Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Nachrichtendienst des Bundes NDB

Erläuternder Bericht

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 zwei Verordnungen vorgesehen: Einerseits die „allgemeine“ Verordnung über den Nachrichtendienst (NDV), andererseits die „technische“ Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB). 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.

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 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. 5 Zusammenarbeit des NDB mit 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 bisherige Praxis, die bis anhin auf Basis von Vereinbarungen zwischen dem NDB und fedpol geregelt wurde, wird somit weitergeführt.

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. Eine summarische Beurteilung der Relevanz dieser Kontakte auf Stufe Bundesrat scheint stufengerecht und rechtfertigt sich auch unter dem Aspekt, dass der dem Bundesrat vorgeschaltete Sicherheitsausschuss (SiA) das Geschäft vorgängig berät und hier auch vertiefte Abklärungen vorgenommen werden können.

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. Auch vertritt der NDB die Schweiz in internationalen nachrichtendienstlichen Gremien. In beiden Fällen sind Ausnahmen mit Bewilligung des NDB möglich. Im militärischen Bereich ist bei der Festlegung einer gemeinsamen Partnerdienstpolitik und Erstellung einer Kontaktplanung Ansprechpartner des NDB der Militärische Nachrichtendienst (MND), der sich seinerseits insbesondere mit dem Kommando Spezialkräfte (KSK) und den Swiss Armed Forces International Command (SWISSINT) austauscht.

Art. 9 Arten der Zusammenarbeit

Der Artikel konkretisiert Artikel 12 Absatz 1 Buchstabe c NDG, laut dem der NDB gemeinsame Tätigkeiten mit ausländischen Nachrichtendiensten und Sicherheitsbehörden zur Beschaffung und Auswertung von Informationen sowie zur Beurteilung der Bedrohungslage durchführen kann. Dabei kann der NDB wie schon heute auf verschiedene Arten mit ausländischen Dienststellen zusammenarbeiten. Neben der Informationsbeschaffung und gemeinsamen Operationsführung ist die gemeinsame Herstellung von Produkten (Produkte nach Artikel 9 Absatz 2 Buchstabe c der Verordnung sind beispielsweise Analysen, Lagebeurteilungen und Auswertungen), die Zusammenarbeit bei der Ausbildung (z.B. im Bereich der Analysetätigkeit oder der Sicherheit) und die Realisierung gemeinsamer Projekte (z.B. der Entwicklung von geschützten Kommunikationsmitteln zwischen den Diensten oder der arbeitsteiligen Auswertung von OSINT-Quellen) vorgesehen.

[1] SR …; BBl **2015** 7211

Art. 10 Internationale Vereinbarungen von beschränkter Tragweite

Der NDB erhält neu die Möglichkeit, selbständig internationale Vereinbarungen mit ausländischen Nachrichtendiensten oder anderen ausländischen Dienststellen, die Aufgaben im Sinne des NDG erfüllen, abzuschliessen. Nach Artikel 48a 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 Informationsaustauschsystems mit einem ausländischen Dienst. Selbstredend wären auch solche Verträge dem Bundesrat zu unterbreiten, sollten (ausnahmsweise) die Voraussetzungen nach Artikel 80 Absatz 3 NDG erfüllt sein.

2. Kapitel: Informationsbeschaffung

1. Abschnitt: Grundsätze

Art. 12 Operationen

Die Einführung 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. Im Übrigen muss der NDB Operationen formell eröffnen und abschliessen und gesondert dokumentieren. Zu betonen bleibt, dass die Aufsichtsorgane – und zwar unbesehen einer Qualifikation von zusammenhängenden Vorgängen als Operation - umfassenden Zugang zu allen sachdienlichen Informationen und Unterlagen sowie Zutritt zu allen Räumlichkeiten des NDB geniessen.

Art. 13 – 16 Zusammenarbeit und Beauftragung in der Beschaffung mit oder von inländischen Amtsstellen bzw. Zusammenarbeit und Beauftragung in der Beschaffung mit oder von ausländischen Amtsstellen bzw. Zusammenarbeit und Beauftragung in der Beschaffung mit oder von Privaten bzw. Zusammenarbeit und Beschaffung mit oder von ausländischen Amtsstellen oder von Privaten im Ausland

Nach Artikel 34 NDG kann der NDB eine Beschaffungsmassnahmen 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 vor allem für die Zusammenarbeit *im Inland mit*

- inländischen Amtsstellen,
- mit 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 wenn die inländische Amtsstelle für die Informationsbeschaffung geeignet scheint und zusätzlich über die für die Beschaffung notwendigen Fertigkeiten sowie 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 erklärt, 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.

Art. 18 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 Interessenabwägung zwischen der informationsersuchenden und der zu schützenden Quelle verankert. Dabei ist eine 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(in) usw.). Technische Quellen sind soweit zu schützen, wie eine Bekanntgabe von Angaben die Auftragserfüllung des NDB in Frage stellen könnte. Zu betonen bleibt, dass der

[2] SR **172.010**

Quellenschutz für den NDB von höchstem Interesse ist, weil wenn er ihn nicht ausreichend sicherstellen kann, er vorhersehbar und sehr schnell vom internationalen Informationsaustausch abgeschnitten würde mit entsprechenden Folgen für die Sicherheit der Schweiz. 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.

2. Abschnitt: Auskunfts- und Meldepflichten

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. 19 Abs. 2 Auskunftsplicht bei einer konkreten Bedrohung

Die Auflistung der Organisationen in Anhang 1, denen der Bund oder die Kantone die Erfüllung öffentlicher Aufgaben übertragen hat, wurde 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 der 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 20 Durchsuchen von Räumlichkeiten, Fahrzeugen oder Behältnissen

Das Durchsuchen von Räumlichkeiten, Fahrzeugen oder Behältnissen ist 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 kann auf eine ausdrückliche Dokumentierungspflicht verzichtet werden, weil gegen den NDB gerichtete Missbrauchsvorwürfe ausgeschlossen oder zumindest sehr unwahrscheinlich scheinen.

Art. 21 Genehmigungsverfahren und Freigabe

Das Genehmigungsverfahren und das Freigabeverfahren sind durch den NDB bzw. das VBS jederzeit nachvollziehbar zu dokumentieren.

Art. 22 Schutz von Berufsgeheimnissen

Der in Artikel 28 NDG verankerte Schutz von Personen, die einer der in Artikel 171 – 173 Strafprozessordnung (StPO) [4] 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, es sei denn, die konkrete Bedrohung erfolge gezielt unter dem Vorwand des Berufsgeheimnisses. Bei gegebener Sachlage hat der NDB deshalb im Genehmigungsverfahren darauf hinzuweisen und eine entsprechende Selektion zu beantragen. Die Aussonderung und Vernichtung geschützter Daten erfolgt unter Aufsicht des Bundesverwaltungsgerichts. Nicht zulässig ist die Anordnung einer genehmigungspflichtigen Beschaffungsmassnahme gegenüber einer *Drittperson*, die einer der in Artikel 171 – 173 StPO genannten Berufsgruppe angehört.

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

Art. 23

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 entscheidet die Vorsteherin oder der Vorsteher des VBS nach vorheriger Konsultation der Vorsteherin oder des Vorstehers des EDA und der Vorsteherin oder des Vorstehers des EJPD über die Durchführung einer solchen Massnahme.

---

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

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 deren 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 Erhebung von technischen Angaben oder zur Umsetzung von Kabelaufklärungsaufträgen zu ermöglichen.

Im Rahmen der Erhebung der technischen Angaben durch die Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsdienstleistungen oder durch das ZEO werden keine Kommunikationsinhalte und keine Verbindungsdaten gespeichert, sondern statistische Angaben über Datenströme auf den Kabelnetzen laufend erhoben. Damit lassen sich die Sende- und Empfangsländer sowie die verwendeten Protokolle und technischen Verfahren erkennen. Daraus lässt sich wiederum die Art und Menge der im Falle einer späteren Ausleitung von Daten notwendigen Ausrüstung bestimmen. Diese statistischen Angaben sind für einen rechtsgenügenden, möglichst fundierten Antrag an das Bundesverwaltungsgericht erforderlich und erlauben es, diesem im konkreten Anwendungsfall darzulegen, bei welchen Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsdienstleistungen potenziell relevante Daten vorliegen.

Im Übrigen können im Rahmen einer Funkaufklärung erfasste Daten auch für die Kabelaufklärungsaufträge verwendet werden.

Nachrichtendienstliche Kontakte des ZEO zu ausländischen Fachstellen erfolgen über den NDB.

Art. 29 Abs. 2 und 3 Datenbearbeitung

Der Begriff Daten ist die Gesamtheit aller Erfassungen aus der Funk- und Kabelaufklärung (Oberbegriff). Er setzt sich zusammen einerseits aus dem Begriff Kommunikation, was den eigentlichen Kommunikationsinhalt der erfassten Daten umfasst (z.B. Sprache, Text, Bilder), und anderseits aus dem Begriff Verbindungsdaten. Verbindungsdaten sind derjenige Teil der erfassten 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, der keine Teilmenge des Begriffs Daten darstellt, sondern vielmehr die aus den Daten erstellten Produkte (d.h. die auftragskonformen Informationen) umfasst, 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. Artikel 4 der zum Jahresende 2012 totalrevidierten Verordnung über die elektronische Kriegsführung 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 neuen Kabelaufklärungsauftrag oder für einen neu fokussierten 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 Vergütung 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 lediglich 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: Datenschutz und Archivierung

5 SR **780.1**

1. Abschnitt: Besondere Bestimmungen über den Datenschutz und Ausnahmen vom Öffentlichkeitsprinzip

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

Art. 32 Bekanntgabe von Personendaten durch kantonale Vollzugsbehörden

Grundlage von Artikel 32 bildet in erster Linie Artikel 46 Absatz 3 NDG, welcher die Datenbearbeitung in den Kantonen regelt.

Die Datenbekanntgabe nach Absatz 3 der Verordnung hat Ausnahmecharakter und soll einzig in notwehr- oder notstandsähnlichen Situationen schnelles behördliches Handeln ermöglichen. Die kantonalen Vollzugsbehörden entscheiden in eigener Verantwortung über das Vorliegen einer solchen Situation. Nach Absatz 4 ist der NDB gleich wie bei anderen Dringlichkeitsfällen anschliessend umgehend zu benachrichtigen.

Art. 33 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.

Art. 35 Ausnahme vom Öffentlichkeitsprinzip

Neu gegenüber heute ist, dass nach Artikel 67 NDG das Öffentlichkeitsgesetz vom 17. Dezember 2004[6] nicht (mehr) für den Zugang zu amtlichen Dokumenten betreffend die Informationsbeschaffung gilt. In der Verordnung wird präzisiert, dass jene amtlichen Dokumente unter die Ausnahmebestimmung fallen, die direkte oder indirekte Rückschlüsse über die Informationsbeschaffung zulassen, und zählt beispielshaft und nicht abschliessend drei typische Anwendungsfälle auf (z.B. Informationen über die operativen Mittel, Methoden und Kontakte des NDB). In Bezug auf die in Buchstabe a erwähnten nachrichtendienstlichen Produkte (z.B. Bericht an den Bundesrat) bleibt zu betonen, dass nur jene darunterfallen, deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen Schaden zufügen kann. Da nicht abschliessend, können auch andere amtliche Dokumente unter die Ausnahmebestimmung fallen. Denkbar sind etwa solche, die aus der Informationsbeschaffung gewonnene ermittlungstaktische Schlussfolgerungen beinhalten oder Rückschlüsse auf weitere Informationsbeschaffungsmassnahmen zulassen.

2. Abschnitt. Archivierung

Art. 36

Es wird auf die Erläuterungen zum nachfolgenden Artikel 57*a* verwiesen.

4. Kapitel: Politische Steuerung und Verbote

Art. 37 Wahrung weiterer wichtiger Landesinteressen

Der engere sicherheitspolizeiliche Bereich wird vom NDG im Zuständigkeitsbereich des VBS abgedeckt. 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 Eidg. 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 entsprechen Antrag einreichen. Im Sinne einer Ordnungsvorschrift sieht die Verordnung eine vorgängige Konsultation des NDB vor, um sicherzustellen, dass der beantragte Einsatz des NDB auch tatsächlich umsetzbar ist. Der Antrag hat sich u.a. zur 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.

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. 38 und 39 Prüfverfahren bzw. Einstellung von Prüfverfahren

Das Prüfverfahren ist im NDG nicht ausdrücklich vorgesehen. Es dient der Klärung, ob eine Person bzw. Organisation oder Gruppierung auf die Beobachtungsliste zu setzen 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

6 SR **152.3**

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

Art. 41 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 darf 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 von allem Anfang an auf aus sicherheitspolitischer Sicht unerwünschte Tätigkeiten. Andere Tätigkeiten bleiben jederzeit möglich. Hinzu kommt, dass wenn die Behörde keine sichere Kenntnis einschlägiger Aktivitäten mehr hat, daraus nicht zwingend auf die Einhaltung des Verbotes geschlossen werden kann (weil die betroffene Person beispielsweise ihr bisheriges Kommunikationsverhalten „erfolgreich“ angepasst hat bzw. vor den Behörden verheimlichen kann oder mündlich Dritte mit einschlägiger Kommunikation beauftragt usw.). Der Entscheid über die Aufrechterhaltung des Tätigkeitsverbotes muss sich deshalb vorrangig auf die Prüfung beschränken, ob und wie sich das Verbot auf die terroristische oder gewalttätig-extremistische Aktivität derjenigen Gruppierung (oder Einzelperson) auswirkt, deren Förderung mit dem Verbot unterbunden werden soll. Alles in allem scheint deshalb ein jährlicher Prüfintervall angemessen.

Im Übrigen bildet die konkrete Rechtsnatur eines Tätigkeitsverbotes zurzeit Gegenstand einer vertieften Abklärung durch das Bundesamt für Justiz.

Art. 42 Organisationsverbot

Nach Artikel 72a NDG muss sich ein Organisationsverbot auf einen entsprechenden Beschluss der Vereinten Nationen oder der Organisation für Sicherheit und Zusammenarbeit in Europa abzustützen. Diese Voraussetzung ist gemäss Verordnung dann erfüllt, wenn die zu verbietende Organisation oder Gruppierung entweder im Beschluss ausdrücklich genannt ist (Bst. a), oder in Zielsetzung und Mitteln mit einer im Beschluss ausdrücklich genannten Organisation oder Gruppierung übereinstimmt (Bst. b). Buchstabe b soll es dem Bundesrat ermöglichen, zeitnah und mit der gebotenen Flexibilität auf bisweilen rasch ändernde Umstände zu reagieren, wenn und soweit sich eine für die Sicherheit der Schweiz erkannte Gefahr lediglich formell wandelt (z.B. Gründung einer Tarn- oder Nachfolgeorganisation), in Kern und Gehalt aber fort- und weiterbesteht. Analoges gilt bei der Prüfung, ob ein Verbot nach Ablauf der Befristung zu verlängern ist: Massgebend wird sein, ob die verbotene Organisation oder Gruppierung weiterhin gelistet ist und ob weiterhin von einer konkreten Bedrohung der inneren oder äusseren Sicherheit der Schweiz ausgegangen werden muss, wenn die verbotene Organisation oder Gruppierung ihre Aktivitäten weiterhin entfalten kann bzw. könnte.

Der Einsatz von Experten im Rahmen der staatlichen Friedens-, Menschenrechts- und humanitären Politik der Schweiz (z.B. Wahlbeobachter) bezweckt keine Förderung oder Unterstützung einer verbotenen Organisation oder Gruppierung und stellt deshalb kein strafbares Verhalten dar. Für die allenfalls notwendigen Anwesenheit von an sich strafbaren Personen auf Schweizer Gebiet (z.B. für die Teilnahme an Friedensverhandlungen) ist in Zusammenarbeit mit den zuständigen Straf-, politischen und allenfalls weiteren involvierten Behörden eine den Umständen des konkreten Einzelfalls dienliche Lösung zu finden.

5. Kapitel: Dienstleistungen

Art. 44 Gebühren

Die vom NDB 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. 45 Selbstkontrolle innerhalb des NDB

Absatz 4 kommt eine Querschnittsfunktion zur VIS-NDB zu: Die Applikation SCC (Sensor Control Center), mit der das Informationssystem ISCO (vgl. Art. 55ff. VIS-NDB) betrieben wird, soll auch für die Steuerung von weiteren Sensoren verwendet werden können (IMINT, TECHINT). Die dabei anfallenden Daten gehören aber nicht zu ISCO (Funk- und Kabelaufklärung), weshalb sie nicht in den besonderen Bestimmungen zu ISCO geregelt werden können. Da sich aber auch weder der allgemeine Teil der VIS-NDB, noch GEVER für eine Regelung dieser Applikation eignet, ist sie als Pflicht zur Selbstkontrolle in Artikel 45 NDV aufzunehmen. Im Übrigen richtet sich die Bearbeitung von Personendaten, die aus dieser Informationsbeschaffung resultieren, nach den Bestimmungen der Verordnung über die Informations- und Speichersysteme des NDB (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. 47 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 einzig um den Beizug von unter der Verantwortung des NDB agierenden „Hilfskräften".

Art. 48 Taschen- und Personenkontrollen

Die im NDG als Gesetz im formellen Sinn 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 die Tatbestandsmerkmale eines Verbrechens oder Vergehens (z.B. Datendiebstahl) erfüllt sein könnten, ist der NDB gestützt auf Artikel 218 StPO (Jedermannsrecht) befugt, eine auf frischer Tat ertappte Person bis zum Eintreffen der Polizei festzuhalten (vorläufige Festnahme), wobei auch hier das Verhältnismässigkeitsprinzip beachtet werden 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 keine 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. 51 Einsatz von Bildübertragungs- und Bildaufzeichnungsgeräten sowie Mitführen von elektronischen Geräten

Die wichtigsten Ergänzungen betreffen im Übrigen 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 so schnell wie möglich, d.h. in der Regel nach 30 Tagen zu löschen sind, es sei denn, die Aufnahme werden zur Beweissicherung bei einem Missbrauchsfall benötigt.. Einzig unter dieser Voraussetzung darf die Aufnahme bis zum rechtskräftigen Abschluss des entsprechen 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 im Regelfall eine gewisse Zeit verstreicht.

8. Kapitel: Bewaffnung

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

Art. 53 Berechtigung zum Tragen einer Dienstwaffe

Gemäss Artikel 3 NDG bestimmt der Bundesrat die Kategorie von waffentragenden Mitarbeiterinnen und Mitarbeiter. Es sind dies die Mitarbeitenden des NDB, die im Rahmen ihrer dienstlichen Funktion und Aufgabe besonderen Gefährdungen ausgesetzt sind. Der Direktor NDB bestätigt durch die Erteilung der Berechtigung zum Tragen einer Dienstwaffe die Zugehörigkeit zur entsprechenden Kategorie. 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. 57a Übergangsbestimmung zur Archivierung

Für die bis zum Inkrafttreten des NDG anfallenden Akten wird eine Übergangsregelung eingeführt (Art. 57*a*). Gemäss dieser Übergangsregelung wird die Schutzfrist für alle Dossiers (d.h. nicht nur für diejenigen, die Meldungen ausländischer Sicherheitsdienste enthalten) um 30 Jahre verlängert (unter entsprechender Benachrichtigung des Bundesarchivs). Für die ab Inkrafttreten des NDG neu dem Bundesarchiv abzuliefernden Daten soll hingegen die Regelung von Artikel 68 NDG uneingeschränkt Anwendung finden.

Anhang 3: Bekanntgabe von Personendaten an inländische Behörden und Amtsstellen

Ziffer 8.3.13

fedpol erhält vom NDB auch Personendaten, welche für die Sicherheit von Passagieren schweizerischer Luftfahrzeuge relevant sind. Welche Daten fedpol zum Erstellen von Risiko- und Bedrohungsanalysen sowie von Einsatzplänen im Zusammenhang mit dem Einsatz von Sicherheitsbeauftragten im Luftverkehr bearbeiten darf, die Zugriffsrechte und die Datenbekanntgabe sollen neu im Luftfahrtgesetz vom 21. Dezember 1948[7] geregelt werden (Art. 21*b* ff. E-LFG; im Herbst 2015 in der Vernehmlassung). Die Datenbekanntgabe vom NDB an fedpol muss jedoch in der NDV geregelt werden.

Anhang 4: Aufhebung und Änderung anderer Erlasse

Aufhebung:

7 SR **748.0**

1. Verordnung vom 1. Dezember 1999[8] über die finanziellen Leistungen an die Kantone zur Wahrung der inneren Sicherheit

Mit der Schaffung des NDG fallen die meisten Regelungsinhalte der Verordnung über die finanziellen Leistungen an die Kantone zur Wahrung der inneren Sicherheit (BWIS-Abgeltungsverordnung) weg, weshalb die verbleibenden Artikel 3, 4 und 4a neu in der Verordnung über das Sicherheitswesen in Bundesverantwortung vom 27. Juni 2001[9] (VSB) respektive Artikel 5 in der Verordnung über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei vom 30. November 2001[10] geregelt werden sollen. Somit kann die BWIS-Abgeltungsverordnung aufgehoben werden.

Änderung:

2. Verordnung vom 27. Juni 2001[11] über das Sicherheitswesen in Bundesverantwortung (VSB)

Die Änderung der VSB ist durch die Änderung des Bundesgesetzes vom 21 März 1997[12] über Maßnahmen zur Wahrung der inneren Sicherheit (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 1^{bis} und 1^{ter} sowie 7 Absatz 1^{bis} werden der neuen gesetzlichen Grundlage (Art. 23 Abs. 1^{bis} BWIS) angepasst. Die völkerrechtlich geschützten Personen werden in Artikel 6 Absatz 1^{bis} Buchstabe c separat aufgeführt, da für sie andere rechtliche Grundlagen gelten, insbesondere verschiedene internationale Abkommen[13] und internationales Gewohnheitsrecht, in Verbindung mit Artikel 4 Gaststaatgesetz vom 22. Juni 2007[14] 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 3–4a 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 Datenschutzverordnung, SR 235.11 und Art. 23 Bundesinformatikverordnung, SR 172.010.58) 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[15] über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei

Wie in Ziffer 1 bereits erwähnt, wird der Artikel 5 der BWIS-Abgeltungsverordnung neu in Artikel 10a der Verordnung über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei geregelt.

7. Verordnung vom 15. Oktober 2008[16] über das automatisierte Polizeifahndungssystem

Der Nachrichtendienst des Bundes (NDB) hat zur Abwehr von Gefahren für die öffentliche Sicherheit nach Massgabe des NDG gemäss Artikel 5 Buchstabe j Verordnung vom 15. Oktober 2008[17] über das automatisierte Polizeifahndungssystem (RIPOL-Verordnung) Zugriff auf RIPOL zur Feststellung des Aufenthaltsortes von Personen und des Standortes von

8 SR **120.6**
9 SR **120.72**
10 SR **360.1**
12 SR **120**
12 SR **120**
13 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)
14 SR 192.12
15 SR **360.1**
16 **SR 361.0**
17 **SR 361.0**

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 über die polizeilichen Informationssysteme des Bundes (BPI; SR 361) zurück.

8. Verordnung vom 8. März 2013[18] über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro

Die zuständigen Einheiten des NDB haben gemäss Artikel 7 Buchstabe h Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro (S-SIS-Verordnung) 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.

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[19] 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 einerseits und solche zu Datenschutz und Datensicherheit andererseits.

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 1-18 geregelt.

1. Abschnitt: Gegenstand und Begriffe

Art. 1 Gegenstand

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

Art. 2 Begriffe

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

Die Definition von „Drittpersonen“ wurde verständlicher formuliert, blieb aber inhaltlich gleich. Die Verwendung von Drittpersonen bei der Erfassung, wie sie bisher im Informationssystem Innere Sicherheit (ISIS) erfolgte, ist künftig im Integralen Analysesystem Gewaltextremismus (IASA-GEX) vorgesehen.

SIDRED und SiLAN werden heute in Artikel 4 und 10 ISV-NDB umschrieben.

2. Abschnitt: Allgemeine Bestimmungen über die Datenbearbeitung und Archivierung

Art. 3 Ablage von Daten

In Absatz 1 ist vorgesehen, dass die Mitarbeiterinnen und Mitarbeiter der Triage bei der Zuweisung der Daten zu den Informationssystemen OSINT-Portal und Restdatenspeicher prüfen, ob genügend Anhaltspunkte bestehen, dass der Aufgabenbezug nach Artikel 6 NDG gegeben ist. Meldungen, die mehrere Personendaten umfassen, werden dabei als Ganzes beurteilt. Da die Mitarbeiterinnen und Mitarbeiter der Triage für die Eingangstriage sämtlicher, beim NDB in nicht automatisierter Weise eingehenden Daten zuständig sind, können diese nicht jede einzelne Meldung eingehend prüfen. Sie 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 zudem erleichtert. Zudem entspricht es der Systematik des vorliegenden Verordnungsentwurfs, dass lediglich abgelegte Daten nicht verwendet oder weitergegeben werden dürfen, bevor diese nicht im Integralen Analysesystem (IASA NDB) oder IASA-GEX NDB überführt, eingehend geprüft und strukturiert erfasst wurden. Sollten die Mitarbeiterinnen und Mitarbeiter der Eingangstriage Zweifel haben, sind sie gehalten, die eingehenden Meldungen inhaltlich zu prüfen. Sie können dabei auch die Mitarbeiterinnen und Mitarbeiter der Datenerfassung oder Spezialisten aus anderen Bereichen beiziehen. Wie heute sind die Daten bei negativem Befund zu vernichten oder zurückzuschicken, wenn diese von einer kantonalen Vollzugsbehörde stammen.

Die gleiche Prüfung ist bei den kantonalen Vollzugsbehörden bei der Ablage von Daten im INDEX NDB vorzunehmen (vgl. Abs. 2).

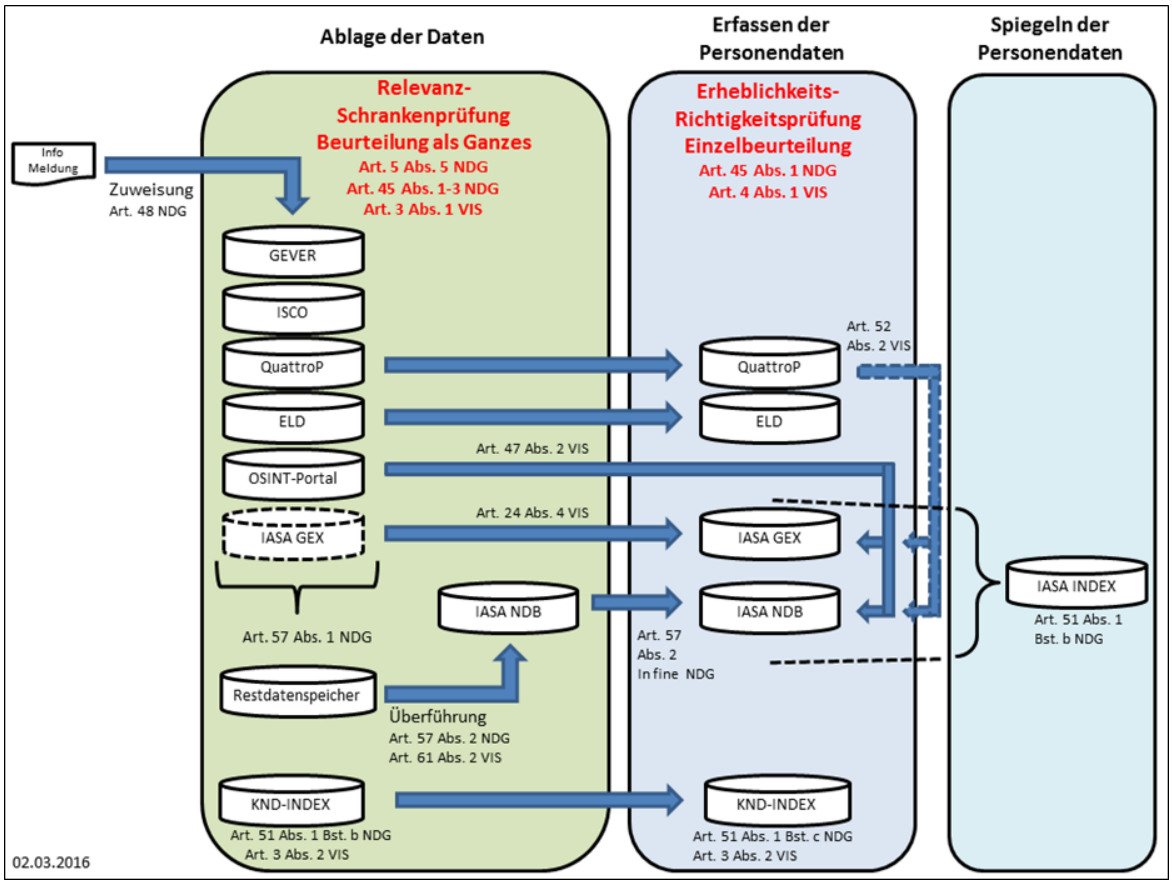
Die OCR-Technik entspricht geltendem Recht. Auch die Geschäftsprüfungsdelegation (GPDel) ist, unter Einhaltung gewisser Auflagen damit einverstanden. So verlangt die GPDel, dass das Auskunftsrecht uneingeschränkt auf alle Personen angewendet wird, die mittels Freitextsuche in ISIS gefunden werden können und, dass bei der Löschung einer Person aus IASA/IASA-GEX ebenfalls alle Textpassagen zu ihr aus den durchsuchbaren Meldungen gelöscht werden. Zudem sollen keine Meldungen, welche die politische Betätigung von Personen betreffen, für eine Textsuche zugänglich sein, wenn nicht der Verdacht besteht, dass diese Personen solche Tätigkeiten zu staatsgefährdenden Zwecken missbrauchen. Dass

[18] **SR 362.0**
[19] SR **121.2**

Originaldokumente mit Hilfe der optischen Zeichenerkennung (OCR-Technik) durchsuchbar gemacht und Papierakten, welche digitalisiert und als Originaldokumente erfasst worden sind, vernichtet werden dürfen, entspricht dem heute geltenden Recht (vgl. Abs. 3 und 4 des vorliegenden Entwurfs und Art. 5 ISV-NDB).

Art. 4 Einzelbeurteilung und Erfassung von Personendaten

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 Erfassung von Vorabklärungen im INDEX NDB (vgl. Abs. 2). 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.



Art. 5 Erteilung und Entzug der Zugriffsrechte

Wie im heute geltenden Recht (vgl. Art. 3 ISV-NDB) wird eine Zugriffsberechtigung auf ein Informationssystem nur auf individuellen Antrag und bezogen auf eine bestimmte Einzelperson erteilt (vgl. Abs. 1). Dies gilt neu auch für die Speichersysteme gemäss Artikel 1 Absatz 2 des vorliegenden Verordnungsentwurfs. Für die ELD kann 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. Zudem ist es bei ELD Standard, dass externe Pikettdienste mit ständig wechselndem Personenkreis Zugriff haben müssen. Die Zugriffserteilung auf individueller Ebene ist hier mit verhältnismässigen Mitteln schlicht nicht machbar. Aber es erfolgt eine Individualisierung auf funktionaler Ebene. Das Zugriffsprofil, das zunächst lediglich auf die Funktion ausgestellt ist, wird dabei bei der Benutzung einer individuellen Person zugeordnet. Die Benutzerorganisation ist verpflichtet zu dokumentieren, welche Person wann auf die ELD zugegriffen hat. Damit kann die Nachvollziehbarkeit der Zugriffe jederzeit gewährleistet werden.

Neu wird explizit geregelt, dass der Antrag nicht nur die Personalien und die Funktion der Antrag stellenden Person enthalten muss, 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.

Neu ist nicht mehr die zuständige Direktionsbereichsleiterin oder der zuständige Direktionsbereichsleiter (vgl. Abs. 3) für die formelle Prüfung der Zugriffsanträge zuständig. Dies soll dazu führen, dass die Zugriffsberechtigungen im ganzen NDB und für alle Informations- und Speichersysteme zentral und nach gleichen Kriterien vergeben werden. Zudem ist neu explizit

vorgesehen, dass Zugriffe entzogen werden können, wenn diese während 6 Monaten nicht verwendet wurden (vgl. Abs. 4). Das Applikationsmanagement des NDB wird bereits heute mit entsprechenden Aufträgen betraut.

In Absatz 5 wird klargestellt, dass der NDB nur für den Vollzug der Zugriffsrechte bei den von ihm selbst betriebenen Informationssystemen zuständig ist.

Art. 6 Systemübergreifender Zugriff und temporäre Auswertung

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 des Entwurfs sind bewusst 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 der Daten der Informations- und Speichersysteme des NDB separat im SiLAN abgelegt und nur den Mitgliedern dieses Projekts zugänglich gemacht werden können. Dies kann geboten sein, um die in Artikel 35 NDG statuierte Pflicht des Quellenschutzes zu erfüllen und entspricht heutiger Praxis und dem Datenhaltungskonzept des NDB. Diese temporären Auswertungen sind vom NDB zu bewilligen. Welche Stelle diese Bewilligung NDB-intern erteilt, wird im Datenschutzkonzept des NDB ausgeführt werden. Nach Abschluss der Arbeiten alle Resultate in die regulären Informationssysteme des NDB übertragen und die Datenkopien auf der Auswerteplattform vernichtet.

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

Temporäre Ablagen werden beispielsweise bei Entführungsfällen erstellt. Die Mitarbeitenden, die den Fall bearbeiten, sind darauf angewiesen, dass sämtliche Informationen, die im Zusammenhang mit der Entführung stehen, aus allen Informationssystemen des NDB zusammengezogen und auf einer Plattform gemeinsam ausgewertet werden können. Nach Abschluss der Arbeiten werden alle Resultate in die regulären Informationssysteme des NDB übertragen und die Datenkopien auf der Auswerteplattform gelöscht.

Art. 7 Operationsbezogene Daten

Bei operationsbezogenen 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 oder zum Schutz der Durchführung einer Operation angezeigt, 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 Person, welche mit der Führung einer Operation beauftragt ist oder deren Stellvertreter (vgl. Abs. 3). Eine Online-Abfrage existiert nicht.

Aus Sicherheitsgründen werden diese Daten in besonders geschützten Behältnissen (bspw. Safe) oder Räumlichkeiten (mit Zutrittsbeschränkungen) aufbewahrt (vgl. Abs. 2).

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 kann wird somit einerseits über diese Systeme und andererseits über die Plattformen der operationsbezogenen Daten garantiert.

Die oder der Leiter/in des Direktionsbereichs Beschaffung ist verpflichtet, periodisch zu prüfen, ob die Daten unter Berücksichtigung der aktuellen Lage für die Aufgabenerfüllung des NDB gemäss Artikel 6 NDG noch benötigt werden (vgl. Abs. 5).

Wie heute, dürfen diese Daten maximal 45 Jahre aufbewahrt werden (vgl. Abs. 6).

Art. 8 Löschen von Daten

Die Bestimmungen in diesem Artikel entsprechen dem heute geltenden Recht (vgl. Art. 7 ISV-NDB).

Die maximale Aufbewahrungsdauer wird bei den entsprechenden Informations- und Speichersystemen geregelt und ist je nach Herkunft, Zweck der Datenbearbeitung und Aufgabengebiet unterschiedlich (vgl. Abs. 1).

In IASA NDB und IASA-GEX NDB sind Objekte zu löschen, wenn diese nicht mehr mit zusätzlichen Informationen (Quellendokumenten) verbunden sind. Dies, damit keine Person verzeichnet ist, zu der man keine zusätzlichen Informationen hat und nicht mehr nachvollziehen kann, weshalb sie einst erfasst wurde (vgl. Abs. 2).

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 des Entwurfs). Dies heisst umgekehrt, dass ein Originaldokument gelöscht werden muss, wenn das letzte darauf referenzierte Quellendokument gelöscht wurde (vgl. Abs. 3). Grund dafür ist die in IASA-GEX NDB vorgesehene Erfassungskontrolle, die nur dann möglich ist, wenn Originaldokumente strukturiert erfasst werden.

Diese Vorschrift existiert nicht für IASA NDB. Dort können auch nicht referenzierte Originaldokumente bei Bedarf bis zur maximalen Aufbewahrungsfrist aufbewahrt werden (vgl. Abs. 4).

Absatz 5 enthält ebenfalls keine inhaltlichen Neurungen. Er stellt aber klar, dass nur die gelöschten und zur Archivierung bestimmten Daten in das Archivierungsmodul übertragen werden müssen. 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, etc.), gehören nicht ins Archivierungsmodul und sind zu vernichten.

Art. 9 Archivierung

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

Daten aus Vorabklärungen und Auftragsverwaltungsdaten der kantonalen Vollzugsbehörden fliessen in IASA NDB, IASA-GEX NDB, den INDEX NDB oder ins Informationssystem zur Geschäftsverwaltung (GEVER) ein, wenn dies für die Aufgabenerfüllung des NDB nach Artikel 6 Absatz 1 NDG notwendig ist. und werden über diese Informationssysteme abgeliefert (vgl. Abs. 2). Eine Doppelablieferung würde keinen Sinn ergeben.

3. Abschnitt: Allgemeine Bestimmungen über den Datenschutz und Daten-sicherheit

Art. 10 Auskunftsrecht von betroffenen Personen

Das Auskunftsrecht betroffener Personen wird ausführlich in Artikel 63 NDG geregelt. Auf Verordnungsstufe sind deshalb keine zusätzlichen Ausführungsbestimmungen notwendig.

Art. 11 Qualitätssicherung

Bei Artikel 11 des vorliegenden Verordnungsentwurfs 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. Diese Aufgabe wird primär von den erfassenden Stellen, also den Spezialisten, wahrgenommen, was einen grösseren Einbezug des Sachwissens zum Beispiel der Auswertung in die Qualitätssicherung ermöglicht. Dieser Einbezug des analytischen Fachwissens bei der Qualitätssicherung der Daten entspricht einer expliziten Forderung der GPDel im ISIS-Bericht von 2010 und wurde vom Bundesrat bereits im Rahmen der ZNDG-Revision auf die Qualitätssicherung der Auslanddaten des NDB umgesetzt. Die Zuständigkeiten und Fristen sowie der Umfang der periodischen Prüfungen werden in den besonderen Bestimmungen des jeweiligen Informationssystems geregelt (vgl. Abs. 1).

Der Absatz 2 entspricht im Prinzip dem heutigen Artikel 13 Absatz 4 ISV-NDB. Die Pflicht zur Stichprobenkontrolle wird jedoch auf sämtliche Informationssysteme ausgedehnt (heute sind ISIS und das Informationssystem Äussere Sicherheit ISAS davon ausgenommen). Im Unterschied zur periodischen Überprüfung, für die primär die erfassenden Stellen zuständig sind, wird die Stichprobenkontrolle ausschliesslich durch die Qualitätssicherungsstelle des NDB vorgenommen. Es werden nicht sämtliche Daten der Informationssysteme geprüft, sondern nur eine Auswahl, welche für die Stichprobe zusammengestellt wurde. Das Resultat der Stichprobenkontrollen fliesst in Empfehlungen und Schulungen insbesondere der erfassenden Stellen ein.

Bereits 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. Diese Überprüfungen sollen auch unter dem Regime des NDG weitergeführt werden. Neu wird dies sowohl IASA-GEX NDB als auch IASA NDB betreffen, was nun explizit in Absatz 3 festgehalten wird. Die Datenbearbeitungsschranke von heute Artikel 3 BWIS ist neu in Artikel 5 Absatz 5 NDG geregelt.

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). Heute wurde dies lediglich im Rahmen der Gesamtbeurteilungen getan.

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 Verantwortlichkeit 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

Auch die Nutzung und Betreibung des SiLAN erfährt im Vergleich zu heute keine Änderung. Gemäss Absatz 2 dürfen weiterhin im SiLAN Daten aller Klassifizierungsstufen bearbeitet werden.

Neu werden auch die Mitarbeiterinnen und Mitarbeiter der kantonalen Vollzugsbehörden Zugriff auf 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. Dadurch entstehen jedoch keine finanziellen Mehraufwendungen.

Art. 15 Datenübermittlung ausserhalb von SiLAN

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

Neu muss aber nicht mehr die Datenübermittlung zu den Kantonen finanziert werden, sondern deren Zugriff auf das SiLAN und die darin geführten Daten (vgl. Abs. 2).

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 Daten

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 Aufgabengebieten des NDB mit Ausnahme desjenigen des gewalttätigen Extremismus (vgl. Abs. 1).

Die Absätze 2, 4 und 5 entsprechen dem heute geltenden Recht und wurden von den Artikeln 16 Absätze 2, 3 und 4 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. Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) wird weiterhin die Datenfelder regeln (vgl. die heutige Verordnung des VBS vom 27. Juli 2015[20] über die Datenfelder und die Zugriffsrechte in den Informationssystemen ISIS und ISAS).

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 Personendaten

In Absatz 1 wird die heutige Pflicht zur periodischen Überprüfung von Personendaten in ISAS übernommen (vgl. Art. 18 Abs. 1 ISV-NDB). Der einzige Unterschied besteht darin, dass (wie in dem ganzen Verordnungsentwurf) 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, wie bereits erwähnt, einen grösseren Einbezug des Sachwissens in die Qualitätssicherung sicherstellt.

Die Aufgaben, welche dabei von den überprüfenden Personen wahrzunehmen sind, haben sich im Vergleich zu heute auch nicht verändert (vgl. Abs. 2 und Art. 18 Abs. 2 ISV-NDB). Es wird aber klargestellt, dass das Ergebnis der Überprüfung nur dann festgehalten werden muss, wenn der Datensatz verändert oder nicht gesamthaft gelöscht wird. Wird der Datensatz nicht verändert, wird die erfolgte Überprüfung automatisch vom System festgehalten.

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 Datensatz mehrmals pro Tag durch verschiedene Mitarbeiterinnen

[20] SR **121.22**

und Mitarbeiter des NDB ergänzt und überprüft wurde. 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 Datensätze 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 Datensatz Quellendokumente aus verschiedenen Bereichen enthält und demnach verschiedene Maximalfristen aufweist.

Art. 21 Aufbewahrungsdauer

Die Aufbewahrungsfristen für Daten in IASA NDB entsprechen exakt denjenigen des heutigen ISAS (vgl. Art. 19 ISV-NDB).

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 Daten

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 oder 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).

Die Absätze 2 bis 5 finden sich im Artikel 22 Absätze 3 und 4 sowie Artikel 23 Absatz 4 ISV-NDB und entsprechen dem geltenden Recht. Das VBS wird weiterhin die Datenfelder regeln.

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 Aufgaben nach dem NDG bestätigt oder verneint. Ist dies nicht der Fall, wird der Datensatz 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 38 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, 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 unverändert von Artikel 24 ISV-NDB übernommen. Nur der Verweis auf die Datenbearbeitungsschranke wurde aktualisiert, da diese neu in Artikel 5 Absatz 5 NDG geregelt wird. 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 Personendaten

Das Instrument der periodischen Überprüfung wird unverändert von ISIS übernommen (vgl. Art. 25 ISV-NDB). Die Qualitätssicherungsstelle des NDB überprüft die Datensätze 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 exakt 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 Daten

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 Abs. 4 geregelt ist.

Ebenfalls wie heute sehen die Absätze 5 und 6 vor, dass der Katalog der Personendaten im Anhang aufgelistet wird und das VBS die Datenfelder festlegt.

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 (vgl. Abs. 1). Das heisst, ein Bezug zum Aufgabengebiet des NDB nach Artikel 6 NDG muss immer (auch bei der Erfassung von Personendaten in den Vorabklärungen gemäss Art. 29 Bst. b des Verordnungsentwurfs) gegeben sein und die Datenbearbeitungsschranke von Artikel 5 Absatz 5 NDG muss eingehalten werden.

In der Vernehmlassung zum NDG hatten die kantonalen Vollzugsbehörden den Wunsch geäussert, gegenseitig Zugriff auf ihre Vorabklärungen gemäss Artikel 29 Bst. b des Verordnungsentwurfs nehmen zu können. Dies um kantonsübergreifend festzustellen, ob bereits über eine natürliche oder juristische Person, einen Gegenstand oder ein Ereignis von einer kantonalen Vollzugsbehörde Abklärungen getätigt werden. Die Anzahl von Personen, die in unterschiedlichen Kantonen leben, arbeiten oder tätig sind, hat stark zugenommen. Die Koordination der für die Vorabklärungen notwendigen Arbeiten erlaubt ein zielgerichteteres und damit auch schlankeres Vorgehen der kantonalen Vollzugsbehörden. Dieses Anliegen wurde in Absatz 2 aufgenommen. Werden im Rahmen von Vorabklärungen Objekte erfasst, soll es somit möglich sein, anderen kantonalen Vollzugsbehörden Zugriff auf diese zu gewähren.

Variante zu Absatz 2

Die KKPKS hat angeregt, dass die kantonalen Vollzugsbehörden jederzeit die Möglichkeit haben sollen, abzuklären, ob eine andere kantonale Vollzugsstelle im Rahmen ihrer Zuständigkeit bereits Informationen zu einer bestimmten Person oder Organisation getätigt hat. Eine Kann-Formulierung genüge nicht, die Kantone müssten proaktiv einen abschliessenden Abgleich der kantonalen Bereiche im INDEX NDB vornehmen können.

Zu Artikel 31 Absatz 2 stehen somit 2 Varianten zur Diskussion. Welcher Variante der Vorzug gegeben wird, entscheidet sich nach den Präferenzen im Vernehmlassungsverfahren.

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 nehmen können. Dies um Doppelspurigkeiten 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 Abs. 2 für die Übersicht über die individuellen Zugriffsrechte auf den Anhang 4.

Art. 33 Periodische Überprüfung der Personendaten

In den IASA INDEX nach Artikel 29 Buchstabe a des Verordnungsentwurfs werden nur diejenigen Daten gespiegelt, die in IASA NDB und IASA-GEX NDB erfasst und nach den für diese Informationssysteme geltenden Vorschriften (periodisch) überprüft werden. Von dem her erübrigt sich im IASA INDEX selber eine periodische Überprüfung. Es ist jedoch angezeigt, dass die Qualitätssicherungsstelle des NDB periodisch überprüft, ob die Vorgaben zur Aufnahme der Daten von IASA NDB und IASA-GEX NDB eingehalten werden. Dies wird sie einmal jährlich tun (vgl. Abs. 1 Bst. a).

Die Daten nach Artikel 29 Buchstabe b und c des Verordnungsentwurfs werden, soweit relevant und genügend verdichtet, in IASA NDB oder IASA-GEX aufgenommen und nach den für diese Informationssysteme massgebenden Vorschriften periodisch überprüft. Die Qualitätssicherungsstelle des NDB hat zudem den Auftrag einmal jährlich zu prüfen, ob die Bearbeitung der Daten durch die kantonalen Vollzugsbehörden im Vollzug des NDG erfolgt, die Datenbearbeitungsschranke von Artikel 5 Absatz 5 NDG eingehalten wird und ob die Daten nicht länger als fünf Jahre aufbewahrt werden (vgl. Abs. 1 Bst. b). Gegebenenfalls korrigiert oder löscht sie Daten und führt Schulungen durch. Sie konzentriert sich dabei je nach Kontrollplan auf die Datenbearbeitung einer oder mehrerer kantonalen Vollzugsbehörden.

Die Qualitätssicherungsstelle hält zur besseren Nachvollziehbarkeit das Ergebnis der Prüfung in einem Bericht an die Direktorin oder den Direktor des NDB fest (vgl. Abs. 2).

Art. 34 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer von Daten des IASA INDEX gemäss Artikel 29 Buchstabe a des Verordnungentwurfs 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 IASA INDEX, 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).

Gemäss Absatz 3 i.V.m. Artikel 45 Absatz 5 Buchstabe d NDG löscht 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 Daten

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[21] in GEVER NDB Daten der Klassifizierungsstufen VERTRAULICH und GEHEIM unverschlüsselt abgelegt werden können (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 Periodische Überprüfung der Personendaten

Gemäss Absatz 1 ist die Qualitätssicherungsstelle des NDB für die neu vorgesehene periodische Überprüfung der GEVER-Daten zuständig. Sie stellt u.a. sicher, dass Daten, die zur Erstellung der Inhalte nach Artikel 52 Absatz 2 Buchstabe a und b NDG verwendet wurden, nicht zu lange aufbewahrt werden. Zu diesem Zweck überprüft sie mindestens alle 10 Jahre die Verzeichnisse und Unterverzeichnisse des Registerplans und beurteilt unter Berücksichtigung der aktuellen Lage, ob die darin enthaltenen Daten für die Geschäftsbearbeitung und –kontrolle sowie zur Sicherung effizienter Arbeitsabläufe des NDB noch benötigt werden.

Ist dies nicht der Fall, werden sie gelöscht und dem Schweizerischen Bundesarchiv abgeliefert (vgl. Abs. 2). Die Qualitätssicherungsstelle hält zur besseren Nachvollziehbarkeit das Ergebnis der Prüfung in einem Bericht an die Direktorin oder den Direktor des NDB fest.

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.

Die ELD ist von der Verwendungssperre nicht betroffen. Für die Lagerverfolgung werden zwangsläufig Daten verwendet, die direkt aus der ELD stammen und auch für die Erstellung von nachrichtendienstlichen Produkten ist es teilweise nötig, diese Daten direkt nutzen zu können, wenn sie in keinem anderen Informationssystem erfasst wurden. Aufgrund der kurzen Aufbewahrungsfrist der Daten in ELD entstehen keine Konflikte mit den anderen Systemen.

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 beträgt unverändert 45 Jahre (vgl. Art. 40 Abs. b ISV-NDB).

---

21 SR **172.010.441**

8. Abschnitt: Besondere Bestimmungen über die ELD

Art. 41 Struktur

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

Art. 42 Daten

Der Inhalt der ELD richtet sich nach Artikel 53 Absatz 2 NDG und erfährt ebenfalls im Vergleich zu heute keine Änderung (vgl. Art. 30 Abs. 1 ISV-NDB). Personendaten werden in der ELD nur insofern geführt, als dies zur Lagedarstellung und -beurteilung unbedingt notwendig ist.

Art. 43 Zugriffsrechte

Die Zugriffsrechte auf die 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 die 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 Periodische Überprüfung

Die neu vorgesehene periodische Überprüfung der Daten der ELD wird von den für die Datenablage in der ELD zuständigen Mitarbeiterinnen und Mitarbeiter des NDB vorgenommen (vgl. Abs. 1). Dabei werden alle Informationen, welche im Hinblick auf die Steuerung und Umsetzung sicherheitspolizeilicher Massnahmen nicht mehr benötigt werden und vor mehr als drei Jahren erfasst wurden, gelöscht und dem Schweizerischen Bundesarchiv abgeliefert (vgl. Abs. 2). Die Qualitätssicherungsstelle des NDB führt zusätzlich Stichproben gemäss Artikel 11 Absatz 2 durch (vgl. Abs. 4).

Die Mitarbeiterinnen und Mitarbeiter, welche die periodische Überprüfung durchgeführt haben, halten zur besseren Nachvollziehbarkeit das Ergebnis der Prüfung in einem Bericht an die Qualitätssicherungsstelle des NDB fest (vgl. Abs. 3).

Art. 45 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer wurde unverändert von Artikel 31 ISV-NDB übernommen und beträgt drei Jahre.

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 Daten

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 diese 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 werden im OSINT-Portal lediglich Daten aus öffentlichen Quellen abgelegt, die automatisierte Erfassung betrifft insbesondere Agenturmeldungen und ähnliches.

Eine Übersicht über die Personendaten und die individuellen Zugriffsrechte findet sich im Anhang 9 (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 10 (vgl. Abs. 2).

Art. 49 Periodische Überprüfung

Die neu vorgesehene periodische Überprüfung des OSINT-Portals wird durch die für die Datenablage im OSINT-Portal zuständigen Mitarbeiterinnen und Mitarbeiter des NDB vorgenommen (vgl. Abs. 1). Diese haben mindestens alle fünf Jahre unter Berücksichtigung der aktuellen Lage zu prüfen, ob die Daten für die Aufgabenerfüllung des NDB gemäss Artikel 6 NDG noch benötigt werden und löschen sämtliche Daten, die älter als 15 Jahre sind und liefern diese dem Schweizerischen

Bundesarchiv ab (vgl. Abs. 2). Die Qualitätssicherungsstelle des NDB führt zusätzlich eine Stichprobe gemäss Artikel 11 Absatz 2 durch (vgl. Abs. 4).

Die Mitarbeiterinnen und Mitarbeiter, welche die periodische Überprüfung durchgeführt haben, halten zur besseren Nachvollziehbarkeit das Ergebnis der Prüfung in einem Bericht an die Qualitätssicherungsstelle des NDB fest (vgl. Abs. 3).

Art. 50 Aufbewahrungsdauer

Um die qualitativ hochwertigen und strukturieren Daten des OSINT-Portals über einen längeren Zeitraum zu nutzen und mittels Analysetools aussagekräftig auswerten zu können (z.B. Verfolgen der Entstehung und Ausbreitung des Islamischen Staates IS und seiner Aktivitäten in den öffentlich zugänglichen Bereichen des Internets) wurde die Aufbewahrungsfrist auf 20 Jahre festgelegt.

10. Abschnitt: Besondere Bestimmungen über Quattro P

Art. 51 Struktur

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

Art. 52 Daten

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

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 11 (vgl. Abs. 4).

Art. 53 Zugriffsrechte

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

Art. 54 Periodische Überprüfung

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 mindestens alle fünf Jahre, ob die Daten, welche die Grenzkontrollorgane dem NDB übermittelt haben und in Quattro P abgelegt wurden, mit der vom Bundesrat festgelegten Liste nach Artikel 55 Absatz 4 NDG übereinstimmen und ob diese für die Aufgabenerfüllung des NDB nach Artikel 6 NDG noch benötigt werden. 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 wie heute höchstens fünf Jahre (vgl. Art. 36 ISV-NDB).

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 Daten

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 Periodische Überprüfung

Bereits heute werden die Aufklärungsaufträge und Datenbestände periodisch 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 Mitarbeiterinnen und Mitarbeiter, welche die periodische Überprüfung durchgeführt haben, halten zur besseren Nachvollziehbarkeit das Ergebnis der Prüfung in einem Bericht an die Qualitätssicherungsstelle des NDB fest (vgl. Abs. 3).

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 Struktur

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). Bei der Eingangsprüfung werden die Daten dahingehend geprüft, ob genügend Anhaltspunkte bestehen, dass der Aufgabenbezug nach Artikel 6 NDG gegeben ist (vgl. Art. 3 Abs. 1 der vorliegenden Verordnung).

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 *Daten*

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 Periodische Überprüfung

Gemäss Absatz 1 überprüft die Qualitätssicherungsstelle des NDB mindestens alle 10 Jahre unter Berücksichtigung der aktuellen Lage, ob die Datenbestände des Restdatenspeichers für die Aufgabenerfüllung des NDB nach Artikel 6 NDG noch notwendig und nicht älter als 10 Jahre sind. Nicht mehr benötigte Daten und Daten, die älter als 10 Jahre sind, werden gelöscht und dem Schweizerischen Bundesarchiv abgeliefert (vgl. Abs. 2).

Zudem hat die Qualitätssicherungsstelle zu prüfen, ob die Auflagen für die Überführung von Daten eingehalten und überführte Daten vernichtet werden (vgl. Abs. 3). Sie hält zur besseren Nachvollziehbarkeit das Ergebnis der Prüfung in einem Bericht an die Direktorin oder den Direktor des NDB fest. Hat die Qualitätssicherungsstelle bei ihrer Prüfung Mängel festgestellt, werden im Bericht Empfehlungen ausgesprochen und deren Umsetzung in die Pendenzenliste der Geschäftsleitung NDB aufgenommen (dies gilt im Übrigen auch für GEVER).

Die Qualitätssicherungsstelle des NDB führt zudem eine Stichprobe gemäss Artikel 11 Absatz 2 durch (vgl. Abs. 4).

Art. 65 Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer für die Daten im Restdatenspeicher beträgt höchstens 10 Jahre.

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

Art. 66 Struktur

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 Daten

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 Verwendungssperre

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.

Für Daten von unbeteiligten Personen und solchen, denen ein Zeugnisverweigerungsrecht nach Artikel 171-173 StPO zusteht, gilt eine absolute Verwendungssperre und sind spätestens 30 Tage nach Beendigung der Massnahme zu vernichten (vgl. Abs. 2). Auf diese Weise wird sichergestellt, dass solche Daten nicht in Produkte des NDB Eingang finden oder weitergegeben werden.

Die Qualitätssicherungsstelle des NDB prüft stichprobenweise, ob diese Verwendungssperre eingehalten wird (vgl. Abs. 3).

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 in Artikel 58 Absatz 3 NDG vorgesehene Aufsicht des Bundesverwaltungsgerichts bei der Vernichtung von Daten wird dadurch sichergestellt, dass vor der Vernichtung derselben ein Antrag mit den Angaben zu den ausgesonderten und für die Vernichtung bestimmten Daten an das Bundesverwaltungsgericht gestellt werden muss (vgl. Abs. 3).

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

Anhänge 1, 3, 5, 7, 9, 11, 13, 15 und 17: 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, 4, 6, 8, 10, 12, 14, 16 und 18: Zugriffsrechte

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