnung

Die Verordnung übernimmt für die Bewaffnung weitestgehend den Regelungsgehalt der heutigen Vorschriften.

Art. 52 Berechtigung zum Tragen einer Dienstwaffe

Gemäss Artikel 3 NDG bestimmt der Bundesrat die Kategorie von waffentragenden Mitarbeiterinnen und Mitarbeiter. Dies sind die Mitarbeitenden des NDB, die im Rahmen ihrer dienstlichen Funktion und Aufgabe besonderen Gefährdungen ausgesetzt sind. Der Direktor NDB erteilt die Berechtigung zum Tragen einer Dienstwaffe, wenn er die Zugehörigkeit zur entsprechenden Kategorie festgestellt hat. Als Dienstwaffe gelten wie bisher Reizstoffe und Feuerwaffen, deren Einsatz einzig zum Selbstschutz bzw. nur in Fällen von Notwehr und Notstand zulässig ist und dem Verhältnismässigkeitsgebot Rechnung tragen muss.

9. Kapitel: Schlussbestimmungen

Art. 57 Übergangsbestimmung zur Archivierung

Das Schweizerische Bundesarchiv unterbreitet der abliefernden Stelle Einsichtsgesuche nach Artikel 13 des Archivierungsgesetzes vom 26. Juni 1998[7] (BGA) in Archivgut, das einer laufenden Schutzfrist unterliegt. In der Folge prüft die abliefernde Stelle, ob das Archivgut der einsichtsgesuchstellenden Person trotz laufender Schutzfrist gestützt auf Artikel 13 BGA herausgegeben werden kann. Für die Einsicht nach Artikel 13 BGA in Archivgut, das von einem ausländischen Sicherheitsdienst stammt, konsultiert der NDB auch diesen Dienst.

Artikel 68 Absatz 2 NDG regelt die Archivierung der Unterlagen, die von ausländischen Sicherheitsdiensten stammen. Demnach kann der Bundesrat die Schutzfrist für Archivgut, das von ausländischen Sicherheitsdiensten stammt, mehrmals befristet verlängern, wenn der betroffene ausländische Sicherheitsdienst Vorbehalte gegen eine allfällige Einsichtnahme geltend macht. Diese Bestimmung entspricht dem (noch) geltenden Artikel 7*a* Absatz 2 des Bundesgesetzes vom 3. Oktober 2008[8] über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG). Der NDB kennzeichnet Archivgut, das von ausländischen Sicherheitsdiensten stammt, bei der Ablieferung, damit nach Ablauf der 50-jährigen Schutzfrist überprüft werden kann, ob die Schutzfrist allenfalls zu verlängern ist. Eine Verlängerung erfolgt nur dann, wenn der betroffene ausländische Dienst dies ausdrücklich verlangt. Es ist Aufgabe des NDB, den betroffenen ausländischen Dienst zu konsultieren. Welche Verlängerung der Schutzfrist angemessen ist, entscheidet der Bundesrat.

Für Archivgut, das bereits abgeliefert wurde und nach Inkrafttreten des NDG noch unter einer Schutzfrist liegt, wird im Einverständnis mit dem Bundesarchiv und dem Bundesamt für Justiz eine Übergangsregelung eingeführt (Art. 57). Gemäss dieser Übergangsregelung wird die Schutzfrist für alle Dossiers mit laufender Schutzfrist (d.h. nicht nur für diejenigen, die Meldungen ausländischer Sicherheitsdienste enthalten) um 30 Jahre verlängert (unter entsprechender Benachrichtigung des Bundesarchivs). Damit kann der NDB künftig überprüfen, ob diese Dossiers noch schutzwürdige Informationen von ausländischen Sicherheitsdiensten enthalten.

Diese Verlängerung bedeutet nicht, dass der Zugang zu dem davon betroffenen Archivgut in jedem Fall verweigert wird, sondern lediglich, dass das Bundesarchiv die abliefernde Stelle kontaktieren muss. Diese prüft dann, ob das Archivgut trotz laufender Schutzfrist der einsichtsgesuchstellenden Person herausgegeben werden kann.

Anhang 4: Aufhebung und Änderung anderer Erlasse

I

1. BWIS-Abgeltungsverordnung vom 1. Dezember 1999

Mit der Schaffung des NDG fallen die meisten Regelungsinhalte der Verordnung vom 1. Dezember 1999[9] über die finanziellen Leistungen an die Kantone zur Wahrung der inneren Sicherheit (BWIS-Abgeltungsverordnung) weg, weshalb die verbleibenden Artikel 3, 4 und 4*a* neu in der Verordnung vom 27. Juni 2001[10] über das Sicherheitswesen in

---

7 SR **152.1**
8 SR **121**
9 SR **120.6**
10 SR **120.72**

Bundesverantwortung (VSB) respektive Artikel 5 der Verordnung vom 30. November 2001[11] über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei geregelt werden sollen. Somit kann die BWIS-Abgeltungsverordnung aufgehoben werden.

II:

2. Verordnung vom 27. Juni 2001 über das Sicherheitswesen in Bundesverantwortung

Die Änderung der VSB ist durch die Änderung des BWIS im Rahmen des NDG bedingt. Durch materielle Änderungen ergeben sich zudem formelle Anpassungen.

Artikel 2 Absatz 4 enthält die bisherige Regelung von Artikel 3 Absatz 2 Buchstabe a.

Artikel 3 erhält einen neuen Sachtitel und beschränkt sich somit auf Ausführungen betreffend Hausrecht. Absatz 1 übernimmt die konkrete Bestimmung, wer das Hausrecht ausübt, aus dem bisherigen Gesetzestext (Art. 23 Abs. 2 BWIS), der neu nur noch allgemein („Bund“) formuliert ist. Absatz 2 übernimmt den Inhalt des bisherigen Absatzes 1. Der bisherige Absatz 2 Buchstabe b muss aufgehoben werden, weil die entsprechende gesetzliche Grundlage aufgehoben wird (bisheriger Art. 23 Abs. 1 Bst. c BWIS).

Die Artikel 6 Absätze 1bis und 1ter sowie 7 Absatz 1bis werden der neuen gesetzlichen Grundlage (Art. 23 Abs. 1bis BWIS) angepasst. Die völkerrechtlich geschützten Personen werden in Artikel 6 Absatz 1bis Buchstabe c separat aufgeführt, da für sie andere rechtliche Grundlagen gelten, insbesondere verschiedene internationale Abkommen[12] und internationales Gewohnheitsrecht, in Verbindung mit Artikel 4 Gaststaatgesetz vom 22. Juni 2007[13] sowie Artikel 24 BWIS.

Durch die Aufhebung der BWIS-Abgeltungsverordnung werden die Bestimmungen über die Abgeltung an Kantone, die in grossem Ausmass Leistungen für den Schutz von Personen und Gebäuden erbringen (Art. 28 Abs. 2 BWIS), neu in der VSB ausgeführt. Die neuen Artikel 12*a*–12*c* VSB entsprechen den bisherigen Artikeln 3–4*a* der BWIS-Abgeltungsverordnung

Artikel 13 führt die mit den Artikeln 23*a*–23*c* BWIS neu geschaffene formell-gesetzliche Grundlage aus. Es geht um das Informations- und Dokumentationssystem des Bundessicherheitsdienstes (BSD) von fedpol. Der BSD benötigt und bearbeitet Daten über sicherheitsrelevante Ereignisse und damit in Verbindung stehende Personen zur Wahrnehmung seines Schutzauftrags nach dem 5. Abschnitt des BWIS.

Auf die bisherigen konkreten Verweise in Artikel 15 Absätze 2 und 3 (auf Art. 23 Abs. 2 BWIS bzw. Art. 20 der Verordnung vom 14. Juni 1993[14] zum Bundesgesetz über den Datenschutz und Art. 23 der Bundesinformatikverordnung vom 9. Dezember 2011[15] wird verzichtet, da diese Erlasse geändert oder aufgehoben wurden. Der Verweis in Absatz 3 zur Datensicherheit umfasst sämtliche datenschutzrelevanten Bestimmungen. Zur Anpassung an aktuelle Gegebenheiten wird in Absatz 2 ergänzt, dass Hausrechtsinhaber beim BSD den Einsatz von Videokameras nicht nur innerhalb, sondern auch ausserhalb des Gebäudes beantragen können, um die nahe Umgebung des Gebäudes zu überwachen. Die neue Regelung in Artikel 23*a* Absatz 3 BWIS, wonach Daten spätestens fünf Jahre, nachdem der Schutzbedarf nicht mehr gegeben ist, vernichtet werden müssen, muss für Bildaufzeichnungen konkret geregelt werden. Die bisher in Absatz 5 festgelegte Frist zur Vernichtung von Bildaufzeichnungen mit personenbezogenen Daten (spätestens 14 Tage seit der Aufzeichnung) hat sich in den Fällen, in welchen die Daten aufgrund eines Straf-, Zivil- oder Verwaltungsverfahrens sichergestellt wurden, als deutlich zu kurz erwiesen. Gemäss Artikel 15 Absatz 4 dürfen die Daten vom BSD nämlich nur gestützt auf eine richterliche Verfügung herausgegeben werden. Dass bei einem Ereignis (z. B. Einbruch) das Entdecken, Abklären, Anzeigen und Erwirken einer richterlichen Verfügung innerhalb von 14 Tagen seit dem Ereignis erfolgen kann, ist in der Praxis kaum möglich. Deshalb wird die Frist auf 30 Tage verlängert. Die Daten müssen demnach nicht schon nach 14 Tagen vernichtet werden.

5. Verordnung vom 30. November 2001 über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei

Wie unter Ziffer 1 bereits erwähnt, wird der Inhalt des bisherigen Artikels 5 der BWIS-Abgeltungsverordnung neu in Artikel 10a der Verordnung vom 30. November 2001 über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei geregelt.

7. Verordnung vom 15. Oktober 2008über das automatisierte Polizeifahndungssystem

Der NDB hat zur Abwehr von Gefahren für die öffentliche Sicherheit nach Massgabe des NDG gemäss Artikel 5 Buchstabe j der Verordnung vom 15. Oktober 2008[16] über das automatisierte Polizeifahndungssystem (RIPOL-Verordnung) Zugriff auf RIPOL zur Feststellung des Aufenthaltsortes von Personen und des Standortes von Fahrzeugen sowie neu zur verdeckten Registrierung oder zur gezielten Kontrolle von Personen und Fahrzeugen. Diese Änderung geht auf die Anpassung von Artikel 15 Absatz 4 Buchstabe i des Bundesgesetzes vom 13. Juni 2008[17] über die polizeilichen Informationssysteme des Bundes zurück.

---

11 SR **360.1**
12 Art. 39 Wiener Übereinkommen vom 18.4.1961 über diplomatische Beziehungen (SR **0.191.01**);
Art. 53 Wiener Übereinkommen vom 24.4.1963 über konsularische Beziehungen (SR **0.191.02**);
Art. 43 Übereinkommen vom 8.12.1969 über Sondermissionen (SR **0.191.2**)
13 SR 192.12
14 SR **235.11**
15 SR **172.010.58**
16 SR **361.0**
17 SR **361**

8. Verordnung vom 8. März 2013 über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro

Die zuständigen Einheiten des NDB haben gemäss Artikel 7 Buchstabe h der Verordnung vom 8. März 2013[18] über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro für den Vollzug des NDG Zugriff auf Daten des SIS zur Feststellung des Aufenthaltsortes von Personen und des Standortes von Fahrzeugen sowie neu zur verdeckten Registrierung oder zur gezielten Kontrolle von Personen und Fahrzeugen.

13. Verordnung vom 9. März 2007 über Frequenzmanagement und Funkkonzessionen

Die Anpassung der Verordnung vom 9. März 2007[19] über Frequenzmanagement und Funkkonzessionen (FKV) gründet auf Artikel 7 Absatz 1 Buchstabe d NDG in Verbindung mit Artikel 34 Absatz 1ter des Fernmeldegesetzes vom 30 April 1997[20] (Fassung gemäss Anhang Ziff. 13 des NDG), der Schutz- und Sicherheitsmassnahmen von Mitarbeitenden des NDB, seiner Einrichtungen und der von ihm bearbeiteten Daten betrifft. Folglich bilden die Bestimmungen in der Verordnung keine eigenständige Regelung, sondern enthalten zusätzliche Einschränkungen gegenüber den in den beiden Gesetzen vorgesehenen Voraussetzungen des Einsatzes von störenden Fernmeldeanlagen. So darf der NDB die Anlagen immer nur zur Gewährleistung des Schutzes und der Sicherheit seiner Mitarbeiterinnen und Mitarbeiter, Informationen und Einrichtungen einsetzen und nicht zu anderen Zwecken, auch wenn diese Einschränkung in Artikel 51 Absatz 3 FKV nicht explizit genannt wird. Zudem darf er auch mobile Anlagen aufgrund von Artikel 7 Absatz 1 Buchstabe d NDG nur in von ihm genutzten Räumlichkeiten einsetzen.

3 Erläuterungen zu den Bestimmungen der VIS-NDB

Zur Struktur

Die Struktur des Entwurfs wurde grundsätzlich von der heute geltenden Verordnung vom 8. Oktober 2014[21] über die Informationssysteme des Nachrichtendienstes des Bundes (ISV-NDB) übernommen. Die allgemeinen Bestimmungen wurden allerdings aus Gründen der Transparenz und Systematik aufgeteilt in allgemeine Bestimmungen zur Datenbearbeitung und Archivierung und solche zu Datenschutz und Datensicherheit.

Die besonderen Bestimmungen zu den Informationssystemen des NDB befinden sich in den Abschnitten 4-12. In Abschnitt 13 werden die Speichersysteme geregelt und in Abschnitt 14 befinden sich die Schlussbestimmungen. Der Katalog der Personendaten sowie die individuellen Zugriffsberechtigungen der Informations- und Speichersysteme werden in den Anhängen 1-13 geregelt.

1. Abschnitt: Gegenstand und Begriffe

Art. 1 Gegenstand

In Artikel 1 werden die Informations- und Speichersysteme aufgeführt, die in der vorliegenden Verordnung geregelt werden. Die Informationssysteme finden ihre formell gesetzliche Grundlage in den Artikeln 47ff. NDG, die Speichersysteme in den Artikeln 36 Absatz 5 und 58 NDG.

Art. 2 Begriffe

Die Begrifflichkeiten wurden weitgehend aus der geltenden ISV-NDB übernommen.

Neu hinzugefügt wurden die Begriffe „Ablage“ und „Erfassung“.

2. Abschnitt: Allgemeine Bestimmungen über die Datenbearbeitung und Archivierung

Die Regelungen in Artikel 3 und 4 entsprechen der durch das NDG vorgegebenen Unterscheidung zwischen der reinen Ablage von Informationen und deren personenbezogenen Erfassung. Es handelt sich dabei um ein vom Verhältnismässigkeitsprinzip des Verwaltungshandelns geprägtes, abgestuftes Vorgehen.

Die Ablage der Daten durch die Triage ist der erste Schritt der Datenbearbeitung beim NDB. Dabei entfalten die Daten noch keinerlei Aussenwirkungen. Die Prüfung der Erheblichkeit und Richtigkeit erfolgt in diesem Stadium nur aufgrund der Quellenqualität und der Übermittlungsart. In einem zweiten Schritt, wenn die Daten zu ihrer Auswertung personenbezogen erfasst werden sollen, erfolgt dann eine inhaltliche Einzelbeurteilung der Erheblichkeit und Richtigkeit der abgelegten Daten durch die zuständigen Mitarbeitenden.

Die vorgeschlagene Regelung steht im Einklang mit dem NDG, dessen Wortlaut leider aufgrund der mehrfachen sprachlichen Überarbeitungen im Gesetzgebungsprozess nicht mehr stringent ist. Bei einer künftigen Revision des NDG wird darauf zu achten sein, dass die Unterscheidung zwischen Ablage und Erfassung begrifflich wieder konsequent umgesetzt wird.

Art. 3 Ablage von Originaldokumenten in der Aktenablage

In Absatz 1 ist vorgesehen, dass die Mitarbeiterinnen und Mitarbeiter der Triage bei der Zuweisung der Originaldokumente zu den Informationssystemen nach Artikel 1 Absatz 1 prüfen, ob genügend Anhaltspunkte bestehen, dass der Aufgabenbezug nach Artikel 6 NDG gegeben ist, die Datenbearbeitungsschranke von Artikel 5 Absatz 5 NDG eingehalten

---

18 SR **362.0**
19 SR **784.102.1**
20 SR **784.10**
21 SR **121.2**

wird und ob die in den Originaldokumenten enthaltenen Informationen aufgrund der Quellenqualität und der Übermittlungsart richtig und erheblich sind.

Da die Anzahl der beim NDB eingehenden Meldungen hoch und die Qualität unterschiedlich ist, ist eine Überprüfung der vorgenannten Kriterien vor der eigentlichen Bearbeitung oft gar nicht möglich. Die Überprüfung des Inhalts einer eingegangenen Meldung ist im Gegenteil oft gerade der Kern der nachrichtendienstlichen Arbeit. Diese kann jedoch nur dann getan werden, wenn die Meldung bereits in einem Informationssystem abgelegt wurde. Die Mitarbeiterinnen und Mitarbeiter der Triage können aber bspw. die Daten liefernden Quellen bestens einschätzen und sind in der Lage, aufgrund des Betreffs einer Meldung die vorgenannte Prüfung vorzunehmen. Zum Teil handelt es sich bei den eingehenden Meldungen um Antworten oder Ergebnisse von Aufträgen, was diese Beurteilung erleichtert. Ob die Prüfung der Richtigkeit und Erheblichkeit bereits zum Zeitpunkt der Ablage praktikabel und umsetzbar ist, wird sich zeigen müssen, da eine solche Prüfung oft nur im Kontext mit weiteren Informationen sinnvoll durchgeführt werden kann. Auch der externe Datenschutzbeauftragte des NDB, Alt-Ständerat Hansruedi Stadler, äusserte erhebliche Bedenken bezüglich der Praktikabilität und Umsetzbarkeit dieser in Artikel 45 Absatz 1 NDG statuierten Prüfungspflicht.

Meldungen, die Daten zu mehreren Personen enthalten, werden als Ganzes beurteilt (Abs. 4). Ist es aufgrund der jährlichen Priorisierung offensichtlich, dass ein Originaldokument im integralen Analysesystem (IASA NDB) abgelegt werden muss, wird das Originaldokument direkt zugewiesen (Abs. 5).

Sollten die Mitarbeiterinnen und Mitarbeiter der Eingangstriage Zweifel haben, sind sie gehalten, die eingehenden Originaldokumente inhaltlich zu prüfen. Sie können dabei auch die Mitarbeiterinnen und Mitarbeiter der Datenerfassung oder Spezialisten aus anderen Bereichen beiziehen (Abs. 2). Wie heute sind die Originaldokumente bei negativem Befund zu vernichten oder zurückzuschicken, wenn diese von einer kantonalen Vollzugsbehörde stammen. Die gleiche Prüfung ist von den kantonalen Vollzugsbehörden vorzunehmen, wenn sie Originaldokumente im INDEX NDB im Bereich der Vorabklärungen oder der Auftragsverwaltung ablegen (vgl. Abs. 6).

Der Einsatz der OCR-Technik (Abs. 7) entspricht geltendem Recht, d.h. der NDB kann die vollständigen Inhalte der abgelegten Dokumente durchsuchen, soweit diese durch die Schriftzeichenerkennung automatisch erschlossen werden konnten (beispielsweise schlecht lesbare Vorlagen oder handschriftliche Dokumente können nicht eingelesen werden). Sie führt dazu, dass das Auskunftsrecht uneingeschränkt für alle Personen gilt, die mittels Freitextsuche in den Systemen gefunden werden können und dass bei der Löschung einer Person aus IASA/IASA-GEX alle Textpassagen zu ihr aus den durchsuchbaren Meldungen gelöscht werden müssen. Zudem dürfen keine Meldungen, welche die politische Betätigung von Personen betreffen, für eine Textsuche zugänglich sein, wenn nicht der Verdacht besteht, dass diese Personen die Tätigkeiten zu sicherheitsbedrohenden Zwecken missbrauchen.

Art. 4 Einzelbeurteilung und personenbezogene Erfassung

Gemäss Artikel 45 Absatz 1 und 2 NDG hat der NDB die Erheblichkeit, Richtigkeit und den Aufgabenbezug nach Artikel 6 NDG der Personendaten zu beurteilen, bevor er diese in einem seiner Informationssysteme erfasst. Diese Pflicht trifft nicht nur die für die Datenerfassung zuständigen Mitarbeiterinnen und Mitarbeiter des NDB (vgl. Abs. 1), sondern neu auch diejenigen der kantonalen Vollzugsbehörden bei der personenbezogenen Erfassung im INDEX NDB im Bereich der Vorabklärungen oder der Auftragsverwaltung (Abs. 3). Dies bedingt, dass die Mitarbeiterinnen und Mitarbeiter der kantonalen Vollzugsbehörden auch entsprechend geschult werden. Wie heute sind die Daten bei negativem Befund zu vernichten oder zurückzuschicken, wenn diese von einer kantonalen Vollzugsbehörde stammen, damit diese ihre Datenhaltung anpassen können (Abs. 2). Ist bei einer Meldung kein Bezug zum Aufgabengebiet des NDB gegeben, muss auch die kantonale Vollzugsbehörde ihre Daten löschen, ausser das Originaldokument wird vom NDB zurückgeschickt, damit sie von der kantonalen Vollzugsbehörde verdichtet und mit weiteren Abklärungen angereichert wird.

In Abs. 4 wird klargestellt, dass sämtliche Berichte der kantonalen Vollzugsbehörden personenbezogen in IASA NDB oder IASA-GEX NDB erfasst werden. Dabei werden diese gemäss Abs. 1 geprüft.

Art. 5 Erteilung und Entzug der Zugriffsrechte

Wie im heute geltenden Recht (vgl. Art. 3 ISV-NDB) wird eine Zugriffsberechtigung für ein Informationssystem auf individuellen Antrag und für eine bestimmte Einzelperson erteilt (vgl. Abs. 1). Dies gilt neu auch für die Speichersysteme gemäss Artikel 1 Absatz 2 des vorliegenden Verordnungsentwurfs. Als Ausnahme kann für ELD der Zugriff auch funktionsbezogen erfolgen. Typischerweise muss bei der ELD bei besonderen Ereignissen rasch einem nicht vorher namentlich bekannten Personenkreis der Zugriff gewährt werden können. In Einsatzzentralen und Pikettdiensten greifen ständig wechselnde Personenkreise auf ELD zu. Die Zugriffserteilung auf individueller Ebene ist hier mit verhältnismässigem Aufwand nicht möglich. Aber es erfolgt eine Individualisierung auf funktionaler Ebene. Das Zugriffsprofil ist zunächst auf die Funktion ausgestellt und wird bei der Benutzung einer individuellen Person zugeordnet. Die Benutzerorganisation ist deshalb verpflichtet zu dokumentieren, welche Person wann die Funktion ausgeübt hat, in der sie berechtigt war, auf die ELD zuzugreifen. Damit ist die Nachvollziehbarkeit der Zugriffe jederzeit gewährleistet.

Neu wird explizit geregelt, dass der Antrag nicht nur die Personalien und die Funktion der Antrag stellenden Person enthalten, sondern dass er auch den Bezug zu einem im NDG verankerten Nutzungszweck ausweisen muss (vgl. Abs. 2). Dies entspricht geltender Praxis und ist eine Voraussetzung für die formelle Prüfung.

Art. 6 Systemübergreifender Zugriff und temporäre Auswertung

Die Daten des NDB werden in einem Verbund von Informationssystemen bearbeitet (vgl, Botschaft zum NDG, BBl 2014 2105 zu Art. 43 Entwurf NDG). Auf diese Weise soll erreicht werden, dass die Daten unterschiedlichen Bearbeitungsregeln in den einzelnen Systemen unterstehen und dennoch gemeinsam ausgewertet werden können, um das Ziel der umfassenden Beurteilung der Bedrohungslage zu erreichen. Die schon heute in ISIS und ISAS praktizierte Vernetzung von Personendatensätzen soll deshalb mit IASA-GEX NDB und IASA NDB weitergeführt werden. Dies ist insbesondere deshalb

gerechtfertigt, weil der Benutzerkreis und die Zugriffsberechtigungen in beiden Systemen gleich sind, nämlich die Mitarbeitenden des NDB. Zu berücksichtigen ist auch, dass es zwischen den thematischen Gebieten der Systeme IASA NDB (u.a. Terrorismus, Krisengebiete und bewaffnete Konflikte im Ausland) und IASA-GEX NDB (Gewaltextremismus Schweiz) zahlreiche Bezugspunkte gibt. Gewaltextremistische Gruppierungen in der Schweiz pflegen teilweise enge Beziehungen zu terroristischen oder anderen bewaffneten Gruppen im Ausland. Es ist deshalb notwendig, bei der Auswertung der Daten auch systemübergreifend arbeiten zu können. Damit vermeidet der NDB auch Doppelerfassungen derselben Personen in beiden Systemen, was mit der Systematik der inhaltlichen Zuweisung von IASA NDB und IASA-GEX NDB nicht vereinbar wäre.

Die entsprechende Grundlage im NDG ist unglücklich formuliert (vgl. Art. 44 Abs. 4) und hat insbesondere von Seiten der GPDel für Kritik gesorgt. Um zukünftig Klarheit zu erhalten, wird das NDG bei der nächsten Revision entsprechend angepasst. Mit diesem Vorgehen sind das Bundesamt für Justiz und die Sicherheitspolitischen Kommissionen einverstanden.

Die in den Absätzen 1 und 2 geregelten Berechtigungen zum systemübergreifenden Zugriff (betrifft alle Informationssysteme), zur systemübergreifenden Erfassung (betrifft nur IASA NDB und IASA-GEX NDB) sowie der Suche und Verteilung von Informationen entsprechen dem heutigen Recht (vgl. Art. 4 ISV-NDB). Die Speichersysteme gemäss Artikel 1 Absatz 2 sind davon ausgenommen, da diese nur den zuständigen Spezialisten offen stehen und nicht mit den Informationssystemen des NDB vernetzt werden sollen.

In Absatz 3 wird klargestellt, dass zur Steuerung der Informationsbeschaffung oder zur operativen Analyse im Rahmen von zeitlich befristeten Projekten (Task Forces, Arbeitsgruppen, etc.) vorübergehend Kopien von Daten der Informations- und Speichersysteme des NDB separat im SiLAN abgelegt und nur den Mitgliedern dieses Projekts zugänglich gemacht werden können. Diese temporären Auswertungen sind vom NDB besonders zu bewilligen. Welche Stelle diese Bewilligung NDB-intern erteilt, wird im Datenschutzkonzept des NDB ausgeführt werden. Nach Abschluss der Arbeiten überträgt der NDB alle Resultate in die regulären Informationssysteme des NDB und vernichtet die Datenkopien auf der Auswerteplattform.

Die Qualitätssicherungsstelle des NDB wird diese Auswertungen und ihre Notwendigkeit in ihre Stichprobenkontrolltätigkeit einbeziehen.

Temporäre Ablagen werden beispielsweise bei Entführungsfällen erstellt. Die Mitarbeitenden, die einen Fall bearbeiten, sind darauf angewiesen, sämtliche Informationen, die im Zusammenhang mit der Entführung stehen, aus allen Informationssystemen des NDB zusammenziehen und auf einer Plattform gemeinsam auswerten zu können.

Art. 7 Besonders sensitive Daten

Bei besonders sensitiven Daten (bspw. operativ notwendige Informationen zu menschlichen Quellen des NDB, zu deren Identität, Auswahl, Risikobeurteilung, Quellenführung, etc.) ist es regelmässig aus Gründen des Quellenschutzes gemäss Artikel 35 NDG unabdingbar, diese ausserhalb der Informationssysteme des NDB zu führen (vgl. Abs. 1). Dadurch kann sichergestellt werden, dass nur ein ganz enger Kreis von Personen auf diese heiklen Daten zugreifen kann, nämlich diejenige Personen, welche mit der Führung einer Operation beauftragt sind oder die Chefin oder der Chef der Beschaffung (vgl. Abs. 3).

Aus Sicherheitsgründen werden diese Daten in besonders geschützten Behältnissen (bspw. Safe) oder Räumlichkeiten (mit Zutrittsbeschränkungen) aufbewahrt (vgl. Abs. 2). Online-Abfragen über ein Netzwerk sind nicht möglich.

Die von den Quellen gelieferten nachrichtendienstlichen Erkenntnisse fliessen anonymisiert in Form von HUMINT-Berichten in die ND-relevanten Daten (IASA NDB oder IASA-GEX NDB) ein (vgl. Abs. 4). Das Auskunftsrecht betroffener Personen erstreckt sich somit über diese Systeme und die Speichersysteme der operationsbezogenen Daten.

Die Chefin oder der Chef des Direktionsbereichs Beschaffung ist verpflichtet, periodisch zu prüfen, ob die Daten im Hinblick auf die aktuellen Lage für die Aufgabenerfüllung des NDB gemäss Artikel 6 NDG noch benötigt werden (vgl. Abs. 6).

Wie heute dürfen diese Daten maximal 45 Jahre aufbewahrt werden (vgl. Abs. 7).

Von Seiten der GPDel und des EJPD wurde die fehlende formell-gesetzliche Grundlage dieser besonderen Bearbeitung kritisiert. Obwohl ein vom NDB in Auftrag gegebenes Gutachten zum Schluss gekommen ist, dass eine materiell-gesetzliche Grundlage ausreicht und die Datenbearbeitung korrekt erfolgt, wird bei der nächsten Revision des NDG eine formell-gesetzliche Grundlage geschaffen werden.

Art. 8 Löschen von Daten

Die Bestimmungen in diesem Artikel entsprechen dem heute geltenden Recht (vgl. Art. 7 ISV-NDB). Absatz 1 enthält keine inhaltlichen Neuerungen. Er stellt aber klar, dass der NDB alle gelöschten Daten in das Archivierungsmodul übertragen muss.

Die maximale Aufbewahrungsdauer wird bei den entsprechenden Informations- und Speichersystemen geregelt und ist je nach Herkunft, Zweck der Datenbearbeitung und Aufgabengebiet unterschiedlich (vgl. Abs. 2).

In IASA NDB und IASA-GEX NDB sind Objekte zu löschen, wenn diese nicht mehr mit inhaltlichen Informationen (Quellendokumenten) verbunden sind. Es soll keine Person verzeichnet sein, zu der man keine inhaltlichen Informationen hat und nicht mehr nachvollziehen kann, weshalb sie einst erfasst wurde (vgl. Abs. 3).

Analog dem heutigen ISIS dürfen in IASA-GEX NDB keine Originaldokumente abgelegt werden, ohne dass diese strukturiert durch Quellendokumente und Objekte erfasst werden (vgl. die neu explizite Regelung in Art. 24 Abs. 4). Dies heisst umgekehrt, dass ein Originaldokument gelöscht werden muss, nachdem das letzte darauf referenzierte Quellendokument gelöscht wurde (vgl. Abs. 4).

Diese Vorschrift existiert nicht für IASA NDB. Dort können auch nicht referenzierte Originaldokumente bei Bedarf bis zur maximalen Aufbewahrungsfrist aufbewahrt werden (vgl. Abs. 5).

Art. 9 Archivierung

Die Ablieferung von Daten aus den Informationssystemen des NDB zur Archivierung wird in Artikel 68 NDG ausführlich geregelt.

Gemäss Artikel 1 Absatz 1 Buchstabe h und Art. 4 Abs. 2 BGA fallen die Kantone, wenn sie Vollzugsaufgaben des Bundes erfüllen, nicht unter den Anwendungsbereich des BGA. Daten aus Vorabklärungen und Auftragsverwaltungsdaten der kantonalen Vollzugsbehörden fliessen in IASA NDB, IASA-GEX NDB oder ins Informationssystem zur Geschäftsverwaltung (GEVER) ein, wenn dies für die Aufgabenerfüllung des NDB nach Artikel 6 Absatz 1 NDG notwendig ist. Der NDB liefert sie über diese Informationssysteme zur Archivierung ab (vgl. Abs. 3). Eine Doppelablieferung würde keinen Sinn ergeben. Vorarbeiten der Kantone, die nicht genügend verdichtet werden konnten und deshalb keine über den Kanton hinausgehende Wirkung erzielt haben, sollen hingegen nicht abgeliefert werden, da sie offensichtlich nie Relevanz erlangt haben.

Daten, die gelöscht, jedoch nicht dem Schweizerischen Bundesarchiv abgeliefert werden müssen (bspw. Fehlerfassungen; Informationen, welche bereits durch andere Ämter abgeliefert werden; Informationen, welche in ein anderes Informationssystem übertragen und durch dieses abgeliefert werden; mangels Relevanz nicht Archivwürdig; etc.), gehören nicht in ein Archivierungsmodul und sind zu vernichten (vgl. Abs. 4).

3. Abschnitt: Allgemeine Bestimmungen über den Datenschutz und Datensicherheit

Art. 10 Auskunftsrecht von betroffenen Personen

Das Auskunftsrecht betroffener Personen wird ausführlich in Artikel 63 NDG geregelt. Ist die gesuchstellende Person im INDEX NDB in den Bereichen nach Artikel 29 Bst. b und c verzeichnet, hat der NDB der zuständigen kantonalen Vollzugsbehörde Gelegenheit zu geben, sich zur Auskunftserteilung zu äussern (vgl. Abs. 2)

Art. 11 Qualitätssicherung

Bei Artikel 11 handelt es sich um den zentralen Artikel zur Qualitätssicherung der Daten des NDB. Gemäss Artikel 45 Absatz 4 NDG hat der NDB periodisch in allen Informationssystemen zu prüfen, ob die erfassten Personendatensätze zur Erfüllung seiner Aufgaben weiterhin notwendig sind. Die Zuständigkeiten und Fristen sowie der Umfang der periodischen Prüfungen sind in den besonderen Bestimmungen des jeweiligen Informationssystems geregelt (vgl. Abs. 1). Eine periodische Überprüfung ist vorgesehen bei IASA NDB, IASA-GEX NDB, Quattro P und bei den KND-Berichten (vgl. Art. 33). Dort, wo es in einem Informationssystem keine Personendatensätze gibt und eine Überprüfung während der Aufbewahrungsfrist sinnvoll ist, wurde eine jährliche Überprüfung durch die Mitarbeiterinnen und Mitarbeiter vorgesehen, welche die betreffenden Daten abgelegt haben (GEVER, ELD und ISCO). Wo solche Überprüfungen nicht sinnvoll sind, wurden die Aufbewahrungsfristen massiv gekürzt (OSINT-Portal und Restdatenspeicher). Die Qualitätssicherungsstelle des NDB überprüft im Rahmen der Stichprobenkontrolle, ob die periodischen und jährlichen Überprüfungen vorschriftsgemäss durchgeführt, rechtzeitig gelöscht und die gelöschten Daten dem Bundesarchiv abgeliefert werden.

Der Absatz 2 entspricht im Prinzip dem heutigen Artikel 13 Absatz 4 ISV-NDB. Die Pflicht zur Stichprobenkontrolle wird jedoch auf die Datenbearbeitungen in sämtlichen Informationssystemen ausgedehnt (heute sind ISIS und das Informationssystem Äussere Sicherheit ISAS davon ausgenommen). Im Unterschied zur periodischen Überprüfung, wird die Stichprobenkontrolle ausschliesslich durch die Qualitätssicherungsstelle des NDB vorgenommen. Diese prüft nicht sämtliche Datensätze der Informationssysteme, sondern sorgt durch besonders zusammengestellte Stichproben dafür, dass sie zu einer repräsentativen Beurteilung der Datenqualität in den überprüften Systemen kommt. Das Resultat der Stichprobenkontrollen fliesst in Empfehlungen und in Schulungen insbesondere der erfassenden Stellen ein.

Wie heute überprüft die Qualitätssicherungsstelle NDB im ISIS jeweils nach der Genehmigung der Beobachtungsliste durch den Bundesrat die Datensätze zu Organisationen und Gruppierungen, welche von der Beobachtungsliste gestrichen wurden und löscht Daten, welche unter die Datenbearbeitungsschranke von Artikel 3 BWIS fallen. Neu wird dies sowohl IASA-GEX NDB als auch IASA NDB betreffen (Abs. 3).

Werden ausserhalb der Beobachtungsliste oder eines Prüfverfahrens ausnahmsweise Daten nach Artikel 5 Absatz 5 NDG beschafft und personenbezogen erschlossen, muss sichergestellt sein, dass diese gelöscht werden, wenn die in Artikel 5 Absatz 6 NDG aufgeführten Tätigkeiten ausgeschlossen werden können oder ein Jahr nach der Erschliessung der Daten nicht erwiesen sind. Die Qualitätssicherungsstelle NDB erhält deshalb neu den Auftrag, die Datensätze, welche solche Daten enthalten, mindestens einmal jährlich zu prüfen bzw. zu löschen (vgl. Abs. 4).

Die umfassendere Rolle der Qualitätssicherungsstelle des NDB wird weiter gestärkt mit dem Auftrag, mittels internen Schulungen und regelmässigen Kontrollen für die Einhaltung der Bestimmungen der vorliegenden Verordnung zu sorgen (vgl. Abs. 5).

Ebenfalls wie heute hat die Direktorin oder der Direktor des NDB die Möglichkeit, die Qualitätssicherungsstelle mit weiteren Überprüfungen in den Informationssystemen zu beauftragen (vgl. Abs. 6).

Art. 12 Verantwortung und Zuständigkeiten

Die Verantwortlichkeit und Zuständigkeiten haben sich nicht verändert. Die vorliegende Bestimmung entspricht dem heutigen Artikel 13 Absätze 1-3 ISV-NDB, ohne im Hinblick auf den Erlass der Bearbeitungsreglemente zu weit ins Detail zu gehen.

Art. 13 Datensicherheit

Die Bestimmungen zur Datensicherheit haben sich ebenfalls im Vergleich zu heute nicht verändert und entsprechen dem heutigen Artikel 8 ISV-NDB.

Art. 14 SiLAN

Die Nutzung und der Betrieb des SiLAN erfährt im Vergleich zu heute keine Änderung. Gemäss Absatz 2 darf der NDB im SiLAN weiterhin Daten aller Klassifizierungsstufen bearbeiten, d.h. bis zur Stufe GEHEIM. Das System ist entsprechend gesichert und verfügt über ein genehmigtes Informations- und Datenschutzkonzept.

Neu werden auch die Mitarbeiterinnen und Mitarbeiter der kantonalen Vollzugsbehörden Zugriff auf für sie bestimmte Teile des SiLAN haben, um dort ihre Vorabklärungen (KND INDEX), Berichte und die Auftragsverwaltung in einer besonders gesicherten IKT-Umgebung führen zu können (vgl. Abs. 3). Dies wurde nötig, da die KND gemäss Artikel 46 NDG keine eigenen Datensammlungen mehr führen dürfen.

Neu muss nicht mehr die Datenübermittlung zu den Kantonen finanziert werden, sondern deren Zugriff auf das SiLAN und die darin geführten Daten (vgl. Abs. 4).

Art. 15 Datenübermittlung ausserhalb von SiLAN

Auch diese Bestimmung entspricht weitgehend dem geltenden Recht (vgl. Art. 11 ISV-NDB).

4. Abschnitt: Besondere Bestimmungen über IASA NDB

Art. 16 Struktur

Die Struktur von IASA NDB entspricht derjenigen des heutigen ISAS bzw. ISIS. Der Index zur Feststellung, ob der NDB in IASA NDB Daten über eine natürliche oder juristische Person, ein Ereignis oder einen Gegenstand bearbeitet, wird neu separat im 6. Abschnitt der besonderen Bestimmungen zum INDEX NDB geregelt.

Art. 17 Inhalt

IASA NDB löst weitestgehend die heutigen Informationssysteme ISIS und ISAS ab. IASA NDB dient somit der nachrichtendienstlichen Erfassung, Recherche, Auswertung und Qualitätssicherung von Daten zu natürlichen und juristischen Personen, Gegenständen und Ereignissen aus allen Aufgabenbereichen des NDB mit Ausnahme desjenigen des gewalttätigen Extremismus (vgl. Abs. 1).

Die Absätze 2 und 4 entsprechen dem heute geltenden Recht und wurden von den Artikeln 16 Absätze 2 und 3 ISV-NDB übernommen. Auch weiterhin sollen Objekte und Quellendokumente sowie deren Relationen bildlich dargestellt und abgespeichert werden können. Der Katalog der Personendaten wird im Anhang 1 ausgewiesen. Die Datenfelder und die Organisationseinheiten, die darauf Zugriff haben, werden neu nicht mehr durch das Departement geregelt, sondern gemäss Artikel 21 Absatz 2 Buchstabe e der Verordnung vom 14. Juni 1993[22] zum Bundesgesetz über den Datenschutz, im Bearbeitungsreglement.

Der Absatz 3 wurde von Artikel 6c Absatz 2 ZNDG übernommen. Auch heute dürfen in ISAS (und ISIS) besonders schützenswerte Personendaten und Persönlichkeitsprofile bearbeitet werden. Dies soll auch in Zukunft möglich sein (vgl. Art. 44 Abs. 1 NDG).

Art. 18 Datenerfassung

Gemäss Artikel 45 Absatz 1 und 2 NDG und Artikel 4 Abs. 1 des vorliegenden Entwurfs haben die für die Datenerfassung zuständigen Mitarbeiterinnen und Mitarbeiter des NDB (und der kantonalen Vollzugsbehörden) vor jeder Erfassung in den Informationssystemen des NDB den Aufgabenbezug nach Artikel 6 NDG, die Erheblichkeit und die Richtigkeit der zu erfassenden Personendaten zu beurteilen und die Datenbearbeitungsschranke von Artikel 5 Absatz 5 NDG zu berücksichtigen. Dies gilt insbesondere auch für die Erfassung von Personendaten in IASA NDB (vgl. Abs. 1).

Zur Erleichterung der Auswertung der Daten einerseits und der späteren Qualitätssicherung andererseits sind zudem Daten zu kennzeichnen, die als Des- oder Falschinformationen erkannt wurden, jedoch erfasst werden, weil diese für die Beurteilung der Lage oder einer Quelle notwendig sind (vgl. Abs. 2 Bst. a und Art. 44 Abs. 2 NDG). Zu kennzeichnen sind aus diesem Grund aber auch Informationen, die ausnahmsweise gestützt auf Artikel 5 Absatz 6 NDG erhoben wurden (vgl. Bst. b) und Informationen, welche gestützt auf die Beobachtungsliste gemäss Artikel 72 NDG oder ein Prüfverfahren erhoben wurden (vgl. Bst. c).

Art. 19 Zugriffsrechte

Die Zugriffsrechte für IASA NDB sind in Artikel 49 Absatz 3 NDG geregelt, weshalb in Absatz 1 lediglich auf diese Bestimmung verwiesen wird. Die Zugriffsrechte stimmen mit den heutigen Zugriffen auf ISIS und ISAS überein. Die Zugriffsberechtigungen für den INDEX NDB werden neu separat im 6. Abschnitt der besonderen Bestimmungen zum INDEX NDB ausgewiesen.

Wie heute verweist Absatz 2 für eine Übersicht über die individuellen Zugriffsrechte auf den Anhang 2.

Art. 20 Periodische Überprüfung der Personendatensätze

In Absatz 1 wird die heutige Pflicht zur periodischen Überprüfung von Personendatensätzen in ISAS übernommen (vgl. Art. 18 Abs. 1 ISV-NDB). Der einzige Unterschied besteht darin, dass (wie in der ganzen Verordnung) statt von Personen oder Organisationen neu von natürlichen und juristischen Personen gesprochen wird. Diejenigen Fachbereiche, die für das Erfassen von Daten verantwortlich sind, führen weiterhin in ihrem Spezialgebiet die periodischen Überprüfungen der im IASA NDB gespeicherten Daten durch, was zu einem grösseren Einbezug des Sachwissens in die Qualitätssicherung führt.

Die Aufgaben, welche dabei von den überprüfenden Personen wahrzunehmen sind, haben sich im Vergleich zu heute auch grundsätzlich nicht verändert (vgl. Abs. 2 und Art. 18 Abs. 2 ISV-NDB). Es wird aber klargestellt, dass das Ergebnis der

[22] SR **235.11**

Überprüfung nur dann festgehalten werden muss, wenn der Personendatensatz verändert oder nicht gesamthaft gelöscht wird. Wird der Personendatensatz nicht verändert, wird die erfolgte Überprüfung automatisch vom System festgehalten. Zudem muss neu geprüft werden, ob die Datenbearbeitungsschranke von Artikel 5 Absatz 5 und 6 NDG eingehalten wird. Diese gilt heute noch nicht für ISAS.

Die heute geltende Regelung von Artikel 18 Absatz 3 ISV-NDB, wonach die periodische Überprüfung bei jeder Ergänzung eines Datensatzes durchgeführt werden muss, führte in der Praxis zu einer ineffizienten Bindung von Ressourcen und zu Doppelspurigkeiten, insbesondere dann, wenn der gleiche Personendatensatz mehrmals pro Tag durch verschiedene Mitarbeiterinnen und Mitarbeiter des NDB ergänzt und überprüft werden musste, weil mehrfach Meldungen dazu erfasst wurden (z.B. vor allem im Bereich Terrorismus täglich mehrere Meldungen zum „Islamischen Staat“ oder zur „Al Qaida“) . Um diese Unzulänglichkeiten zu beseitigen und im Hinblick darauf, dass ein Grossteil der ISIS-Daten inskünftig im IASA NDB bearbeitet werden, wurden für die periodische Überprüfung die heutigen ISIS-Regeln übernommen (vgl. Art. 25 ISV-NDB). Das heisst, die Personendatensätze sind spätestens dann zu überprüfen, wenn die Maximalfristen seit der Erfassung in einem Informationssystem oder der letzten periodischen Überprüfung abgelaufen sind (vgl. Abs. 3). Die Maximalfristen wurden hingegen von den heutigen Bestimmungen zu ISAS (Art. 18 Abs. 3 ISV-NDB) übernommen (10 Jahre im Bereich des internationalen Terrorismus, 15 Jahre in den Bereichen des verbotenen Nachrichtendienstes und der Weiterverbreitung von Massenvernichtungswaffen und 20 Jahre für die übrigen sicherheitspolitisch bedeutsamen Informationen). In Absatz 4 wird neu ausdrücklich geregelt, dass die kürzere Maximalfrist gilt, wenn ein Personendatensatz Quellendokumente aus verschiedenen Bereichen enthält und demnach verschiedene Maximalfristen aufweist.

Art. 21 Aufbewahrungsdauer

Die Aufbewahrungsdauern für Daten in IASA NDB entsprechen grundsätzlich denjenigen des heutigen ISAS (vgl. Art. 19 ISV-NDB). Neu wird analog dem heutigen ISIS und IASA-GEX NDB eine besondere Aufbewahrungsfrist für Einreisesperren eingeführt (vgl. Bst. c). Die Aufbewahrungsfrist für Originaldokumente, welche nicht mit einem Quellendokument verbunden sind, wird neu von 45 auf 15 Jahre reduziert.

5. Abschnitt: Besondere Bestimmungen über IASA-GEX NDB

Art. 22 Struktur

Die Struktur von IASA-GEX NDB entspricht derjenigen des heutigen ISAS bzw. ISIS. Der Index zur Feststellung, ob der NDB in IASA-GEX NDB Daten über eine natürliche oder juristische Person bearbeitet, wird neu separat im 6. Abschnitt der besonderen Bestimmungen zum INDEX NDB geregelt.

Art. 23 Inhalt

Die Daten von IASA-GEX NDB stammen zum grössten Teil aus dem heutigen ISIS. IASA-GEX NDB dient der nachrichtendienstlichen Erfassung, Recherche, Auswertung und Qualitätssicherung von Daten zu natürlichen und juristischen Personen, Gegenständen und Ereignissen aus dem Bereich des gewalttätigen Extremismus. Die in IASA-GEX NDB bearbeiteten Personendaten weisen entweder einen Bezug zu den vom Bundesrat gemäss Artikel 70 Absatz 1 Buchstabe c NDG bezeichneten Gruppierungen auf (vgl. Abs. 1 Bst. a) oder es handelt sich um Daten zu natürlichen und juristischen Personen, welche die Demokratie, die Menschenrechte und den Rechtsstaat ablehnen und zum Erreichen ihrer Ziele Gewalttaten verüben, befürworten oder fördern (vgl. Abs. 1 Bst. b). Weist eine natürliche oder juristische Person einen nur indirekten Bezug zu dem so definierten gewalttätigen Extremismus auf, kann sie in IASA-GEX NDB als Drittperson gekennzeichnet werden (vgl. Art. 2 Bst. g des Verordnungsentwurfs). Ihre Daten werden dann bei der ersten periodischen Überprüfung gelöscht (vgl. Art. 27 Abs. 4 des Entwurfs). Ein indirekter Bezug zum gewalttätigen Extremismus kann gegeben sein, wenn eine Person an Ereignissen aus dem Bereich des gewalttätigen Extremismus teilnimmt selber jedoch keine Gewalttaten verübt, diese aber mit ihrer Anwesenheit befürwortet oder fördert. Als Gewalttat gelten physische Angriffe auf Personen oder Einrichtungen wie etwa Gebäude, Infrastruktureinrichtungen oder Fahrzeuge sowie psychische Gewalt wie Nötigung oder Drohung.

Die Absätze 2 bis 4 finden sich im Artikel 22 Absätze 3 und 4 sowie Artikel 23 Absatz 4 ISV-NDB und entsprechen dem geltenden Recht. Die Datenfelder und die Organisationseinheiten, die darauf Zugriff haben, werden neu nicht mehr durch das VBS geregelt, sondern gemäss Artikel 21 Absatz 2 Buchstabe e der Verordnung vom 14. Juni 1993[23] zum Bundesgesetz über den Datenschutz, im Bearbeitungsreglement.

Art. 24 Datenerfassung

Der Absatz 1 wurde unverändert vom heutigen Artikel 23 Absatz 1 ISV-NDB übernommen und sieht vor, dass auch weiterhin vor jeder Erfassung einer neuen Information zwingend zu beurteilen ist, ob die neue Information die Relevanz der sie betreffenden natürlichen oder juristischen Person für die Wahrnehmung der nachrichtendienstlichen Aufgaben im Bereich des gewalttätigen Extremismus bestätigt oder verneint. Ist dies nicht der Fall, wird der Personendatensatz im IASA-GEX NDB gelöscht.

Wie bis anhin haben die für die Datenerfassung zuständigen Mitarbeiterinnen und Mitarbeiter zur Erleichterung der Auswertung der Daten einerseits und der späteren Erfassungskontrolle und Qualitätssicherung andererseits die Pflicht, die erfassten Daten zu bewerten und entsprechend zu kennzeichnen (vgl. Abs. 2). Dies wird (wie im IASA NDB) auf Stufe des Quellendokumentes getan und betrifft ungesicherte Informationen, Informationen, welche gestützt auf die Beobachtungsliste gemäss Artikel 72 NDG oder ein Prüfverfahren nach Artikel 37 NDV erhoben wurden und neu auch Des- oder Falschinformationen sowie Informationen, die ausnahmsweise gestützt auf Artikel 5 Absatz 6 NDG erhoben wurden.

Wie bereits erwähnt, sind Objekte zu natürlichen oder juristischen Personen, die nur einen indirekten Bezug zum gewalttätigen Extremismus aufweisen, als Drittpersonen zu kennzeichnen. Objekte zu natürlichen und juristischen Personen,

[23] SR **235.11**

die gestützt auf die Beobachtungsliste oder gestützt auf ein Prüfverfahren erfasst wurden oder die keiner vom Bundesrat gemäss Artikel 70 Absatz 1 Buchstabe c NDG bezeichneten Gruppierung angehören, sind ebenfalls zu kennzeichnen, damit dem Bundesrat die Anzahl dieser Objekte jährlich zur Kenntnis gebracht werden kann (vgl. Abs. 3). Objekte können nur zu natürlichen und juristischen Personen erstellt werden, von denen eine Gefährdung der Sicherheit der Schweiz angenommen wird.

In Absatz 4 wird neu explizit vorgeschrieben, dass in IASA-GEX NDB keine Originaldokumente abgelegt werden dürfen, ohne dass diese strukturiert durch Quellendokumente und Objekte erfasst werden. Dies gilt bereits heute im ISIS, konnte aber nur aus den Bestimmungen zur Löschung von ISIS-Daten abgeleitet werden (vgl. Art. 7 Abs. 4 ISV-NDB). Grund dafür ist die in IASA-GEX NDB vorgesehene Erfassungskontrolle, die nur dann durchgeführt werden kann, wenn die relevanten Personendaten der Originaldokumente strukturiert (mit Quellendokument, Objekt und Relationen) erfasst werden.

Wie heute im ISIS werden die Daten in IASA-GEX NDB zunächst provisorisch erfasst und wechseln ihren Status erst nach der Erfassungskontrolle auf definitiv (vgl. Abs. 5).

Sollten in einem Originaldokument Daten zu natürlichen oder juristischen Personen enthalten sein, welche noch nicht in IASA-GEX NDB durch Objekte abgebildet wurden, dürfen diese erst verwendet oder weitergegeben werden, wenn entsprechende Objekte im System erfasst und diese erfassungskontrolliert wurden (vgl. Abs. 6). Diese Regelung findet sich heute in Artikel 23 Absatz 5 ISV-NDB für ISIS.

Art. 25 Erfassungskontrolle

Diese Bestimmung wurde praktisch unverändert von Artikel 24 ISV-NDB übernommen. Die Erfassungskontrolle wird somit gleich weitergeführt, wie heute in ISIS. Daten, welche von der Qualitätssicherungsstelle NDB nicht bestätigt werden können, sind zu löschen und die erfassende Stelle zu orientieren, damit die Qualität der Datenerfassung stetig verbessert werden kann (vgl. Abs. 3).

Art. 26 Zugriffsrechte

Die Zugriffsrechte für IASA-GEX NDB sind in Artikel 50 Absatz 3 NDG geregelt, weshalb in Absatz 1 lediglich auf diese Bestimmung verwiesen wird. Die vorgesehenen Zugriffsrechte stimmen mit den heutigen Zugriffen auf ISIS überein. Die Zugriffsberechtigungen für den INDEX NDB werden neu separat im 6. Abschnitt der besonderen Bestimmungen zum INDEX NDB geregelt.

Wie heute verweist Absatz 2 für eine Übersicht über die individuellen Zugriffsrechte auf den Anhang 2.

Art. 27 Periodische Überprüfung der Personendatensätze

Das Instrument der periodischen Überprüfung wird unverändert von ISIS übernommen (vgl. Art. 25 ISV-NDB). Die Qualitätssicherungsstelle des NDB überprüft die Personendatensätze spätestens fünf Jahre nach deren ursprünglichen Erfassung in einem Informationssystem des NDB. Anschliessend führt sie mindestens alle drei Jahre eine periodische Überprüfung der Datensätze durch.

Aus Transparenzgründen wird in Absatz 2 neu detailliert aufgelistet, was die Qualitätssicherungsstelle des NDB zu überprüfen hat und, dass sie das Ergebnis der Überprüfung festhalten muss. Die Prüfung entspricht vom Inhalt und Umfang her derjenigen der Gesamtbeurteilung im heutigen ISIS.

Wie heute im ISIS (vgl. Art. 25 Abs. 3 ISV-NDB), dürfen Daten, die als ungesichert gekennzeichnet sind, nur unter abschliessend aufgezählten Voraussetzungen bis zur nächsten periodischen Überprüfung weiterverwendet werden (vgl. Abs. 3). Auf Wunsch der nachrichtendienstlichen Aufsicht wurde die Aufbewahrungsfrist der ungesicherten Daten mit dem Rhythmus der periodischen Prüfung abgestimmt und beträgt neu fünf Jahre.

Objekte, die als Drittpersonen gekennzeichnet sind, sind ebenfalls bei der ersten periodischen Prüfung zu löschen (vgl. Abs. 4). Ihre maximale Aufbewahrungsfrist beträgt somit fünf Jahre. Auch diese Angleichung an den Rhythmus der periodischen Prüfung entspricht einer Anregung der nachrichtendienstlichen Aufsichtsstelle.

Art. 28 Aufbewahrungsdauer

Die Aufbewahrungsfristen für Daten in IASA-GEX NDB entsprechen grundsätzlich denjenigen des heutigen ISIS (vgl. Art. 26 ISV-NDB).

6. Abschnitt: Besondere Bestimmungen über den INDEX NDB

Art. 29 Struktur

Der INDEX NDB wird neu als eigenes Informationssystem geregelt, das seine formell gesetzliche Grundlage in Artikel 51 NDG findet und aus den folgenden drei Teilen besteht:

Er enthält ein Verzeichnis zur Feststellung, ob der NDB in IASA NDB oder IASA-GEX NDB Daten über eine natürliche oder juristische Person, einen Gegenstand oder ein Ereignis bearbeitet (IASA INDEX; vgl. Bst. a). Darin sind die gleichen Objekte zu natürlichen oder juristischen Personen, Gegenstände und Ereignisse abgebildet, wie heute im ISIS- und ISAS-Index.

Dazu kommt neu ein Bereich zur Ablage, Erfassung, Bearbeitung, Abfrage und Auswertung von Daten aus Vorabklärungen der kantonalen Vollzugsbehörden (KND INDEX; vgl. Bst. b). Hier können die kantonalen Vollzugsbehörden Daten bearbeiten, bevor sie diese soweit verdichtet haben, dass sie dem NDB Bericht erstatten können. Diese Daten werden heute bei den kantonalen Vollzugsbehörden geführt, unterstehen aber den Bestimmungen des BWIS und sind streng von den übrigen Daten der kantonalen Vollzugsbehörden zu trennen. Neu sollen diese Daten in einem Informationssystem des NDB geführt werden, was dazu führt, dass diese leichter von der Qualitätssicherungsstelle des NDB eingesehen und geprüft werden können. Auch die Behandlung von Auskunftsgesuchen gemäss Artikel 63 NDG wird dadurch vereinfacht. Darüber

hinaus trägt diese Lösung der Datensicherheit (bei der Übermittlung von den kantonalen Vollzugsbehörden an den NDB) Rechnung.

Dazu kommt ein Bereich zur Erstellung, Auftragsverwaltung und Ablage der Berichte der kantonalen Vollzugsbehörden sowie zur Ablage der vom NDB erhaltenen Produkte (vgl. Bst. c). Ein Bericht wird dann vom NDB abgenommen, wenn dieser entweder dem erteilten Auftrag des NDB entspricht oder wenn der Bericht aufgrund des allgemeinen Informationsauftrages selbständig erstattet wurde, der Aufgabenbezug nach Artikel 6 NDG gegeben ist und die Informationen im Bericht erheblich und richtig sind. Auch die Auftragsverwaltung wird heute bei den kantonalen Vollzugsbehörden geführt und untersteht den Bestimmungen des BWIS. Informationen, die der NDB den kantonalen Vollzugsbehörden zum Vollzug ihrer gesetzlichen Aufgaben zukommen lässt, können ebenfalls hier abgelegt werden.

Art. 30 Inhalt

Der Inhalt des Index wird in Artikel 51 Absatz 3 NDG ausführlich geregelt, weshalb im vorliegenden Entwurf auf weitergehende Ausführungen verzichtet werden kann (vgl. Abs. 1).

Wie heute (vgl. Art. 16 Abs. 5 und 22 Abs. 5 ISV-NDB) gibt es in Absatz 2 einen Vorbehalt im Sinne des Quellenschutzes von Artikel 35 NDG. Die in IASA NDB oder IASA-GEX NDB bearbeiteten Daten von natürlichen und juristische Personen werden ausnahmsweise nicht in den INDEX IASA NDB aufgenommen, wenn dies aus Gründen des Quellenschutzes als geboten erscheint. Diese Praxis hat sich in der Vergangenheit bewährt.

Gemäss Artikel 44 Absatz 1 NDG dürfen auch die kantonalen Vollzugsbehörden besonders schützenswerte Personendaten und Persönlichkeitsprofile bearbeiten. Der INDEX NDB kann demzufolge auch solche Daten enthalten (vgl. Abs. 3).

Gemäss heutiger Praxis werden Daten zu (ISIS-)Drittpersonen nicht in den Index aufgenommen. Dies soll auch in Zukunft so bleiben, da Drittpersonen nur über den Bezug zu einer anderen natürlichen oder juristischen Person eine Relevanz zu den Aufgabengebieten des NDB nach Artikel 6 NDG haben. Dies wird nun ausdrücklich in Absatz 4 geregelt ist.

Ebenfalls wie heute sieht der Absatz 5 vor, dass der Katalog der Personendaten im Anhang aufgelistet wird. Die Datenfelder und die Organisationseinheiten, die darauf Zugriff haben, werden neu nicht mehr durch das VBS geregelt, sondern gemäss Artikel 21 Absatz 2 Buchstabe e der Verordnung vom 14. Juni 1993[24] zum Bundesgesetz über den Datenschutz, im Bearbeitungsreglement.

Art. 31 Datenbearbeitung durch die kantonalen Vollzugsbehörden

Die kantonalen Vollzugsbehörden haben sich sowohl bei der Bearbeitung von konkreten Aufträgen des NDB als auch bei der selbstständigen Berichterstattung an die Schranken des NDG zu halten. Das heisst, ein Bezug zum Aufgabengebiet des NDB nach Artikel 6 NDG muss immer (auch bei der Erfassung von Personendatensätze in den Vorabklärungen gemäss Art. 29 Bst. b des Verordnungsentwurfs) gegeben sein und die Datenbearbeitungsschranke von Artikel 5 Absatz 5 NDG muss eingehalten werden.

Art. 32 Zugriffsrechte

Die Zugriffsrechte auf die Daten im INDEX NDB richten sich nach Artikel 51 Absatz 4 NDG und entsprechen dem heutigen Umfang.

Wie bereits erwähnt, ist in Artikel 31 des vorliegenden Verordnungsentwurf vorgesehen, dass die kantonalen Vollzugsbehörden gegenseitig Zugriff auf ihre Vorabklärungen gemäss Artikel 29 Buchstabe b des Entwurfs haben können. Dies um Doppelspurigkeiten und Informationspannen zu verhindern. Die Mitarbeitenden des NDB erhalten lediglich ein Leserecht in der Auftragsverwaltung des Index KND, auf die Vorabklärungen sind sie nicht zugriffsberechtigt. Lediglich die Qualitätssicherungsstelle des NDB kann für die periodische Überprüfung der Personendaten im Index KND nach Artikel 33 Buchstabe b auch auf die Daten der Vorabklärungen zugreifen. Wie heute verweist Absatz 2 für die Übersicht über die individuellen Zugriffsrechte auf den Anhang 3.

Art. 33 Periodische Überprüfung der Berichte der kantonalen Vollzugsbehörden

Artikel 45 Absatz 5 Buchstabe b NDG schreibt vor, dass die Qualitätssicherungsstelle des NDB die im INDEX NDB im Verzeichnis nach Art. 29 Bst. a des Verordnungsentwurfs erfassten Berichte der kantonalen Vollzugsbehörden periodisch auf ihre Erheblichkeit und Richtigkeit überprüft. In den IASA INDEX werden nur diejenigen Berichte repliziert, die in den Informationssystemen IASA NDB und IASA-GEX NDB erfasst werden. Deshalb ist in Absatz 1 vorgesehen, dass die periodische Überprüfung der Berichte in diesen beiden Informationssystemen durchgeführt wird. Das Ergebnis und insbesondere allfällige Löschungen übertragen sich automatisch in den INDEX NDB. Die Qualitätssicherungsstelle des NDB hat daneben in den Bereichen gemäss Artikel 29 Buchstabe b und c Stichproben nach Artikel 11 Absatz 2 NDG durchzuführen (vgl. Abs. 2). Sie konzentriert sich dabei je nach Kontrollplan auf die Datenbearbeitung einer oder mehrerer kantonalen Vollzugsbehörden.

Art. 34 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer von Daten des INDEX NDB gemäss Artikel 29 Buchstabe a des Verordnungsentwurfs richtet sich nach den Bestimmungen, welche für die Informationssysteme gelten, aus denen die Daten stammen (für Daten aus IASA NDB nach Art. 21 und für Daten aus IASA-GEX NDB nach Art. 28 des vorliegenden Entwurfs). Die Löschung von Daten in diesen Informationssystemen führt automatisch zur Löschung der Daten im INDEX NDB, da es sich lediglich um Spiegelbilder handelt (vgl. Abs. 1).

Die Daten der kantonalen Vollzugsbehörden gemäss Artikel 29 Buchstabe b und c des Verordnungsentwurfs sollen wie heute fünf Jahre aufbewahrt werden können (vgl. Abs. 2).

---

[24] SR **235.11**

Gemäss Absatz 3 i.V.m. Artikel 45 Absatz 5 Buchstabe d NDG vernichtet die Qualitätssicherungsstelle NDB auf Antrag der kantonalen Vollzugsbehörden oder nach Ablauf der in Absatz 2 genannten Dauer die Daten gemäss Artikel 29 Buchstabe b und c des Verordnungsentwurfs. Fehlerfassungen können von den kantonalen Vollzugsbehörden innert 10 Tagen selbst vernichtet werden.

7. Abschnitt: Besondere Bestimmungen über GEVER NDB

Art. 35 Struktur

Die Struktur von GEVER, wie sie heute besteht, wird unverändert beibehalten. Sie besteht aus einem Bereich zur Ablage und Bearbeitung von Daten, die der Geschäftsbearbeitung und –kontrolle sowie zur Sicherung effizienter Arbeitsabläufe des NDB dient (vgl. Bst. a), einem Bereich, in dem die hängigen und erledigten Aufträge der Mitarbeiterinnen und Mitarbeitern des NDB eingesehen und bearbeitet werden können (vgl. Bst. b) und einer Suchmaschine, mit der innerhalb von GEVER mittels Volltextsuche gesucht werden kann (vgl. Bst. c).

Art. 36 Inhalt

Der Inhalt von GEVER NDB richtet sich nach Artikel 52 Absatz 2 NDG und bleibt im Vergleich zu heute unverändert, auch wenn bspw. die Geschäftskontrolle der Dokumentationsstelle Rassismus nicht mehr ausdrücklich genannt wird (vgl. Abs. 1 und Art. 38 Abs. 1 ISV-NDB). Die Geschäftskontrolldaten zur Funkaufklärung werden im vorliegenden Verordnungsentwurf im 11. Abschnitt bei den besonderen Bestimmungen zum Informationssystem ISCO geregelt.

Da die heutige Regelung von Artikel 38 Absatz 2 ISV-NDB sich als praktisch nicht umsetzbar erwiesen hat (Daten, die zur Erstellung der Inhalte nach Art. 38 Abs. 1 Bst. a-c ISV-NDB verwendet wurden, können in GEVER mangels Kennzeichnung nicht mit vernünftigem Aufwand aussortiert werden), wurde sie im vorliegenden Verordnungs-Entwurf weggelassen. Stattdessen sollen diese Daten im Rahmen einer konsequenten periodischen Überprüfung gepflegt werden (vgl. Art. 38 des Entwurfs).

Absatz 2 sieht vor, dass wie heute in Abweichung von Artikel 12 Absätze 2 und 3 der GEVER-Verordnung vom 30. November 2012[25] in GEVER NDB Daten der Klassifizierungsstufen VERTRAULICH und GEHEIM unverschlüsselt abgelegt werden (vgl. Art. 37 Abs. 2 ISV-NDB und die besonderen Sicherheitsmassnahmen von GEVER).

Der Katalog der Personendaten wird weiterhin in einem Anhang des vorliegenden Verordnungsentwurfs aufgelistet.

Art. 37 Zugriffsrechte

Die Zugriffsrechte werden in Artikel 52 Absatz 3 NDG geregelt und ändern sich im Vergleich zu heute nicht (vgl. Abs. 1). Wie heute verweist Absatz 2 für eine Übersicht über die individuellen Zugriffsrechte auf den entsprechenden Anhang.

Art. 38 Qualitätssicherung

Wie bereits erwähnt, sind im GEVER primär diejenigen Mitarbeiterinnen und Mitarbeiter für die Qualitätssicherung zuständig, welche Daten ablegen, da im GEVER keine Personendatensätze erfasst werden. Im Bearbeitungsreglement wird zu diesem Zweck für jedes GEVER-Dossier eine verantwortliche Person festgelegt. Diese haben gemäss Absatz 1 den Auftrag, das entsprechende Dossier jährlich unter Berücksichtigung der aktuellen Lage, ob die Datenbestände des Dossiers für die Geschäftsbearbeitung und –kontrolle sowie zur Sicherung effizienter Arbeitsabläufe des NDB noch notwendig sind, zu prüfen.

Ist dies nicht der Fall, werden die Daten gelöscht und dem Schweizerischen Bundesarchiv abgeliefert oder berichtigt (vgl. Abs. 2 und 3). Die Qualitätssicherungsstelle des NDB prüft im Rahmen der jährliche Stichprobenkontrolle, ob diese Qualitätssicherung vorschriftsgemäss durchgeführt wurde (vgl. Abs. 4).

Art. 39 Verwendungssperre

In der Weisung des Direktors NDB vom 9. September 2013 betreffend die Bearbeitung von Daten in der elektronischen Auftrags- und Geschäftsverwaltung (GEVER NDB) ist in Ziffer 3 vorgesehen, dass Amts- und Lageberichte oder Meldungsausgänge nicht allein gestützt auf Daten des GEVER erstellt werden dürfen. Das heisst, dass keine in GEVER einem Auftrag angehängte Daten aus IASA NDB oder IASA-GEX NDB verwendet werden dürfen, ohne dass im betreffenden Informationssystem überprüft wird, ob diese Daten dort noch geführt werden. Der Grund für diese Regelung ist der, dass die Daten in der Zwischenzeit von der Qualitätssicherung aus IASA NDB oder IASA-GEX NDB gelöscht worden sein könnten. Diese Verwendungssperre wird neu in Absatz 1 aufgenommen. Mit dem Begriff Verwenden ist somit die Aufnahme der Information in ein Produkt gemeint.

Gemäss Absatz 2 prüft die Qualitätssicherungsstelle des NDB stichprobenweise einmal im Jahr, ob diese Verwendungssperre eingehalten wird

Art. 40 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer für Daten im GEVER wird von heute 45 Jahren auf 20 Jahre reduziert.

8. Abschnitt: Besondere Bestimmungen über ELD

Art. 41 Struktur

Die Struktur von ELD bleibt trotz überarbeiteter Formulierung der Bestimmung im Vergleich zu heute unverändert (vgl. Art. 29 Abs. 2 ISV).

---

25 SR **172.010.441**

Art. 42 Inhalt

Der Inhalt von ELD richtet sich nach Artikel 53 Absatz 2 NDG. Personendaten werden in ELD nur insofern erfasst, als dies zur Lagedarstellung und -beurteilung oder zur polizeilichen Gefahrenabwehr unbedingt notwendig ist. Unter die polizeiliche Gefahrenabwehr fallen alle Handlungen der Sicherheitsbehörden, die für die öffentliche Sicherheit und Ordnung sowie innere und äussere Sicherheit dienlich sind. Die polizeiliche Gefahrenabwehr kann kriminalpolizeiliche, sicherheitspolizeiliche sowie verwaltungspolizeiliche Informationen enthalten. Im Rahmen der polizeilichen Gefahrenabwehr können dies zum Beispiel Personendaten von im Zusammenhang mit Ermittlungen oder Fahndungen stehenden Personen sein.

Art. 43 Zugriffsrechte

Die Zugriffsrechte auf von ELD richten sich nach Artikel 53 Absätze 3 und 4 NDG und bleiben im Vergleich zu heute unverändert (vgl. Abs. 1 und Art. 32 ISV-NDB).

Wie bis anhin hat der NDB unter bestimmten Voraussetzungen die Möglichkeit, privaten Stellen sowie ausländischen Sicherheits- und Polizeibehörden bei Ereignissen, die zu einer erhöhten Gefährdung der Sicherheit führen, zeitlich und inhaltlich begrenzt Zugriff auf ELD zu gewähren (vgl. Abs. 3). Die Verwendung der Daten durch diese Stellen und Behörden kann gemäss Absatz 4 überprüft werden. Eine Übersicht über die individuellen Zugriffsrechte findet sich im Anhang 8 (vgl. Abs. 5). Die Absätze 2-5 des Entwurfs wurden unverändert von Artikel 32 Absätze 2-4 ISV-NDB übernommen.

Art. 44 Qualitätssicherung

Neu wird in ELD unterschieden zwischen Daten, welche der NDB eingibt und denjenigen, welche vom Bundesamt für Polizei eingegeben werden. Da in ELD jedoch keine Personendatensätze erfasst werden, ist die jährliche Qualitätssicherung die Aufgabe der für die Datenablage zuständigen Mitarbeiterinnen und Mitarbeiter des NDB und des Bundesamtes für Polizei (vgl. Abs. 1). Dementsprechend sind die Kriterien für die Qualitätssicherung unterschiedlich (vgl. Abs. 2-4).

Die Qualitätssicherungsstelle des NDB prüft im Rahmen der jährlich Stichprobenkontrolle, ob die Qualitätssicherung von beiden Stellen vorschriftsgemäss durchgeführt wurde (vgl. Abs. 5).

Art. 45 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer wurde unverändert von Artikel 31 ISV-NDB übernommen und beträgt drei Jahre. Daten die vom Bundesamt für Polizei erfasst wurden, dürfen höchstens zwei Jahre aufbewahrt werden.

9. Abschnitt: Besondere Bestimmungen über das OSINT-Portal

Art. 46 Struktur

In der heutigen ISV-NDB wird die Struktur des OSINT-Portals nicht ausgewiesen. Aus Gründen der Transparenz wird dies im vorliegenden Entwurf getan. Das OSINT-Portal besteht insbesondere aus einer nach Quellen geordneten Aktenablage zur Erfassung und Auswertung von Daten aus öffentlich zugänglichen Quellen.

Art. 47 Inhalt

Wie beim bisherigen Zwischenspeicher OSINT (vgl. Art. 42 Abs. 1 ISV-NDB) werden im OSINT-Portal öffentlich zugänglichen Daten abgelegt. Bei den Daten im OSINT-Portal handelt es sich jedoch nicht einfach um Kopien von Internetdaten. Es werden hier qualitativ möglichst hochwertige Informationen, die immer einen Bezug zu einem Aufgabengebiet des NDB haben müssen, gesammelt. Die Daten stammen teilweise aus kostenpflichtigen Quellen (versch. Abonnemente von Online Medien) oder können das Ergebnis gezielter Recherchen sein (Dschihadismus-Monitoring). Alle im OSINT-Portal vorhandenen Daten werden nach Quelle und Thematik strukturiert erfasst und können mittels Analysetools ausgewertet und genutzt werden. (vgl. Abs. 1).

Sollen Daten aus dem OSINT-Portal verwendet oder weitergegeben werden, sind in IASA NDB, IASA-GEX NDB oder GEVER zu erfassen resp. abzulegen (vgl. Abs. 2).

Werden Daten automatisiert abgelegt und nicht manuell triagiert, muss vorgängig die Qualität der Quelle geprüft werden (vgl. Abs. 3). Dies geschieht durch festgelegte Prozesse und Vorgaben. So werden im OSINT-Portal lediglich Daten aus öffentlichen Quellen abgelegt, die automatisierte Erfassung betrifft insbesondere Agenturmeldungen und ähnliches.

Eine Übersicht über die Personendaten findet sich im Anhang 1 (vgl. Abs. 4).

Art. 48 Zugriffsrechte

Auf die Daten des OSINT-Portals haben wie heute sämtliche Mitarbeiterinnen und Mitarbeiter des NDB Zugriff. Neu kann auch den Mitarbeiterinnen und Mitarbeitern der kantonalen Vollzugsbehörden Zugriff gewährt werden (vgl. Abs. 1 i.V.m. Art. 54 Abs. 3 und 4 NDG). Eine Übersicht über die individuellen Zugriffsrechte findet sich im Anhang 7 (vgl. Abs. 2).

Art. 49 Stichprobenkontrolle

Im OSINT-Portal gibt es keine Personendatensätze. Im Hinblick auf den klaren Wortlaut von Art. 45 Abs. 4 NDG wurde deshalb auf eine periodische Überprüfung verzichtet. Da eine jährliche Überprüfung von OSINT-Daten wenig sinnvoll ist, wurde auf dieses Instrument ebenfalls verzichtet und stattdessen die Aufbewahrungsfrist drastisch eingeschränkt (vgl. Art. 50). Die Qualitätssicherungsstelle des NDB führt aber auch in diesem Informationssystem jährlich eine Stichprobe gemäss Artikel 11 Absatz 2 durch.

Art. 50 Aufbewahrungsdauer

Die Aufbewahrungsfrist von heute 20 (Inland) bzw. 45 Jahren (Ausland) wird auf 2 Jahre verkürzt. Ausgenommen davon sind die Daten, welche im Rahmen des Monitoring Dschimon erhoben werden. Diese müssen länger aufbewahrt werden können, da einerseits ein Monitoring über mehrere Jahre hinweg durchgeführt werden kann und andererseits daraus nur die wichtigsten Daten in IASA NDB ausgewertet werden. Es muss die Möglichkeit bestehen, auf die noch nicht ausgewerteten Daten während einer gewissen Zeit zurückgreifen zu können.

10. Abschnitt: Besondere Bestimmungen über Quattro P

Art. 51 Struktur

Diese Bestimmung wurde praktisch unverändert vom heutigen Artikel 33 Absatz 2 ISV-NDB übernommen.

Art. 52 Inhalt

Der Inhalt von Quattro P ist unverändert geblieben und entspricht dem heutigen Artikel 34 Absatz 1 ISV-NDB (vgl. Abs. 1).

Es sei an dieser Stelle darauf hingewiesen, dass die sog. API-Daten (Advance Passenger Informations) nicht in Quattro P bearbeitet werden. Diese Daten werden dem NDB vom SEM übermittelt, mit den Informationssystemen IASA-GEX und IASA NDB abgeglichen und unverzüglich nach dem Abgleich vernichtet. Nur die sich dabei ergebenden Treffer werden in den vorgenannten Systemen erfasst.

Sollen Daten aus Quattro P verwendet oder weitergegeben werden, sind diese zunächst nach den Regeln, welche für die. Ablage bzw Erfassung von Informationen gelten, in IASA NDB, IASA-GEX NDB oder GEVER zu überführen (vgl. Abs. 2).

Werden Daten automatisiert abgelegt und nicht manuell triagiert, muss vorgängig die Qualität der Quelle geprüft werden (vgl. Abs. 3). Dies geschieht durch festgelegte Prozesse und Vorgaben. So beruht beispielsweise die automatisierte Ablage der Daten in Quattro P auf einer vom Bundesrat genehmigten vertraulichen Länderliste. Bei Treffern findet eine manuelle Prüfung statt und die Qualitätssicherungsstelle des NDB prüft im Rahmen von Stichproben, ob Daten zu Ländern erfasst wurden, welche nicht auf der Länderliste figurieren.

Eine Übersicht über die Personendaten und die individuellen Zugriffsrechte finden sich im Anhang 8 (vgl. Abs. 4).

Art. 53 Zugriffsrechte

Die Zugriffsberechtigungen sind unverändert geblieben und entsprechen dem heutigen Artikel 35 ISV-NDB.

Art. 54 Periodische Überprüfung der Personendatensätze

Absatz 1 schreibt vor, dass die für die Datenerfassung in Quattro P zuständigen Mitarbeiterinnen und Mitarbeiter des NDB neu eine periodische Prüfung durchführen müssen. In diesem Sinne beurteilen sie jährlich, ob die Personendatensätze, welche die Grenzkontrollorgane dem NDB übermittelt haben und die in Quattro P abgelegt wurden, mit der vom Bundesrat festgelegten Liste nach Artikel 55 Absatz 4 NDG übereinstimmen. Ändert die Bundesratsliste, ist der Datenbestand entsprechend anzupassen. Die Qualitätssicherungsstelle des NDB führt zusätzlich Stichproben gemäss Artikel 11 Absatz 2 durch (vgl. Abs. 3).

Nicht mehr benötigte Daten sind zu löschen und dem Schweizerischen Bundesarchiv abzuliefern (vgl. Abs. 2).

Art. 55 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer für die Daten in Quattro P beträgt fünf Jahre (vgl. Art. 36 ISV-NDB) verlängert.

11. Abschnitt: Besondere Bestimmungen über ISCO

Art. 56 Struktur

Neu wird ISCO aus Gründen der Transparenz als eigenes Informationssystem ausgewiesen, das aus einer Aktenablage zur Verwaltung und Steuerung der Aufklärungsmittel sowie zum Controlling und Reporting besteht. Die Ablage der diesbezüglichen Daten wird heute in den Bestimmungen zu GEVER geregelt (vgl. insb. Art. 38 Abs. 1 Bst. e ISV-NDB).

Art. 57 Inhalt

Der Inhalt von ISCO richtet sich nach Artikel 56 Absatz 2 NDG (vgl. Abs. 1) und besteht insbesondere aus Aufklärungsaufträgen mit dem Zentrum für elektronische Operationen der Führungsunterstützungsbasis der Schweizer Armee (FUB ZEO). Die Resultate der Funk- und Kabelaufklärung werden aber nicht in ISCO abgelegt, sondern in IASA NDB oder dem Restdatenspeicher und können in ISCO referenziert werden (Beispiel für den Ablauf: Ein in IASA NDB erfasstes Objekt (Tf-Nummer) soll durch die FUB ZEO aufgeklärt werden. Die Tf-Nummer sowie der Auftrag an die FUB ZEO werden in ISCO erfasst, damit die Steuerung und Compliance lückenlos sichergestellt werden kann. Anschliessend wird die TF-Nummer als Target an die FUB ZEO übermittelt. Das Resultat der Aufklärung wird in Form eines COMINT-Reports an den NDB übermittelt und fliesst als Originaldokument in IASA NDB mit Referenzierung zum ISCO.)

Werden Daten automatisiert abgelegt und nicht manuell triagiert, muss vorgängig die Qualität der Quelle geprüft werden (vgl. Abs. 3). Dies geschieht durch festgelegte Prozesse und Vorgaben. So wird der Leistungsauftrag (z.B. Telefonnummer) von den Mitarbeitenden des NDB überprüft und manuell geladen. Die Resultate (z.B. Verbindungsdaten) werden vom Sensor (z.B. Mitarbeiter des FUB ZEO) auf den Aufgabenbezug nach Artikel 6 NDG hin geprüft an den NDB übermittelt und automatisch in ISCO abgelegt.

Art. 58 Zugriffsrechte

Zugriff auf ISCO haben nur diejenigen Mitarbeiterinnen und Mitarbeiter des NDB, die mit der unmittelbaren Steuerung der Funk- und Kabelaufklärung befasst sind (heute weniger als zehn Personen).

Art. 59 Qualitätssicherung

Bereits heute werden die Aufklärungsaufträge und Datenbestände jährlich unter Berücksichtigung der aktuellen Lage auf ihre Zweckmässigkeit und Verhältnismässigkeit hin überprüft (vgl. Abs. 1).). Dies wird nun explizit so in Absatz 1 geregelt. Zuständig sind die für die Datenablage in ISCO zuständigen Mitarbeiterinnen und Mitarbeiter des NDB.

Die Qualitätssicherungsstelle des NDB führt zusätzlich Stichproben gemäss Artikel 11 Absatz 2 durch und stellt sicher, dass die Qualitätssicherung der für die Datenablage in ISCO zuständigen Mitarbeiterinnen und Mitarbeiter gemäss diesen Vorgaben durchgeführt wird (vgl. Abs. 4).

Art. 60 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer für die Daten in ISCO beträgt höchstens fünf Jahre nach Abschluss des entsprechenden Aufklärungsauftrags.

12. Abschnitt: Besondere Bestimmungen über den Restdatenspeicher

Art. 61 Zweck

Im Restdatenspeicher werden alle Informationen abgespeichert, die bei der Triage nach der Eingangsprüfung nicht einem anderen System zugewiesen werden konnten (vgl. Abs. 1 i.V.m. Art. 57 NDG). Die Ablageprüfung richtet sich nach Artikel 3 Absatz 1

Daten, welche für die Aufgabenerfüllung des NDB benötigt werden, sind in IASA NDB, IASA-GEX NDB oder GEVER zu überführen und können im Restdatenspeicher vernichtet werden, da diese über die vorgenannten Informationssysteme an das Schweizerische Bundesarchiv abgeliefert werden (vgl. Abs. 2). Dabei gelten für die Ablage von Daten die Bestimmungen von Art. 3 Abs. 1. Sollen Personendaten verwendet oder weitergegeben werden, dann gelten für die Überführung die Bestimmungen von Art. 4 Abs. 1. Das heisst, die Personendaten müssen vorher einzeln im Hinblick auf den Aufgabenbezug, die Erheblichkeit, Richtigkeit und die Datenbearbeitungsschranke von Art. 5 Abs. 5 NDG geprüft und in IASA NDB strukturiert erfasst werden (für IASA GEX NDB gilt bereits eine generelle Pflicht zur strukturierten Erfassung).

Art. 62 Inhalt

Der Inhalt des Restdatenspeichers richtet sich nach Artikel 57 Absatz 2 NDG. Es handelt sich dabei vor allem um die Meldungen von ausländischen Sicherheitsbehörden, Daten aus der Funk- und Kabelaufklärung, Informationen von menschlichen Quellen und nicht aktiv vom NDB beschaffte Informationen.

Art. 63 Zugriffsrechte

Die Mitarbeiterinnen und Mitarbeiter des NDB, die mit der Erfassung, Recherche, Auswertung und Qualitätssicherung von Daten beauftragt sind, haben Zugriff auf die Daten des Restdatenspeichers (vgl. Art. 57 Abs. 3 NDG).

Art. 64 Stichprobenkontrolle

Da eine periodische Überprüfung von Daten des Restdatenspeichers wenig sinnvoll ist (die Daten werden hier nur abgelegt, noch nicht einem Bereich zugeordnet und nicht personenbezogen erfasst), wurde auf dieses Instrument verzichtet und stattdessen die Aufbewahrungsfrist drastisch eingeschränkt (von 10 Jahren auf fünf Jahre). Die Qualitätssicherungsstelle des NDB führt aber auch in diesem Informationssystem jährlich eine Stichprobe gemäss Artikel 11 Absatz 2 durch.

Art. 65 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer für die Daten im Restdatenspeicher beträgt höchstens fünf Jahre.

13. Abschnitt: Daten aus genehmigungspflichtigen Beschaffungsmassnahmen und aus Beschaffungen im Ausland

Art. 66 Zweck

Die Speichersysteme dienen der Aktenablagen zur fallbezogenen Erfassung, Bearbeitung und Abfrage von Daten aus genehmigungspflichtigen Beschaffungsmassnahmen und aus Beschaffungen im Ausland (vgl. Abs. 1).

Artikel 58 Absatz 1 NDG sieht vor, dass Daten aus solchen Beschaffungsmassnahmen in vom Verbund von Informationssystemen getrennten Systemen gespeichert und dort gesichtet werden (vgl. Abs. 2).

Art. 67 Inhalt

Wie in IASA NDB und IASA-GEX NDB können in den Speichersystemen Daten über natürliche und juristische Personen, Gegenstände, Ereignisse, besonders schützenswerte Personendaten und Persönlichkeitsprofile bearbeitet werden.

Art. 68 Zugriffsrechte

Die Zugriffsrechte sind in Artikel 58 Absatz 5 NDG umschrieben (vgl. Abs. 1).

Für jede einzelne Operation sind gesonderte Zugriffsrechte einzurichten (vgl. Abs. 2). Dabei ist sicherzustellen, dass nur diejenigen Personen Zugriff haben, welche die Operation führen bzw. mit der Durchführung der Beschaffungsmassnahmen und der Auswertung der Ergebnisse beauftragt sind (vgl. Art. 58 Abs. 5 NDG).

Die individuellen Zugriffsrechte werden für jede Beschaffungsmassnahme durch den NDB bewilligt (vgl. Abs. 3).

Art. 69 Einschränkung der Verwendung und Vernichtungspflicht

Sollen Daten verwendet oder weitergegeben werden, sind diese vorher unter den entsprechenden Auflagen in IASA NDB zu überführen (vgl. Abs. 1). Diese müssen im Gegensatz zum Restdatenspeicher angesichts der kurzen Aufbewahrungsdauer in den Speichersystemen nicht vernichtet werden.

Die Qualitätssicherungsstelle des NDB prüft stichprobenweise, ob diese Einschränkung der Verwendung und die Vernichtungspflicht eingehalten werden (vgl. Abs. 2).

Art. 70 Aufbewahrungsdauer

Die Daten in den Speichersystemen 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. Daten, welche nicht für ein laufendes rechtliches Verfahren benötigt werden, werden deshalb rasch wieder gelöscht (vgl. Abs. 1).

Wird eine Mitteilung aufgeschoben, so muss die Löschung spätestens sechs Monate nach der erfolgten Mitteilung erfolgen (vgl. Abs. 2).

Die Aufbewahrungsdauer für Daten, welche gestützt auf Artikel 36 Absatz 5 NDG beschafft werden, beträgt drei Jahre (vgl. Abs. 3).

Anhänge 1,5, 8 und 10: Kataloge der Personendaten

In den oben genannten Anhängen werden gestützt auf Artikel 47 Absatz 2 Buchstabe a NDG diejenigen Daten ausgewiesen, welche entweder eine Person oder Organisation betreffen oder im Zusammenhang mit einer solchen erfasst werden können.

Sobald die entsprechende formell-gesetzliche Grundlage vorliegt, werden die Kataloge der Personendaten bei der nächsten Revision mit der AHVN13 ergänzt

Anhänge 2, 3, 4, 6, 7, 9, 11, 12 und 13: Zugriffsrechte

In den oben genannten Anhängen werden gestützt auf Artikel 47 Absatz 2 Buchstabe c NDG die Zugriffsrechte auf die Informationssysteme des NDB ausgewiesen.