

Verordnung über das Staatsschutz-Informationssystem (ISIS-Verordnung)

vom 30. November 2001 (Stand am 1. Januar 2009)

Der Schweizerische Bundesrat,

gestützt auf die Artikel 15 Absätze 3 und 5 sowie 30 des Bundesgesetzes vom 21. März 1997¹ über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) und auf die Artikel 31c, 32a und 32b des Waffengesetzes vom 20. Juni 1997^{2,3}
verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand

Diese Verordnung regelt Betrieb, Datenbestand und Nutzung des informatisierten Staatsschutz-Informationssystems (ISIS).

Art. 2 Zweck

¹ ISIS dient folgenden Zwecken:

- a. dem eidgenössischen präventiven Staatsschutz;
- b. sicherheits- und verwaltungspolizeilichen Aufgaben;
- c. dem Vollzug der Waffengesetzgebung.

² Es wird verwendet zur:

- a.⁴ Recherche und Analyse der erfassten Daten;
- b. Erstellung von Lageberichten;
- c. Erledigung von administrativen Aufgaben;
- d. Ablage und Verwaltung von Akten;

AS 2001 3173

¹ SR 120

² SR 514.54

³ Fassung gemäss Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR 514.541).

⁴ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS 2004 3495).

- e.⁵ Dokumentation;
- f.⁶ Geschäftsabwicklung.

Art. 3⁷ Begriffe

In dieser Verordnung bedeuten:

- a. Daten: im ISIS gespeicherte Informationen;
- b. Objekte: Zusammenstellungen von Daten, die sich auf eine oder mehrere Personen, Sachen oder Ereignisse beziehen;
- c. Meldungen: Einzelne Informationseingänge zu einem oder mehreren Objekten;
- d. Relationen: Beziehungen zwischen einzelnen Objekten und Meldungen;
- e. Datensätze: Meldungen und Relationen eines Objekts;
- f. OCR-Daten: Daten von Akten, die so eingelesen wurden, dass eine Freitextsuche möglich ist;
- g. Bilddaten: Dokumente, die in Form von Bildern eingelesen wurden;
- h. Kurzabfragen: Online-Abfragen zur Feststellung, ob eine Person im ISIS verzeichnet ist;
- i. Drittpersonen: Personen oder Organisationen, die nur über den Bezug zu einem Objekt eine Staatsschutzrelevanz haben;
- j. Factsheets: Standardisierte, periodisch nachgeführte Beurteilungen der strategischen Analyse zu einem bestimmten Objekt.

Art. 4⁸ Systeme und Datenbanken

¹ ISIS besteht aus den folgenden Systemen und Datenbanken:

- a. «ISIS00 Allgemein» mit der Aktenablage, Auftragsverwaltung, Risikoanalyse, Statistik und dem Archivierungsmodul;
- b.⁹ «ISIS01 Staatsschutz» mit den Datenbanken «Staatsschutz», «Dokumentation» und «Nummernsystem»;
- c. «ISIS02 Verwaltung» mit der Datenbank «Verwaltung»;

⁵ Eingefügt durch Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁶ Eingefügt durch Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁷ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁸ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁹ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

- d.¹⁰ «ISIS03 Waffen» mit den Datenbanken «Waffenerwerb durch Ausländer», «Entzug von Bewilligungen und die Beschlagnahme von Waffen» und «Verwaltungspolizei»;
 - e. «ISIS04 Sprengstoff» mit der Datenbank «BARBARA»;
 - f. «ISIS05 News» mit den Datenbanken «NEWS», «Interaktives Portal für Open Sources», «ELIS», «IPIS», «Infopress» und «ISIS-Info»;
 - g. «ISIS06 Personensicherheitsprüfung» mit der Datenbank «Personensicherheitsprüfung».
- ² Die Datenbanken beinhalten folgende Informationen:
- a. «Staatsschutz» (ST): personen- und ereignisbezogene Informationen aus der präventiven Staatsschutzstätigkeit;
 - b.¹¹ «Verwaltungspolizei» (VP): personen- und ereignisbezogene Informationen aus dem Bereich der verwaltungspolizeilichen Zentralstellen des Bundesamtes für Polizei (fedpol);
 - c. «Dokumentation» (DO): dokumentarische Informationen aus dem gesamten Arbeitsbereich des DAP sowie gemäss Artikel 11 der Verordnung vom 27. Juni 2001¹² über Massnahmen zur Wahrung der inneren Sicherheit (VWIS);
 - d. «Nummernsystem» (NU): ereignisbezogene Informationen aus ausgewählten Fahndungsprogrammen;
 - e. «Verwaltung» (VE): Informationen, die für die Geschäftskontrolle notwendig sind;
 - f. «Waffenerwerb durch Ausländer» (DEWA): personenbezogene Informationen über den Erwerb von Waffen durch Ausländer ohne Niederlassungsbewilligung in der Schweiz;
 - fbis.¹³ «Waffenerwerb durch Personen mit Wohnsitz in einem anderen Schengen-Staat» (DEWS): personenbezogene Informationen über den Erwerb von Waffen oder wesentlichen Waffenbestandteilen durch Personen, die in einem anderen Staat Wohnsitz haben, der durch eines der Schengen-Assoziierungsabkommen gebunden ist;
 - g. «Entzug von Bewilligungen und die Beschlagnahme von Waffen» (DEBBWA): personenbezogene Informationen über den Entzug von Bewilligungen und die Beschlagnahme von Waffen in der Schweiz;

¹⁰ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

¹¹ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

¹² SR **120.2**

¹³ Eingefügt durch Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR **514.541**).

g^{bis}.¹⁴ «Abgabe und Entzug von Waffen der Armee» (DAWA): Informationen über Personen, die beim Austritt aus der Armee eine Waffe zu Eigentum erhalten haben oder denen aufgrund der Militärgesetzgebung die persönliche Waffe oder die persönliche Leihwaffe entzogen wurde;

g^{ter}.¹⁵ «Auswertung von Schusswaffenspuren» (ASWA): personenbezogene Informationen zur Auswertung von Schusswaffenspuren an Waffen, Munition, insbesondere Tatmunition, und an Personen, die an Straftaten beteiligt oder von ihnen betroffen waren;

h. «BARBARA»: ereignisbezogene Informationen aus dem Arbeitsbereich der Zentralstelle Sprengstoff und Pyrotechnik;

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

j. «Interaktives Portal für Open Sources» (IPOS): personalisiertes Portal zur Nutzung öffentlich zugänglicher Quellen;

k. «ELIS»: Elektronische Lagedarstellung der inneren Sicherheit;

l. «IPIS»: staatsschutzrelevante Presseagenturmeldungen;

m. «Infopress»: vom DAP täglich erstellte Presseauswertungen;

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

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

³ Die Schengen-Assoziierungsabkommen sind im Anhang aufgeführt.¹⁶

Art. 5¹⁷ 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. Die einzelnen Datenfelder werden vom Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) und vom Eidgenössischen Departement für Justiz und Polizei (EJPD) im jeweiligen Verantwortungsbereich nach Artikel 22 geregelt.¹⁸

¹⁴ Eingefügt durch Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR **514.541**).

¹⁵ Eingefügt durch Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR **514.541**).

¹⁶ Eingefügt durch Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR **514.541**).

¹⁷ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

¹⁸ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

Art. 6 Intranet

¹ Das «Intranet ISIS» ist ein chiffriert betriebenes Kommunikationssystem innerhalb von ISIS.¹⁹

² Der DAP stellt dieses System ausschliesslich den ISIS-Benutzern zur Verfügung.

2. Abschnitt: Benutzer, Anschluss und Datenzugriff**Art. 7²⁰** Benutzerinnen und Benutzer

¹ Benutzerinnen und Benutzer von ISIS sind:

- a. die Bediensteten des Dienstes für Analyse und Prävention (DAP) und der kantonalen Organe zur Wahrung der inneren Sicherheit; sie sind über ein Abrufverfahren an das System angeschlossen;
- b. die Mitarbeiterinnen und Mitarbeiter des Bundessicherheitsdienstes (BSD), der Bundeskriminalpolizei (BKP), der Zentralstellen Waffen und Sprengstoff und Pyrotechnik und der für den Erlass von Verfügungen von Fernhaltmassnahmen nach den Artikeln 67 Absatz 2 und 68 des Bundesgesetzes vom 16. Dezember 2005²¹ über die Ausländerinnen und Ausländer zuständigen Stelle von fedpol; sie können mittels Abrufverfahren Kurzabfragen vornehmen;
- c. die Mitarbeiterinnen und Mitarbeiter der für die Personensicherheitsprüfung beim Bund zuständigen Stelle (Fachstelle PSP, Abteilung Informations- und Objektsicherheit); sie können mittels Abrufverfahren Kurzabfragen vornehmen.²²

² Die Benutzerinnen und Benutzer von ISIS haben auf die Daten Zugriff, die sie zur Erfüllung ihrer gesetzlichen Aufgaben benötigen.

³ Den kantonalen Organen zur Wahrung der inneren Sicherheit werden die klassifizierten Daten aus dem direkten Verkehr mit ausländischen Sicherheitsbehörden nicht angezeigt.

⁴ Die Zugriffsberechtigungen werden vom VBS und vom EJPD im jeweiligen Verantwortungsbereich nach Artikel 22 geregelt. Über die individuellen Anträge entscheidet die Direktorin oder der Direktor des DAP oder von fedpol beziehungsweise die jeweilige Stellvertretung.²³

¹⁹ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

²⁰ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

²¹ SR **142.20**

²² Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

²³ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

⁵ Die Qualitätssicherung des DAP und die zuständige Stelle bei fedpol sind für den Vollzug der Zugriffsberechtigungen im jeweiligen Verantwortungsbereich nach Artikel 22 zuständig.²⁴

Art. 8²⁵ Anschluss der Kantone

Das VBS²⁶ legt die Voraussetzungen für den Anschluss der kantonalen Organe zur Wahrung der inneren Sicherheit fest. Diese werden erst an ISIS angeschlossen, wenn sie diese Voraussetzungen erfüllen.

Art. 9²⁷

3. Abschnitt: Datenbearbeitung

Art. 10 Dateneingabe und Qualitätskontrolle

¹ In ISIS dürfen nur Informationen bearbeitet werden, die den Zweckbestimmungen nach Artikel 2 entsprechen.

² Die Voranalyse des DAP gibt die Daten in ISIS ein und legt die Meldungskategorie fest.²⁸

^{2bis} Zusätzlich können folgende Personen Daten eingeben und die Meldungskategorien festlegen:

- a. die Mitarbeiterinnen und Mitarbeiter des Ausländerdienstes des DAP: Daten aus der Fotopasskontrolle;
- b. die Mitarbeiterinnen und Mitarbeiter der Zentralstelle Waffen von fedpol: Daten der Datenbanken DEWA, DEWS, DEBBWA, DAWA und VP;
- c. die Mitarbeiterinnen und Mitarbeiter der Zentralstelle Sprengstoff und Pyrotechnik von fedpol: Daten der Datenbank BARBARA und VP;
- d. die Mitarbeiterinnen und Mitarbeiter der Analyse des DAP: Factsheets;
- e. die Mitarbeiterinnen und Mitarbeiter des Bereichs Personensicherheitsprüfungen: Daten der Datenbank PSP.²⁹

²⁴ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

²⁵ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

²⁶ Ausdruck gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305). Diese Änderung wurde im ganzen Erlass berücksichtigt.

²⁷ Aufgehoben durch Ziff. I der V vom 30. Juni 2004, mit Wirkung seit 1. Sept. 2004 (AS **2004** 3495).

²⁸ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

²⁹ Eingefügt durch Ziff. I der V vom 30. Juni 2004 (AS **2004** 3495). Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

³ Informationen der Datenbanken ST und VP werden vorerst provisorisch eingegeben («p»-Code) und nach Herkunft, Übermittlungsart, Inhalt und bereits vorliegenden Erkenntnissen bewertet («g»-Code für gesicherte Meldungen und «u»-Code für ungesicherte Meldungen).³⁰

⁴ Die Qualitätssicherung des DAP und die zuständige Stelle bei fedpol überprüfen im jeweiligen Verantwortungsbereich nach Artikel 22 den Inhalt der provisorischen Erfassungen, namentlich die Quellenangabe, die Bewertung der Information und das Datum der nächsten Gesamtbeurteilung und bestätigen die definitive Erfassung der Daten («k»-Code).³¹

⁵ Die Direktorin oder der Direktor des DAP und von fedpol beziehungsweise die jeweilige Stellvertretung können den Qualitätssicherungsdienst mit der Überprüfung der übrigen Datenbanken in ihrem Verantwortungsbereich beauftragen.³²

Art. 11³³ Aktenablage

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

² Die den Objekten und Meldungen zu Grunde liegenden Akten können mit Ausnahme der Datenbanken ST, BARBARA und PSP als OCR-Daten erfasst werden. In den vorgenannten Datenbanken 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 Bilddaten erfasst sind.

Art. 12 Abfragen von Daten

¹ Die Daten können abgefragt werden nach Objekten, Relationen, Meldungen, Aufträgen und Freitext. Bilddaten sind nicht separat abrufbar.³⁴

² Die Abfrage von Meldungen ist jeweils nur innerhalb eines Systems zulässig.³⁵

³ Besonders ausgebildete Bedienstete des DAP können in ihrem Tätigkeitsgebiet Auswertungen vornehmen.

⁴ Die Objekte und ihre Relationen können visuell dargestellt und gespeichert werden.³⁶

³⁰ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

³¹ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

³² Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

³³ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

³⁴ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

³⁵ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

³⁶ Eingefügt durch Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

Art. 13 Weitergabe von Personendaten

¹ Der DAP kann, mit Ausnahme der im Rahmen von Personensicherheitsprüfungen erhobenen Daten, die in ISIS bearbeiteten Personendaten im Einzelfall weitergeben an:³⁷

- a. die kantonalen Strafverfolgungsbehörden zur Verhütung und Verfolgung strafbarer Handlungen;
- b. das Eidgenössische Departement für auswärtige Angelegenheiten für die Beurteilung von Akkreditierungsgesuchen oder der Anwesenheitsrechte von Angehörigen ausländischer Staaten oder internationaler Organisationen und dann, wenn es für die Wahrung völkerrechtlicher Schutzpflichten notwendig ist, sowie im Rahmen seiner Mitwirkungsrechte auf dem Gebiet des Aussenwirtschaftsrechts;
- c.³⁸ fedpol:
 1. zur Unterstützung von gerichtspolizeilichen Ermittlungsverfahren sowie für sachdienliche Vorabklärungen bei der Bekämpfung des organisierten Verbrechens und des unerlaubten Betäubungsmittelverkehrs,
 2. im Rahmen einer internationalen Amtshilfe in Strafsachen (INTERPOL),
 3. zur Aufnahme ins automatisierte Fahndungsregister RIPOl und ins N-SIS,
 4. zur Beurteilung von Sicherheitsrisiken beim Schutz von Personen und Gebäuden;
- d. das Bundesamt für Justiz, um Rechtshilfeersuchen in Strafsachen zu ergänzen oder auszuführen;
- e.³⁹ das Bundesamt für Migration (BFM) für Massnahmen gegenüber Ausländern, insbesondere zu deren Fernhaltung, für die Behandlung von Einbürgerungsgesuchen sowie für die Beurteilung von Asylgesuchen;
- f. ...⁴⁰
- g.⁴¹ andere Verwaltungseinheiten des VBS im Rahmen der Mitwirkungsrechte des VBS auf dem Gebiet des Aussenwirtschaftsrechts;

³⁷ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS 2008 6305).

³⁸ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS 2008 6305).

³⁹ Fassung gemäss Anhang Ziff. 2 der V vom 3. Nov. 2004, in Kraft seit 1. Jan. 2005 (AS 2004 4813).

⁴⁰ Aufgehoben durch Anhang Ziff. 2 der V vom 3. Nov. 2004, mit Wirkung seit 1. Jan. 2005 (AS 2004 4813).

⁴¹ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS 2008 6305).

- h. den Dienst für militärische Sicherheit:
 - 1. zur Beurteilung der militärischen Sicherheitslage,
 - 2. zum Schutz militärischer Informationen und Objekte,
 - 3. zur Erfüllung kriminal- und sicherheitspolizeilicher Aufgaben im Armeebereich,
und, wenn die Angehörigen des Dienstes zu Aktivdienst aufgeboden sind,
 - 4. zur präventiven Sicherung der Armee vor Spionage, Sabotage und anderen rechtswidrigen Handlungen,
 - 5. zur Beschaffung von Nachrichten,
 - 6. zum Schutz von Personen in staatstragenden Ämtern;
- i.⁴² den Strategischen Nachrichtendienst des VBS im Zusammenhang mit sicherheitspolitisch bedeutsamen Informationen und den Nachrichtendienst der Armee im Zusammenhang mit für die Armee bedeutsamen Informationen;
- j. die Militärjustiz zur Erfüllung kriminal- und sicherheitspolizeilicher Aufgaben;
- k. die Grenzschutz- und Zollorgane zur Aufenthaltsfeststellung von Personen, zur Durchführung zollamtlicher Kontrollen und von Verwaltungsstrafverfahren;
- l. das Staatssekretariat für Wirtschaft für den Vollzug des Bundesgesetzes vom 13. Dezember 1996⁴³ über das Kriegsmaterial sowie von Massnahmen auf dem Gebiet des Aussenwirtschaftsrechts;
- m. das Bundesamt für Berufsbildung und Technologie für die Erteilung von Sprengausweisen;
- n. das Bundesamt für Zivilluftfahrt und die Schweizerische Post für sicherheitspolizeiliche Massnahmen;
- o. das Bundesamt für Energie für den Vollzug des Atomgesetzes vom 23. Dezember 1959⁴⁴ und im Rahmen seiner Mitwirkungsrechte auf dem Gebiet des Aussenwirtschaftsrechts;
- p.⁴⁵ die für die Einleitung von Personensicherheitsprüfungen des Bundes und der Kantone zuständigen Stellen (ersuchende Stellen) oder die für die Durchführung zuständige Stelle des Bundes (Fachstelle PSP, IOS) oder die Fachstellen der Kantone;
- q. die betroffene Amtsstelle, wenn es zu deren Sicherheit notwendig ist;

⁴² Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

⁴³ SR **514.51**

⁴⁴ [AS **1960** 541, **1983** 1886 Art. 36 Ziff. 2, **1987** 544, **1993** 901 Anhang Ziff. 9, **1994** 1933 Art. 48 Ziff. 1, **1995** 4954, **2002** 3673 Art. 17 Ziff. 3, **2004** 3503 Anhang Ziff. 4. AS **2004** 4719 Anhang Ziff. I 1]. Siehe heute das Kernenergiegesetz vom 21. März 2003 (SR **732.1**).

⁴⁵ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

- r. Amtsstellen und Private, wenn die Weitergabe notwendig ist, um ein Auskunftsgesuch zu begründen;
- s. Private, wenn dadurch eine erhebliche Gefährdung abgewendet werden kann;
- t.⁴⁶ ausländische Sicherheitsbehörden im Rahmen von Clearing-Anfragen (Unbedenklichkeitsanfragen); Daten, die nicht im Interesse der betroffenen Person sind, können nur mit deren ausdrücklichen Zustimmung weitergegeben werden;
- u.⁴⁷ das Europäische Polizeiamt (Europol) zum Zweck der im Abkommen zwischen der Schweiz und dem Europäischen Polizeiamt vom 24. September 2004⁴⁸ vorgesehenen Zusammenarbeit.

² Für die Weitergabe an das Ausland gilt Artikel 17 Absätze 3–5 und 7 BWIS.

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

⁴ Bei jeder Weitergabe ist der Empfänger über die Bewertung und die Aktualität der Daten (Art. 10) in Kenntnis zu setzen. Er darf die Daten nur für den Zweck verwenden, für den sie ihm weitergegeben werden. Er ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass sich die weitergebende Behörde vorbehält, Auskunft über die vorgenommene Verwendung zu verlangen.

⁵ Die Weitergabe sowie ihr Adressat, Gegenstand und Grund sind zu registrieren.

⁶ Die Weitergabe von Daten der Datenbanken DEWA, DEWS, DEBBWA, DAWA und ASWA richtet sich nach den Artikeln 63 und 64 der Waffenverordnung vom 2. Juli 2008^{49,50}.

Art. 14 Kopieren von Daten in Datensammlungen

¹ ISIS-Daten dürfen weder über Kommunikationseinrichtungen noch über Datenträger in andere Datensammlungen kopiert werden. Von dieser Bestimmung ausgenommen ist die elektronische Archivierung der ISIS-Daten im Bundesarchiv.

² Zur Vornahme spezieller Auswertungen dürfen Daten aus ISIS kurzfristig in Arbeitsdatenbanken überführt werden. Nach Abschluss der Auswertungsarbeiten sind diese Daten zu löschen.

Art. 15 Auskunftsrecht von betroffenen Personen

¹ Das Auskunftsrecht richtet sich nach Artikel 18 BWIS.

⁴⁶ Eingefügt durch Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁴⁷ Eingefügt durch Ziff. I der V vom 10. März 2006 (AS **2006** 921).

⁴⁸ SR **0.360.268.2**

⁴⁹ SR **514.541**

⁵⁰ Fassung gemäss Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR **514.541**).

² Das Auskunftsrecht betreffend Daten der Datenbanken DEWA, DEWS, DEBBWA, DAWA und ASWA richtet sich nach Artikel 32g des Waffengesetzes vom 20. Juni 1997.⁵¹

Art. 16 Periodische Gesamtbeurteilung der Daten in der Datenbank ST

¹ Die Qualitätssicherung des DAP 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.⁵²

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.⁵³

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 sie für die Erfüllung der gesetzlichen Aufgaben notwendig sind und die Chefin oder der Chef des DAP oder deren oder dessen Stellvertreterin oder Stellvertreter diese Bearbeitung bewilligt hat.⁵⁴

⁴ Objekte, die seit über drei Jahren als Daten über Drittpersonen gekennzeichnet sind, werden anlässlich der Gesamtbeurteilung gelöscht.⁵⁵

⁵ Die Qualitätssicherung löscht die nicht mehr benötigten Daten. Bei der Weiterverwendung noch benötigter Daten ist die Gesamtbeurteilung zu vermerken.

Art. 17 Aufbewahrungsdauer

¹ Die präventiv-polizeilichen Daten dürfen in ISIS längstens 15 Jahre gespeichert werden.

² Für nachstehende Daten gilt folgende maximale Aufbewahrungsdauer:

- a. für Daten laufender präventiv-polizeilicher Fahndungsprogramme: 20 Jahre;
- b. für Daten über Einreisesperren: bis zehn Jahre nach deren Ablauf;
- c. für Daten aus Personensicherheitsprüfungsverfahren: Fünf Jahre;
- d. für Daten aus Korrespondenz mit Amtsstellen und Privaten: 30 respektive zehn Jahre.

⁵¹ Fassung gemäss Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR **514.541**).

⁵² Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁵³ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁵⁴ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁵⁵ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

³ Die Daten der Datenbank DO, BARBARA, IPOS, NEWS, IPIS, Infopress und ISIS-Info können zeitlich unbeschränkt aufbewahrt werden.⁵⁶

⁴ Die Aufbewahrung der Daten in den Datenbanken DEWA, DEWS, DEBBWA, DAWA und ASWA richtet sich nach Artikel 66 der Waffenverordnung vom 2. Juli 2008^{57,58}

Art. 18 Löschung der Daten

¹ Die Daten werden innert drei Monaten nach Ablauf ihrer Aufbewahrungsdauer gelöscht, es sei denn die Daten seien unter Beurteilung der aktuellen Risiken und Gefahren für die Erfüllung der gesetzlichen Aufgaben nach dem Entscheid der Chefin oder des Chefs des DAP oder von deren Stellvertreterin oder dessen Stellvertreter unentbehrlich.⁵⁹

² In den Fällen nach Absatz 1 beträgt die weitere Aufbewahrungsdauer drei Jahre. Die Verlängerung kann nur einmal erfolgen.

³ Mit der Löschung der letzten Meldung (inklusive der dazugehörigen Relationen, Bilddaten und Aufträge) werden der gesamte Datensatz sowie ein allfällig vorhandenes Factsheet gelöscht.⁶⁰

⁴ Zur Löschung vorgesehene Daten werden mit Ausnahme der in Artikel 20 Absatz 2 genannten Informationen ins Archivierungsmodul übertragen.⁶¹

Art. 19⁶² Daten und Akten der kantonalen Staatsschutzdienste

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

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

Art. 20 Anbietepflicht von Akten

¹ Nicht mehr benötigte oder zur Löschung oder Vernichtung bestimmte Daten und Akten werden dem Bundesarchiv zur Archivierung angeboten.⁶³

⁵⁶ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁵⁷ SR **514.541**

⁵⁸ Fassung gemäss Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR **514.541**).

⁵⁹ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁶⁰ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁶¹ Eingefügt durch Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁶² Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁶³ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

² Die aus dem direkten Verkehr mit ausländischen Sicherheitsdiensten und aus der operativen Beschaffung stammenden klassifizierten Unterlagen (Daten und Akten) werden nicht angeboten, sondern in Absprache mit dem Bundesarchiv intern aufbewahrt.⁶⁴

³ Die vom Bundesarchiv als nicht archivwürdig bezeichneten Daten werden aus dem Archivierungsmodul gelöscht. Die nicht als archivwürdig bezeichneten Akten werden vernichtet. Vorbehalten bleiben weitere gesetzliche Bestimmungen über die Datenvernichtung.⁶⁵

⁴ Der DAP trägt vor der Aktenabgabe der persönlichen Dossiers an das Bundesarchiv das Ablieferungsdatum, die Registraturnummer sowie die Personalien der betroffenen Person in die Datenbank Verwaltung ein, wo sie zehn Jahre aufbewahrt und alsdann gelöscht werden.

4. Abschnitt: Organisatorische Bestimmungen

Art. 21 Datensicherheit und Protokollierung

¹ Für die Gewährleistung der Datensicherheit gelten Artikel 20 der Verordnung vom 14. Juni 1993⁶⁶ zum Bundesgesetz über den Datenschutz, die Verordnung vom 26. September 2003⁶⁷ über die Informatik und Telekommunikation in der Bundesverwaltung sowie die vom VBS nach Artikel 8 festzulegenden Voraussetzungen für den Anschluss der kantonalen Organe zur Wahrung der inneren Sicherheit.⁶⁸

² Der DAP regelt in einem Bearbeitungsreglement die organisatorischen und technischen Massnahmen gegen unbefugtes Bearbeiten der Daten sowie die automatische Protokollierung der eingegebenen Daten.

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

Art. 22 Verantwortlichkeiten und Zuständigkeiten

¹ Der DAP trägt die Verantwortung für die folgenden Systeme und Datenbanken von ISIS: «ISIS00 Allgemein», «ISIS01 Staatsschutz», «ISIS02 Verwaltung», «ISIS05 News» und «ISIS06 Personensicherheitsüberprüfung». Er erlässt das Bearbeitungsreglement.⁶⁹

⁶⁴ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁶⁵ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁶⁶ SR **235.11**

⁶⁷ SR **172.010.58**

⁶⁸ Fassung gemäss Ziff. I der V vom 30. Juni 2004, in Kraft seit 1. Sept. 2004 (AS **2004** 3495).

⁶⁹ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

^{1bis} Fedpol trägt die Verantwortung für die folgenden Systeme und Datenbanken von ISIS: «ISIS03 Waffen», DEWA, DEWS, DEBBWA, DAWA, «ISIS04 Sprengstoff» und BARBARA. Es erlässt das Bearbeitungsreglement.⁷⁰

² Der DAP und fedpol sind zuständig für die Ausbildung und Betreuung der Benutzerinnen und Benutzer und sorgen für die Durchsetzung ihrer Bearbeitungsreglemente.⁷¹

³ Die technische Gesamtverantwortung für ISIS obliegt dem VBS. Der EDV-Leistungserbringer sorgt für den Betrieb, den Unterhalt und die Sicherheit von ISIS. Weiterentwicklungen des Informationssystems ISIS erfolgen in Absprache mit dem Anwendungsverantwortlichen von fedpol. Die Details der Zusammenarbeit werden in einer Verwaltungsvereinbarung geregelt.⁷²

⁴ Die Datenschutzberater des DAP und von fedpol können einzelfallweise und im jeweiligen Verantwortungsbereich die Bearbeitung von ISIS-Daten auf die Einhaltung der Datenschutzvorschriften überprüfen.⁷³

Art. 23 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.

Art. 24 Technische Anforderungen

¹ Das VBS legt die technischen Anforderungen fest, denen die Endgeräte der Kantone genügen müssen.

² Das Bearbeitungsreglement legt die Einzelheiten fest.

5. Abschnitt: Schlussbestimmungen

Art. 25 Aufhebung bisherigen Rechts

Die Verordnung vom 1. Dezember 1999⁷⁴ über das Staatsschutz-Informationssystem wird aufgehoben.

⁷⁰ Eingefügt durch Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

⁷¹ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

⁷² Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

⁷³ Fassung gemäss Anhang Ziff. 3 der V vom 12. Dez. 2008, in Kraft seit 1. Jan. 2009 (AS **2008** 6305).

⁷⁴ [AS **1999** 3461, **2000** 1227 Anhang Ziff. II 1 2027]

Art. 26⁷⁵**Art. 27** Inkrafttreten

Diese Verordnung tritt am 1. Januar 2002 in Kraft.

⁷⁵ Aufgehoben durch Ziff. I der V vom 30. Juni 2004, mit Wirkung seit 1. Sept. 2004 (AS **2004** 3495).

*Anhang*⁷⁶
(Art. 4 Abs. 3)

Schengen-Assoziierungsabkommen

Die Schengen-Assoziierungsabkommen umfassen:

- a. Abkommen vom 26. Oktober 2004⁷⁷ zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (SAA);
- b. Abkommen vom 26. Oktober 2004⁷⁸ in Form eines Briefwechsels zwischen dem Rat der Europäischen Union und der Schweizerischen Eidgenossenschaft über die Ausschüsse, die die Europäische Kommission bei der Ausübung ihrer Durchführungsbefugnisse unterstützen;
- c. Übereinkommen vom 17. Dezember 2004⁷⁹ zwischen der Schweizerischen Eidgenossenschaft, der Republik Island und dem Königreich Norwegen über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands und über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in der Schweiz, in Island oder in Norwegen gestellten Asylantrags;
- d. Abkommen vom 28. April 2005⁸⁰ zwischen der Schweizerischen Eidgenossenschaft und dem Königreich Dänemark über die Umsetzung, Anwendung und Entwicklung derjenigen Teile des Schengen-Besitzstands, die auf Bestimmungen des Titels IV des Vertrags zur Gründung der Europäischen Gemeinschaft basieren;
- e. Protokoll vom 28. Februar 2008⁸¹ zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union, der Europäischen Gemeinschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zum Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands.

⁷⁶ Eingefügt durch Anhang 4 Ziff. II 1 der Waffenverordnung vom 2. Juli 2008, in Kraft seit 12. Dez. 2008 (SR **514.541**).

⁷⁷ SR **0.360.268.1**

⁷⁸ SR **0.360.268.10**

⁷⁹ SR **0.360.598.1**

⁸⁰ SR **0.360.314.1**

⁸¹ SR **0.360.514.1**; noch nicht publiziert.