Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes (ISV-NDB)

vom 4. Dezember 2009

Der Schweizerische Bundesrat,

gestützt auf Artikel 5 Absätze 1 und 4 des Bundesgesetzes vom 3. Oktober 2008[1] über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG), auf die Artikel 15 Absätze 3 und 5 sowie 30 des Bundesgesetzes vom 21. März 1997[2] über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) sowie auf Artikel 17*a* des Bundesgesetzes vom 19. Juni 1992[3] über den Datenschutz,

verordnet:

1. Abschnitt: Gegenstand und Begriffe

Art. 1 Gegenstand

Diese Verordnung regelt Betrieb, Datenbestand und Nutzung der folgenden Informationssysteme des Nachrichtendienstes des Bundes (NDB):

a. Informationssystem Äussere Sicherheit (ISAS);

b. Informationssystem Innere Sicherheit (ISIS).

Art. 2 Begriffe

In dieser Verordnung bedeuten:

a. Daten: in den Informationssystemen des NDB gespeicherte Informationen;

b. Objekt: Zusammenstellungen von Daten, die sich auf eine oder mehrere Personen, Organisationen, Sachen oder Ereignisse beziehen;

c. Meldung: einzelner Informationseingang zu einem oder mehreren Objekten;

d. Relation: Beziehung zwischen einem Objekt und einer Meldung;

e. Datensatz: Gesamtheit an Meldungen und Relationen eines Objekts;

f. OCR-Daten: Daten von Akten, die so eingelesen wurden, dass eine Freitextsuche möglich ist;

SR **121.2**

1 SR **121**
2 SR **120**
3 SR **235.1**

g. Bilddaten: Dokumente, die in Form von Bildern eingelesen wurden;

h. Kurzabfrage: eingeschränkte Online-Abfrage zur Feststellung, ob eine Person in einem Informationssystem des NDB verzeichnet ist;

i. Drittperson: Person oder Organisation, die nur über den Bezug zu einem Objekt eine Staatsschutzrelevanz hat;

j. Faktenblatt: standardisierte, periodisch nachgeführte Beurteilungen der strategischen Analyse zu einem Objekt.

2. Abschnitt: Allgemeine Bestimmungen über die Informationssysteme des NDB

Art. 3 Zweck der Informationssysteme des NDB

1 Die Informationssysteme des NDB dienen dem NDB zur Erfüllung seiner Aufgaben gemäss Artikel 1 ZNDG.

2 Sie werden verwendet:

a. zur Recherche in den erfassten Daten und zu deren Analyse;

b. zur Erstellung von Lageberichten;

c. zur Erledigung administrativer Aufgaben;

d. zur Ablage und zur Verwaltung von Akten;

e. zur Dokumentation;

f. zur Geschäftsabwicklung.

Art. 4 Abfrageberechtigungen

1 Wer die Informationssysteme des NDB grundsätzlich abfragen darf, hat auf diejenigen Daten Zugriff, die er oder sie zur Erfüllung der gesetzlichen Aufgaben benötigt.

2 Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) regelt die Abfrageberechtigungen.

3 Die Direktorin oder der Direktor des NDB oder die Stellvertreterin oder der Stellvertreter entscheidet über die individuellen Anträge.

4 Das Informationsmanagement des NDB ist für den Vollzug der Abfrageberechtigungen zuständig.

Art. 5 Abfrage und visuelle Darstellung von Daten

1 Die Benutzerinnen und Benutzer der Informationssysteme des NDB können die Daten nach Objekten, Relationen, Meldungen, Aktivitäten und Freitext abfragen.

2 Die Objekte und ihre Relationen können visuell dargestellt und die Darstellungen abgespeichert werden.

Art. 6 Informatisiertes Analyse- und Auswertungstool

Die Benutzerinnen und Benutzer der Informationssysteme des NDB können im Rahmen ihrer Zugriffsberechtigungen mittels eines informatisierten Analyse- und Auswertungstools auf alle Informationssysteme des NDB gleichzeitig zugreifen.

Art. 7 SILAN

[1] Das SILAN ist ein chiffriert betriebenes Kommunikationssystem innerhalb des NDB zur Bearbeitung von geheim klassifizierten Daten.

[2] Der NDB stellt dieses System ausschliesslich den Benutzerinnen und Benutzern des NDB zur Verfügung.

Art. 8 Intranet NDB

[1] Das Intranet NDB ist ein chiffriert betriebenes Kommunikationssystem zur Bearbeitung von vertraulich klassifizierten Daten.

[2] Der NDB stellt dieses System ausschliesslich den Benutzerinnen und Benutzern von ISIS zur Verfügung.

Art. 9 Allgemeine Dokumentation

[1] Der NDB führt in seinen Informationssystemen eine Dokumentation aus öffentlich zugänglichen Quellen mit:

a. Informationen über Personen, Organisationen und Sachverhalten im Aufgabenbereich des ZNDG;

b. Informationen über Personen und Organisationen, deren Sicherheit in der Schweiz gefährdet sein könnte;

c. Informationen über Länder sowie gesellschaftliche und politische Hintergründe, die für die Lagebeurteilung relevant sein können;

d. wissenschaftlichen und technischen Informationen im Arbeitsgebiet der Sicherheitsbehörden.

[2] Er betreibt zur Nutzung öffentlich zugänglicher Quellen ein personalisiertes Portal (Interaktives Portal für Open Sources; IPOS).

[3] Er führt eine Dokumentationsstelle über Material, das Rassismus oder Gewalt propagiert. Diese Stelle unterstützt strafrechtliche oder administrative Verfahren, die sich mit solchem Propagandamaterial befassen.

Art. 10 Weitergabe von Personendaten

[1] Der NDB kann die in seinen Informationssystemen bearbeiteten Personendaten an die Behörden und Amtsstellen nach Anhang 3 der Verordnung vom 4. Dezember 2009[4] über den Nachrichtendienst des Bundes (V-NDB) weitergeben, zu den in

4 SR **121.1**

diesem Anhang aufgeführten Zwecken und unter den dort festgelegten Bedingungen.

2 Für die Weitergabe an das Ausland gelten:

a. für Informationen über das Ausland: die Artikel 5 Absatz 3 ZNDG und 14 V-NDB;

b. für Informationen über das Inland: die Artikel 17 Absätze 3–5 BWIS.

3 Die Weitergabe von Daten ist nicht zulässig, wenn ihr überwiegende öffentliche oder private Interessen entgegenstehen.

4 Der NDB setzt bei jeder Weitergabe die Empfängerin oder den Empfänger über die Bewertung und die Aktualität der Daten in Kenntnis.

5 Er weist die Empfängerin oder den Empfänger hin:

a. auf den Zweck, zu dem sie oder er die Daten ausschliesslich verwenden darf;

b. darauf, dass er sich vorbehält, Auskunft über die vorgenommene Verwendung zu verlangen.

6 Er registriert die Weitergabe von ISIS-Daten sowie die Empfängerin oder den Empfänger, den Gegenstand und den Grund der Weitergabe.

Art. 11 Kopieren von Daten in Datensammlungen

1 Die Daten der Informationssysteme des NDB dürfen weder über Kommunikationseinrichtungen noch über Datenträger in andere Datensammlungen kopiert werden.

2 Zur Vornahme spezieller Auswertungen dürfen Daten aus den Informationssystemen des NDB kurzfristig in Arbeitsdatenbanken überführt werden. Nach Abschluss der Auswertungsarbeiten sind diese Daten zu vernichten.

Art. 12 Vernichtung von Daten

1 Die Daten werden innert drei Monaten nach Ablauf ihrer Aufbewahrungsdauer gemäss den Artikeln 24 und 33 vernichtet.

2 Die Direktorin oder der Direktor des NDB oder die Stellvertreterin oder der Stellvertreter kann für Daten, die unter Beurteilung der aktuellen Risiken und Gefahren für die Erfüllung der gesetzlichen Aufgabe des NDB unentbehrlich sind, eine einmalige Verlängerung der Aufbewahrungsfrist von drei Jahren beschliessen.

3 Mit der Vernichtung der letzten Meldung (inklusive der dazugehörigen Relationen, Bilddaten und Aufträge) werden der gesamte Datensatz sowie ein allfällig vorhandenes Faktenblatt vernichtet.

4 Zur Vernichtung vorgesehene Daten werden in das Archivierungsmodul übertragen; vorbehalten bleibt Artikel 13 Absatz 2.

Art. 13 Archivierung

1 Der NDB bietet nicht mehr benötigte oder zur Vernichtung bestimmte Daten und Akten dem Bundesarchiv zur Archivierung an.

2 Er bietet die aus dem direkten Verkehr mit ausländischen Sicherheitsdiensten und aus der operativen Beschaffung stammenden klassifizierten Daten und Akten nicht zur Archivierung an. Er bewahrt diese in Absprache mit dem Bundesarchiv intern auf und vernichtet sie nach 45 Jahren.

3 Er vernichtet die vom Bundesarchiv als nicht archivwürdig bezeichneten Daten des Archivierungsmoduls sowie die dazugehörigen Akten. Vorbehalten bleiben weitere gesetzliche Bestimmungen über die Datenvernichtung.

Art. 14 Datensicherheit und Protokollierung

1 Für die Gewährleistung der Datensicherheit gelten:

a. Artikel 20 der Verordnung vom 14. Juni 1993[5] zum Bundesgesetz über den Datenschutz;

b. die Verordnung vom 26. September 2003[6] über die Informatik und Telekommunikation in der Bundesverwaltung;

c. die vom VBS nach Artikel 28 festzulegenden Voraussetzungen für den Anschluss der kantonalen Organe zur Wahrung der inneren Sicherheit.

2 Der NDB regelt in Bearbeitungsreglementen:

a. die organisatorischen und technischen Massnahmen gegen unbefugtes Bearbeiten der Daten;

b. die automatische Protokollierung der eingegebenen Daten.

3 ISIS-Daten dürfen während des gesamten Übertragungsvorganges nur in chiffrierter Form übertragen werden.

Art. 15 Verantwortlichkeiten und Zuständigkeiten

1 Der NDB trägt die Verantwortung für seine Informationssysteme.

2 Er erlässt die Bearbeitungsreglemente.

3 Das Informationsmanagement NDB ist zuständig für die Ausbildung und Betreuung der Benutzerinnen und Benutzer und sorgt für die Durchsetzung der Bearbeitungsreglemente.

4 Das VBS trägt die technische Gesamtverantwortung für die Informationssysteme des NDB.

5 Der EDV-Leistungserbringer sorgt für den Betrieb, den Unterhalt und die Sicherheit.

6 Die Datenschutzberaterin oder der Datenschutzberater des NDB kann einzelfallweise die Bearbeitung von Daten in seinen Informationssystemen auf die Einhaltung der Datenschutzvorschriften überprüfen.

5 SR **235.11**
6 SR **172.010.58**

Art. 16 Technische Anforderungen

[1] Das VBS legt die technischen Anforderungen fest, denen die Endgeräte der Benutzerinnen und Benutzer genügen müssen.

[2] Die Bearbeitungsreglemente für die jeweiligen Informationssysteme legen die Einzelheiten fest.

3. Abschnitt: Informationssystem Äussere Sicherheit (ISAS)

Art. 17 Pilotbetrieb ISAS

[1] ISAS wird im Rahmen eines befristeten Pilotbetriebes im Sinne von Artikel 17*a* des Bundesgesetzes vom 19. Juni 1992[7] über den Datenschutz geführt.

[2] Der NDB legt dem Bundesrat innert zwei Jahren nach Inbetriebnahme von ISAS einen Evaluationsbericht vor.

[3] Der Bundesrat entscheidet über die Überführung von ISAS vom Pilotbetrieb in den regulären Betrieb.

[4] Die Bestimmungen des 1. und 2. Abschnitts (Art. 1–16) sind für den Pilotbetrieb von ISAS anwendbar.

Art. 18 Datenbanken

[1] ISAS besteht aus den folgenden Datenbanken:

a. Rohdaten (RD);
b. Extremismus (EX);
c. Terrorismus (TE);
d. Non-Proliferation (NP);
e. Nachrichtendienst (ND);
f. Militär (MI);
g. Wirtschaft und Ressourcen (WR);
h. internationale Politik und Strategie (IPS);
i. Dokumentation (DO).

[2] Die Datenbanken enthalten die folgenden für die Aufgabenerfüllung des NDB gemäss Artikel 1 ZNDG bedeutsamen Informationen über das Ausland:

a. RD: OCR-Daten in unstrukturierter oder semi-strukturierter Form, die in EX, TE, NP, ND, MI, WR, IPS und DO bearbeitet werden können;
b. EX: personen- und ereignisbezogene Informationen in strukturierter Form aus dem Bereich des gewalttätigen Extremismus;

7 SR **235.1**

c. TE: personen- und ereignisbezogene Informationen in strukturierter Form aus dem Bereich des Terrorismus;

d. NP: personen- und ereignisbezogene Informationen in strukturierter Form aus dem Bereich der Non-Proliferation; die Informationen können auch solche über das Inland umfassen;

e. ND: personen- und ereignisbezogene Informationen in strukturierter Form aus dem Bereich des verbotenen Nachrichtendienstes;

f. MI: personen-, ereignis- und sachbezogene Informationen in strukturierter Form aus dem Bereich Militär;

g. WR: personen- und ereignisbezogene Informationen in strukturierter Form aus dem Bereich Wirtschaft und Ressourcen;

h. IPS: personen- und ereignisbezogene Informationen in strukturierter Form aus dem Bereich internationale Politik und Strategie;

i. DO: personen- und ereignisbezogene dokumentarische Informationen aus der präventiven Staatsschutztätigkeit sowie Informationen aus öffentlich zugänglichen Quellen gemäss Artikel 9.

Art. 19 Bearbeitete Daten

1 Die ISAS-Datenbanken EX, TE, NP, ND, MI, WR, IPS und DO sind nach Meldungen, Objekten und Relationen strukturiert.

2 Das VBS regelt die einzelnen Datenfelder.

Art. 20 Abfrageberechtigungen

Die für die Durchführung des Pilotbetriebes zuständigen Mitarbeiterinnen und Mitarbeiter des NDB können ISAS abfragen, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben notwendig ist.

Art. 21 Dateneingabe und Qualitätskontrolle

1 In ISAS dürfen nur Informationen bearbeitet werden, die den Zweckbestimmungen nach Artikel 3 entsprechen.

2 Die Voranalyse des NDB gibt die Daten in ISAS ein.

3 Zusätzlich können die folgenden Personen Daten in die nachstehenden Datenbanken eingeben und die Meldungskategorien festlegen:

a. die Mitarbeiterinnen und Mitarbeiter des ComCenters des NDB: Daten in die Datenbank RD;

b. die Mitarbeiterinnen und Mitarbeiter der Auswertung des NDB: Daten in die Datenbanken EX, TE, NP, ND, MI, WR, IPS und DO.

4 Die Direktorin oder der Direktor des NDB beziehungsweise die Stellvertreterin oder der Stellvertreter kann die Qualitätssicherung ISIS mit einer Überprüfung der ISAS-Datenbanken beauftragen.

Art. 22 Aktenablage

[1] Die Aktenablage hat die ordnungsgemässe Aktenführung und Archivierung zu gewährleisten.

[2] Die den Objekten und Meldungen zu Grunde liegenden Akten können als OCR-Daten erfasst werden.

[3] Auf die Ablage der Akten in Papierform kann verzichtet werden, sofern die den Objekten und Meldungen zu Grunde liegenden Akten als OCR-Daten erfasst sind.

Art. 23 Auskunftsrecht von betroffenen Personen

Das Auskunftsrecht richtet sich nach den Bestimmungen des Bundesgesetzes vom 19. Juni 1992[8] über den Datenschutz.

Art. 24 Aufbewahrungsdauer

[1] Die ISAS-Daten und die dazugehörigen Akten dürfen vom Zeitpunkt ihrer letzten Bearbeitung an längstens 30 Jahre aufbewahrt werden.

[2] Die maximale Aufbewahrungsfrist beträgt 45 Jahre.

4. Abschnitt: Informationssystem Innere Sicherheit (ISIS)

Art. 25 Systeme und Datenbanken

[1] ISIS besteht aus den folgenden Subsystemen und Datenbanken:

a. «ISIS00 Allgemein» mit der Aktenablage, Auftragsverwaltung, Risikoanalyse, Statistik und dem Archivierungsmodul;

b. «ISIS01 Staatsschutz» mit den Datenbanken:
   1. «Staatsschutz»,
   2. «Verwaltungspolizei»,
   3. «Dokumentation»,
   4. «Nummernsystem»;

c. «ISIS02 Verwaltung» mit der Datenbank «Verwaltung»;

d. «ISIS05 News» mit den Datenbanken:
   1. «NEWS»,
   2. «ELIS»,
   3. «IPIS»,
   4. «Infopress»,
   5. «ISIS-Info»;

8 SR **235.1**

e. «ISIS06 Personensicherheitsprüfung» mit der Datenbank «Personensicherheitsprüfung»;

f. «ISIS07 Sicherheitspolitik» mit der Datenbank «Sicherheitspolitik».

2 Die Datenbanken enthalten die folgenden für die Aufgabenerfüllung des NDB gemäss Artikel 1 ZNDG bedeutsamen Informationen über das Inland:

a. «Staatsschutz» (ST): personen- und ereignisbezogene Informationen aus der präventiven Staatsschutztätigkeit;

b. «Verwaltungspolizei» (VP): personen- und ereignisbezogene Informationen aus dem Bereich der verwaltungspolizeilichen Zentralstellen des Bundesamtes für Polizei (fedpol);

c. «Dokumentation» (DO): dokumentarische Informationen aus der präventiven Staatsschutztätigkeit sowie Informationen aus öffentlich zugänglichen Quellen gemäss Artikel 9;

d. «Nummernsystem» (NU): ereignisbezogene Informationen aus ausgewählten Fahndungsprogrammen;

e. «Verwaltung» (VE): Informationen, die für die Geschäftskontrolle notwendig sind;

f. «NEWS»: staatsschutzrelevante Pressemeldungen aus dem Internet;

g. «ELIS»: elektronische Lagedarstellung der inneren Sicherheit;

h. «IPIS»: staatsschutzrelevante Presseagenturmeldungen;

i. «Infopress»: vom NDB täglich erstellte Presseauswertungen;

j. «ISIS-Info»: Informationsplattform für die Benutzerinnen und Benutzer von ISIS;

k. «Personensicherheitsprüfungen» (PSP): Informationen, die für die Geschäftskontrolle im Bereich Personensicherheitsprüfungen notwendig sind;

l. «ISIS07 Sicherheitspolitik» (SIPOL): sicherheitspolitisch bedeutsame Informationen zu Militär, Wirtschaft, Ressourcen, internationaler Politik und Strategie.

Art. 26 Bearbeitete Daten

1 Die in den ISIS-Datenbanken gespeicherten Daten werden, soweit für die Zugriffssteuerung sinnvoll, nach Sachgebieten in Kategorien eingeteilt.

2 Die ISIS-Datenbanken sind nach Meldungen, Objekten und Relationen strukturiert.

3 Das VBS regelt die einzelnen Datenfelder.

Art. 27 Abfrageberechtigungen

[1] ISIS kann von den folgenden Behörden und Amtsstellen abgefragt werden, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben notwendig ist:

a. von den Mitarbeiterinnen und Mitarbeitern des NDB und der kantonalen Organe zur Wahrung der inneren Sicherheit; sie sind über ein Abrufverfahren an das System angeschlossen;

b. von den Mitarbeiterinnen und Mitarbeitern des Bundessicherheitsdienstes (BSD), der Bundeskriminalpolizei (BKP), der Operativen Polizeikooperation, der Einsatzzentrale und der für den Erlass von Verfügungen von Fernhaltemassnahmen nach den Artikeln 67 Absatz 2 und 68 des Bundesgesetzes vom 16. Dezember 2005[9] über die Ausländerinnen und Ausländer zuständigen Stelle von fedpol; sie können mittels Abrufverfahren Kurzabfragen vornehmen;

c. von den Mitarbeiterinnen und Mitarbeitern der für die Personensicherheitsprüfung beim Bund zuständigen Stelle; sie können mittels Abrufverfahren Kurzabfragen vornehmen.

[2] Den kantonalen Organen zur Wahrung der inneren Sicherheit werden die klassifizierten Daten aus dem direkten Verkehr mit ausländischen Sicherheitsbehörden nicht angezeigt.

Art. 28 Technische Voraussetzungen für den Anschluss der Kantone

[1] Das VBS legt die technischen Voraussetzungen für den Anschluss der kantonalen Organe zur Wahrung der inneren Sicherheit fest.

[2] Die kantonalen Organe werden erst an ISIS angeschlossen, wenn sie diese Voraussetzungen erfüllen.

Art. 29 Dateneingabe und Qualitätskontrolle

[1] In ISIS dürfen nur Informationen bearbeitet werden, die den Zweckbestimmungen nach Artikel 3 entsprechen.

[2] Die Voranalyse des NDB gibt die Daten in ISIS ein und legt die Meldungskategorie fest.

[3] Zusätzlich können die folgende Personen die nachstehenden Daten eingeben und die Meldungskategorien festlegen:

a. die Mitarbeiterinnen und Mitarbeiter des Ausländerdienstes des NDB: Daten aus der Fotopasskontrolle;

b. die Mitarbeiterinnen und Mitarbeiter der Auswertung des NDB: Faktenblätter;

c. die Mitarbeiterinnen und Mitarbeiter des Bereichs Personensicherheitsprüfungen: Daten der Datenbank PSP.

9 SR **142.20**

4 Informationen der Datenbank ST werden vorerst provisorisch eingegeben («p»-Code) und nach Herkunft, Übermittlungsart, Inhalt und bereits vorliegenden Erkenntnissen wie folgt bewertet:

a. mit dem «g»-Code für gesicherte Meldungen;

b. mit dem «u»-Code für ungesicherte Meldungen.

5 Die Qualitätssicherung ISIS überprüft den Inhalt der provisorischen Erfassungen, namentlich die Quellenangabe, die Bewertung der Information und das Datum der nächsten Gesamtbeurteilung, und bestätigt die definitive Erfassung der Daten («k»-Code).

6 Die Direktorin oder der Direktor des NDB oder die Stellvertreterin oder der Stellvertreter kann die Qualitätssicherung ISIS mit einer Überprüfung der übrigen Datenbanken beauftragen.

Art. 30 Aktenablage

1 Die Aktenablage hat die ordnungsgemässe Aktenführung und Archivierung zu gewährleisten.

2 Die den Objekten und Meldungen zu Grunde liegenden Akten können als OCR-Daten erfasst werden. Ausgenommen sind die Datenbanken ST und PSP; in diesen erfolgt die Erfassung der Akten nur als Bilddaten.

3 Auf die Ablage der Akten in Papierform kann verzichtet werden, sofern die den Objekten und Meldungen zu Grunde liegenden Akten als OCR- oder Bilddaten erfasst sind.

Art. 31 Auskunftsrecht betroffener Personen

Das Auskunftsrecht betroffener Personen richtet sich nach Artikel 18 BWIS.

Art. 32 Periodische Gesamtbeurteilung der Daten in der Datenbank ST

1 Die Qualitätssicherung ISIS führt spätestens fünf Jahre nach der Erfassung der ersten Meldung eines Datensatzes und drei Jahre nach der letzten Gesamtbeurteilung eine neue Gesamtbeurteilung des betreffenden Datensatzes durch.

2 Sie beurteilt unter Berücksichtigung der aktuellen Gefahren und Risiken, ob die in einem Datensatz erfassten Meldungen und Objekte bezüglich des Risikos für die innere Sicherheit einen erhöhten Plausibilitätsgrad aufweisen und die Daten für die weitere Staatsschutztätigkeit benötigt werden.

3 Meldungen und Relationen, die seit über drei Jahren als ungesichert gespeichert sind («u»-Code), können als solche bis zur nächsten Gesamtbeurteilung nur weiterbearbeitet werden, wenn:

a. sie für die Erfüllung der gesetzlichen Aufgaben notwendig sind; und

b. die Direktorin oder der Direktor des NDB oder die Stellvertreterin oder der Stellvertreter diese Bearbeitung bewilligt hat.

4 Bei der Weiterverwendung noch benötigter Daten ist die Gesamtbeurteilung zu vermerken.

5 Objekte, die seit über drei Jahren als Daten über Drittpersonen gekennzeichnet sind, werden anlässlich der Gesamtbeurteilung gelöscht.

6 Die Qualitätssicherung ISIS löscht die nicht mehr benötigten Daten.

Art. 33 Aufbewahrungsdauer

1 Für die Daten in ISIS gelten die folgenden maximalen Aufbewahrungsdauern:

a. für präventive Daten: 15 Jahre;

b. für Daten laufender präventiver Fahndungsprogramme: 20 Jahre;

c. für Daten über Einreiseverbote: bis 10 Jahre nach deren Ablauf;

d. für Daten aus Personensicherheitsprüfungsverfahren: 5 Jahre;

e. für Daten aus der Korrespondenz mit Amtsstellen: 30 Jahre;

f. für Daten aus der Korrespondenz mit Privaten: 10 Jahre;

g. für Daten der Datenbanken DO, NEWS, IPIS, Infopress und ISIS-Info: 45 Jahre.

2 Nach Ablauf ihrer Aufbewahrungsdauer sind die Daten und Akten zu vernichten.

Art. 34 Daten und Akten der kantonalen Organe zur Wahrung der inneren Sicherheit

1 Die kantonalen Organe zur Wahrung der inneren Sicherheit dürfen die im Rahmen ihrer Staatsschutztätigkeit für den Bund angelegten Daten und Akten längstens 5 Jahre aufbewahren.

2 Nach Ablauf ihrer Aufbewahrungsdauer sind die Daten und Akten zu vernichten.

Art. 35 Finanzierung

1 Der Bund finanziert den Datentransport bis zum zentralen Anschlusspunkt bei den Kantonen.

2 Die Kantone übernehmen:

a. die Anschaffungs- und Unterhaltskosten ihrer Geräte;

b. die Installations- und Betriebskosten für ihr Feinverteilungsnetz.

5. Abschnitt: Schlussbestimmungen

Art. 36 Aufhebung bisherigen Rechts

Die Verordnung vom 30. November 2001[10] über das Staatsschutz-Informations-System wird aufgehoben.

Art. 37 Inkrafttreten und Geltungsdauer

[1] Diese Verordnung tritt am 1. Januar 2010 in Kraft.

[2] Die Bestimmungen des 3. Abschnitts (Art. 17–24) gelten bis zum 31. Dezember 2014.

4. Dezember 2009

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Hans-Rudolf Merz
Die Bundeskanzlerin: Corina Casanova

10 AS **2001** 3173, **2004** 3495 4813, **2006** 921, **2008** 4943 5525 6305